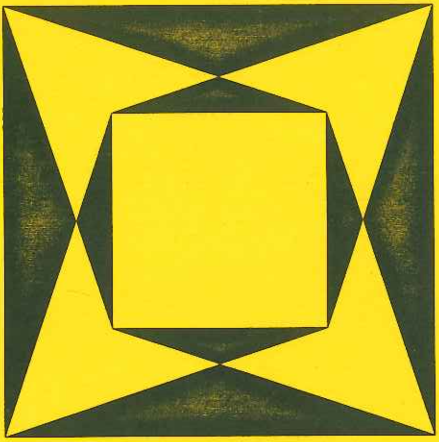
IRISH MATHEMATICAL SOCIETY

cumann matamaitice
na héireann



BULLETIN

NUMBER 37 CHRISTMAS 1996
ISSN 0791-5578

cumann matamaitice na héireann
IRISH MATHEMATICAL SOCIETY BULLETIN

EDITOR: Dr R. Gow
BOOK REVIEW EDITOR: Dr Michael Tuite
PRODUCTION MANAGER: Dr Mícheál Ó Searcóid

The aim of the Bulletin is to inform Society members about the activities of the Society and about items of general mathematical interest. It appears twice each year, at Easter and at Christmas. The Bulletin is supplied free of charge to members; it is sent abroad by surface mail. Libraries may subscribe to the Bulletin for IR£20.00 per annum.

The Bulletin seeks articles of mathematical interest written in an expository style. All areas of mathematics are welcome, pure and applied, old and new. The Bulletin is typeset using TEX. Authors are invited to submit their articles in the form of TEX input files if possible, in order to ensure speedier processing.

Correspondence concerning the Bulletin should be addressed to:

Irish Mathematical Society Bulletin
Department of Mathematics
University College
Dublin
Ireland

Printed in the University of Limerick

CONTENTS

Obituary

Articles

Book Review

cumann matamaitice na héireann
THE IRISH MATHEMATICAL SOCIETY

Officers and Committee Members

President	Dr D. Hurley	Department of Mathematics University College, Cork
Vice-President	Dr C. Nash	Department of Math. Physics St Patrick's College, Maynooth
Secretary	Dr P. Mellon	Department of Mathematics University College, Dublin
Treasurer	Dr J. Pulé	Department of Math. Physics University College, Dublin

Dr M. Clancy, Dr E. Gath, Mr G. Lessells, Dr R. Gow, Dr B. Goldsmith, Dr M. Tuite, Dr A. Wickstead, Dr K. Hutchinson.

Local Representatives

Carlow	RTC	Dr D. Ó Sé
Cork	RTC	Mr D. Flannery
	UCC	Dr M. Stynes
Dublin	DIAS	Dr D. Ó Mathúna
	DIT	
	DCU	Dr M. Clancy
	St Patrick's	Dr J. Cosgrave
	TCD	Dr R. Timoney
	UCD	Dr R. Gow
	Tallaght	
Dundalk	RTC	Dr M. O'Reilly
Galway	UCG	Dr M. Tuite
Limerick	MICE	Dr G. Enright
	UL	Mr G. Lessells
Maynooth		Dr C. Nash
Waterford	RTC	
Belfast	QUB	Prof. D. Armitage

NOTES ON APPLYING FOR I.M.S. MEMBERSHIP

1. The Irish Mathematical Society has reciprocity agreements with the American Mathematical Society and the Irish Mathematics Teachers Association.

2. The current subscription fees are given below.

Institutional member	IR£50.00
Ordinary member	IR£15.00
Student member	IR£6.00
I.M.T.A. reciprocity member	IR£5.00

   The subscription fees listed above should be paid in Irish pounds (puint) by means of a cheque drawn on a bank in the Irish Republic, a Eurocheque, or an international money-order.

3. The subscription fee for ordinary membership can also be paid in a currency other than Irish pounds using a cheque drawn on a foreign bank according to the following schedule:

   If paid in United States currency then the subscription fee is US$25.00.
   If paid in sterling then the subscription fee is £15.00 stg.
   If paid in any other currency then the subscription fee is the amount in that currency equivalent to US$25.00.

   The amounts given in the table above have been set for the current year to allow for bank charges and possible changes in exchange rates.

4. Any member with a bank account in the Irish Republic may pay his or her subscription by a bank standing order using the form supplied by the Society.

5. The subscription fee for reciprocity membership by members of the American Mathematical Society is US$10.00.

6. Any ordinary member who has reached the age of 65 years and has been a fully paid up member for the previous five years may pay at the student membership rate of subscription.

7. Subscriptions normally fall due on 1 February each year.

8. Cheques should be made payable to the Irish Mathematical Society. If a Eurocheque is used then the card number should be written on the back of the cheque.

9. Any application for membership must be presented to the Committee of the I.M.S. before it can be accepted. This Committee meets twice each year.

10. Please send the completed application form with one year's subscription fee to

The Treasurer, I.M.S.
Department of Math. Physics
University College, Dublin
Ireland

Minutes of the Meeting of the Irish Mathematical Society

Ordinary Meeting
4th April 1996

The Irish Mathematical Society held an Ordinary Meeting at 12.15pm on Thursday 4th April 1996 in the Dublin Institute for Advanced Studies, 10 Burlington Road. There were 16 members present. The President, D. Hurley was in the chair. Apologies were received from F. Holland and K. Hutchinson.

1. The minutes of the meeting of 21st December 1995 were approved and signed.

2. **Matters arising**

- A letter has been sent to the European Mathematical Society (EMS) explaining that the society could not afford to pay the full level of its subscriptions to the EMS, and enclosing part-payment. No reply has yet been received. Concern was expressed that individual membership should be continued in the usual manner and it was agreed that the individual memberships would be forwarded at the end of the month.
- It was reported that letters had been sent to the college officers of the University of Rochester, protesting at the proposed closure of its graduate program. No further information was available to date.
- It was felt that a perpetual trophy for the winner of the Irish National Mathematical Olympiad Competition would help in publicizing the event and raising sponsorship. It was suggested that the trophy should have some interesting geometric shape. T. Laffey, G. Lessells and J. Pulé agreed to investigate sponsorship, design and other practicalities of the trophy and to report back to the December meeting.
- It was agreed that the society should liaise with the Irish Mathematics Teachers Association (IMTA) to organize a mathematics afternoon for Transition Year students from secondary schools in

Cork, Dublin and Limerick in September 1996. All were encouraged to suggest speakers.

- R. Timoney was thanked for setting up an IMS page on the World Wide Web. Its address is

http://www.maths.tcd.ie/pub/ims.

Departments were asked to add a pointer in the home pages of their entry on the WWW to the IMS page.

3. Bulletin

The issue of advertising in the bulletin was discussed. M. Tuite agreed to approach publishers on this matter.

It was mentioned that instructions to authors may be changed from Tex to Latex, as Latex appears to be more commonly used. Thanks were expressed to the editor.

4. Treasurer's business

The treasurer gave his financial report and was thanked. G. Lessells agreed to send a letter of thanks and a copy of the Bulletin to those people and institutions who gave financial support to last year's September Meeting.

5. September Meeting

D. Armitage reported that organization for the 1996 September Meeting is well under way and principal speakers arranged. Speakers for short talks were requested. The conference will be held in the Applied Mathematics building in Queen's University Belfast. A conference banquet will be held in the Great Hall of the university. The president appealed to all members to make a special effort to attend the September Meeting.

6. Any other business

The issue of awarding bonus points to honours mathematics in the Leaving Certificate was discussed. S. Dineen requested that any information or statistics that might support this practice be sent to him.

The meeting closed at 1.05pm.

Pauline Mellon
University College Dublin.

PROFESSOR JOHN LIGHTON SYNGE, FRS
Obituary

Professor John Lighton Synge, the most distinguished Irish mathematician and theoretical physicist since Sir William Rowan Hamilton (1805-1865), died in Dublin on March 30, 1995, exactly one week after his 98th birthday.

He entered Trinity College in 1915 and by the end of his first year he won a Foundation Scholarship in mathematics, an extraordinary achievement in view of the fact that in those days the Foundation Scholarship examination was normally taken in the third year. He graduated in 1919 with a Senior Moderatorship in Mathematics and Experimental Physics and a Large Gold Medal.

After a brief lectureship in mathematics in Trinity College he left for Canada in 1920 to join the University of Toronto as Assistant Professor in Mathematics. He returned to Trinity in 1925 to a Fellowship and the Chair of Natural Philosophy until 1930. His most brilliant students during this period were the late Dr A. J. McConnell (geometer and one time Provost of Trinity College) and the late Professor E. T. S. Walton (experimental physicist and Nobel laureate with Cockcroft).

He left Trinity College again in 1930 and after a succession of senior appointments at the universities of Toronto, Ohio, Princeton, Maryland and Pittsburgh, and a brief appointment as ballistic mathematician in the US Air Force during the war, he returned to his native Dublin in 1948 as a Senior Professor in the School of Theoretical Physics of the Dublin Institute for Advanced Studies.

It was during Professor Synge's tenure that the Dublin Institute for Advanced Studies became one of the great centres in relativity theory. Up to the mid sixties, and primarily under his influence, about 12% of the world's relativists passed, physically, through the Institute.

Professor Synge made outstanding contributions to widely varied fields: classical mechanics, geometrical mechanics and geometrical optics, gas dynamics, hydrodynamics, elasticity, electrical networks, mathematical methods, differential geometry and, above all, Einstein's theory of relativity. His approach to mathematical physics in general, and to relativity theory in particular, is characterized by his extraordinary geometrical insight. He felt just as much at home in the ordinary three dimensional Euclidean space as in the four dimensional space-time of relativity. In an astonishing paper in the Proceedings of the Royal Irish Academy (Vol. 53, Section *A*, No. 6, 1950) he was able, for the first time, to penetrate and explore in detail the region inside the Schwarzschild radius (what we now call a black hole). At a time when many relativists thought that it didn't even make sense to talk about this region, this work is very remarkable indeed.

The almost universal **geometrical** approach to the theory of relativity in the last thirty years or so is due primarily to Professor Synge's influence. As Professor Sir Hermann Bondi remarked in 1992, besides the 12% of relativists who were directly influenced by Professor Synge, "Every one of the other 88% has been deeply influenced by his geometric vision and the clarity of his expression". It is on record that the outstanding relativist Professor Sir Roger Penrose, and through him Stephen Hawking, decided to go seriously into the field of relativity after reading Synge's books on the subject.

He published eleven books, including three fascinating and delightful semi-popular books, and over two hundred papers, the last one at the age of 92; it was, appropriately enough, on geometry. Every single book and every single paper is a remarkable work of art.

His geometric insight and clarity of expression permeate all his scientific and semi-popular writings and all his superb lectures and seminars. His motto in all his writings, but especially in his semi-popular ones, is "The mind is at its best when at play", as he put it. He uses his fertile imagination and the "clarity of expression", and the sheer beauty of his prose, a gift he no doubt inherited from his uncle, the famous playwright J. M. Synge, to set the mind of the reader "at play"; at the same time, imparting knowledge to the mind effortlessly and almost unconsciously.

His two passionate hobbies were cycling and sailing. While at the University of Pittsburgh he was cycling wearing a nose mask to protest against the polluted atmosphere of the city. He was, also, an accomplished painter. Well after retirement he took up the mandoline but without much success.

His mind was lively and vivid almost to the very end of his life. He continued reading three or four books a week and thinking about mathematical problems. On one of his visits just a few months before his death the present author was evidently surprised to see him reading a big medical book on the circulation of blood. Seeing my surprise he said "Oh, I have some troubles with the circulation of blood in my legs and I decided to learn something about it". On another visit, towards the end of 1993, he told me that the problem that occupied his mind at the time was Fermat's last theorem. When I ventured to say that "the problem was solved last July", he said"Oh, I know that, but I am thinking of the problem from a different angle, in terms of the zeroes of the Fermat function $x^t + y^t - z^t$. You can think of t as a parameter and (x, y, z) as a point in a three dimensional space or you can think of (x, y, z, t) as a point in a four dimensional space". I don't know how far this approach would have led him, but it clearly indicated that his "geometrical vision" remained undiminished to the very end.

Professor Synge married Elizabeth Eleanor Mabel Allen in 1918 while they were both undergraduates in Trinity College; she died after a prolonged illness in 1985. He is survived by two daughters, Mrs Isobel Seddon and Professor Cathleen Morawetz. Professor Morawetz, an eminent mathematician in her own right, has the distinction of having been the first woman to hold the Directorship of the famous New York Courant Institute. She is currently the President of the American Mathematical Society.

Trinity College, Synge's *Alma Mater*, honours one of its most distinguished graduates on a permanent basis by the **J. L. Synge Prize in Mathematics** and the **J. L. Synge Public Lecture**, each being given in alternate years. The first J. L. Synge Prize in Mathematics was shared by John Callan and Raymond Russell in 1993, and the second was awarded to Conal Kennedy in 1995. The first J. L. Synge Public Lecture was given by Professor Sir Hermann Bondi in 1992, and the second by Professor Werner Israel, a student of Professor Synge. The third lecture was given by Professor Sir Roger Penrose on May 7, 1996.

Professor Synge was a kind and generous man. He encouraged and inspired several generations of students who will always remember him with gratitude, fondness and the deepest respect.

Petros S. Florides,
School of Mathematics,
Trinity College,
Dublin 2,
Ireland.

A CONIC AND A PASCAL LINE AS CUBIC LOCUS

P. D. Barry

1. Statement of results

This material arose out of an effort to generalize a result of William Wallace in 1797, to the effect that the feet of the perpendiculars from a point on the circumcircle of a triangle onto the side-lines are collinear. Through historical mis-attribution, the lines of collinearity have been widely known as *Simson lines*.

Our most general result is Theorem 3. A reduced case of that is Theorem 1. A converse of the latter is Theorem 2, and this constitutes an enhancement of the configuration in the celebrated Pascal's theorem.

Theorem 1. *In a projective plane, let A_1, A_2, A_3 be non-collinear points and B_1, B_2, B_3 distinct collinear points such that*

$$B_1 \neq A_2,\, A_3,\ B_2 \neq A_3,\, A_1,\ B_3 \neq A_1,\, A_2,$$

$$A_2B_3 \neq A_3B_2,\ A_3B_1 \neq A_1B_3,\ A_1B_2 \neq A_2B_1 \tag{1}$$

Let C_1, C_2, C_3 be the points specified by

$$C_1 = A_2B_3 \cap A_3B_2,\ C_2 = A_3B_1 \cap A_1B_3,\ C_3 = A_1B_2 \cap A_2B_1. \tag{2}$$

For a variable point P, take points $Q_1 \in A_2A_3$, $Q_2 \in A_3A_1$, $Q_3 \in A_1A_2$, such that $Q_1 \in PB_1$, $Q_2 \in PB_2$, $Q_3 \in PB_3$. Then the set $\mathcal{E}_1$ of points P for which Q_1, Q_2, Q_3 are collinear, contains the points A_1, A_2, A_3, B_1, B_2, B_3, C_1, C_2, C_3. It is either the whole plane or else a conic through A_1, A_2, A_3, C_1, C_2, C_3, and *the line $B_1B_2B_3$. The degenerate case of the plane occurs when $B_1 \in A_2A_3$, $B_2 \in A_3A_1$, $B_3 \in A_1A_2$.*

Now by (2) we also have

$$A_2C_3 \cap A_3C_2 = B_1,\ A_3C_1 \cap A_1C_3 = B_2,\ A_1C_2 \cap A_2C_1 = B_3, \quad (3)$$

so we have the conic through A_1, A_2, A_3, C_1, C_2 and C_3, and the Pascal line $B_1B_2B_3$. This is the configuration of Pascal's theorem.

Working somewhat in reverse and starting differently, we can also state the following, which is a converse of Theorem 1.

Theorem 2. *In a projective plane, let $\mathcal{C}_1$ be a proper point conic, and A_1, A_2, A_3, C_1, C_2, C_3 distinct points on $\mathcal{C}_1$. Let*

$$A_2C_3 \cap A_3C_2 = B_1,\ A_3C_1 \cap A_1C_3 = B_2,\ A_1C_2 \cap A_2C_1 = B_3,$$

so that B_1, B_2, B_3 are collinear. If for any point P, PB_1 meets A_2A_3 at Q_1, PB_2 meets A_3A_1 at Q_2 and PB_3 meets A_1A_2 at Q_3, then Q_1, Q_2 and Q_3 are collinear if and only P is on $\mathcal{C}_1$ or on the line $B_1B_2B_3$.

Figure 1 refers to Theorems 1 and 2.

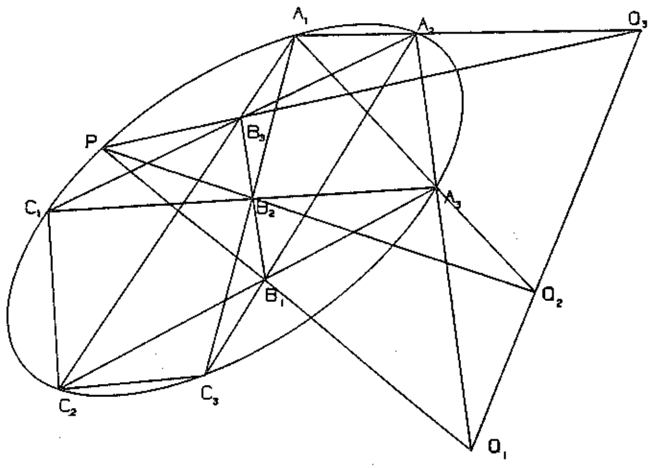


Figure 1

A conic and a line constitute a reducible cubic and our locus is essentially a cubic. Our approach has caused us to take B_1, B_2 and B_3 to be collinear, and if we take them to be non-collinear we find that we obtain a cubic which passes through A_1, A_2, A_3, B_1, B_2, B_3, C_1, C_2, and C_3.

Theorem 3. *In a projective plane, let a_1, a_2, a_3 be distinct lines and write*

$$A_1 = a_2 \cap a_3,\ A_2 = a_3 \cap a_1,\ A_3 = a_1 \cap a_2.$$

Let B_1, B_2, B_3 be distinct points such that (1) is satisfied, and let C_1, C_2, C_3 be defined by (2). For a variable point P, let

$$PB_1 \cap a_1 = Q_1,\ PB_2 \cap a_2 = Q_2,\ PB_3 \cap a_3 = Q_3.$$

Then the set $\mathcal{E}_1$ of points P such that Q_1, Q_2, Q_3 are collinear is either a point cubic or the whole plane. The set $\mathcal{E}_1$ contains each of the points A_1, A_2, A_3, B_1, B_2, B_3, C_1, C_2, C_3, and it degenerates to the plane if and only if B_1, B_2, B_3 are collinear and $B_1 \in a_1$, $B_2 \in a_2$, $B_3 \in a_3$.

2. Proofs

To start on our proofs, in a projective plane we let a_1, a_2, a_3 be distinct lines and write

$$A_1 = a_2 \cap a_3,\ A_2 = a_3 \cap a_1,\ A_3 = a_1 \cap a_2.$$

Let B_1, B_2, B_3 be distinct points satisfying (1). We then introduce the points C_1, C_2, C_3 in (2). For a variable point P, let

$$PB_1 \cap a_1 = Q_1,\ PB_2 \cap a_2 = Q_2,\ PB_3 \cap a_3 = Q_3.$$

We seek the set $\mathcal{E}_1$ of points P such that Q_1, Q_2, Q_3 are collinear. It can be checked directly from the definition that A_1, A_2, A_3, B_1, B_2, B_3, C_1, C_2, C_3 are all in $\mathcal{E}_1$, and indeed that if B_1, B_2, B_3 are collinear, then every point P of the line $B_1B_2B_3$ is in $\mathcal{E}_1$.

Supposing first that a_1, a_2, a_3 are not concurrent, as in [1] we use homogeneous coordinates and take a triangle of reference so that

$$A_1 = (1,0,0),\ A_2 = (0,1,0),\ A_3 = (0,0,1).$$

Suppose that

$$B_1 = (a,b,c),\ B_2 = (d,e,f),\ B_3 = (g,h,k),\ P = (x,y,z). \quad (4)$$

Then

$$\begin{aligned} Q_1 &= (0, -bx + ay, -cx + az), \\ Q_2 &= (ex - dy, 0, ez - fy), \\ Q_3 &= (kx - gz, ky - hz, 0). \end{aligned} \quad (5)$$

Hence for Q_1, Q_2, Q_3 to be collinear it is necessary and sufficient that

$$\det \begin{pmatrix} 0 & -bx + ay & -cx + az \\ ex - dy & 0 & ez - fy \\ kx - gz & ky - hz & 0 \end{pmatrix} = 0,$$

which expands to

$$(ay - bx)(ez - fy)(kx - gz) + (az - cx)(ex - dy)(ky - hz) = 0,$$

and then to

$$\begin{aligned} &a(fg - dk)y^2z + a(dh - eg)yz^2 + e(bg - ah)z^2x + e(ch - bk)zx^2 \\ &\quad + k(bf - ce)x^2y + k(cd - af)xy^2 + (2aek - bfg - cdh)xyz = 0.(6) \end{aligned}$$

Turning now specifically to Theorem 1, we note that a condition that B_1, B_2, B_3 be collinear is that

$$\Delta = \det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & k \end{pmatrix}$$

satisfy $\Delta = 0$. As A_1, A_2, A_3 are not collinear, at least one of them is not on B_1B_2. If $A_3 \notin B_1B_2$ we can solve $\Delta = 0$ for k and insert in (6) to obtain the product of

$$(bf - ce)x + (cd - af)y + (ae - bd)z \quad (7)$$

which gives the equation of $B_1B_2B_3$, and

$$a(dh - eg)yz + e(bg - ah)zx + [f(ah - bg) + c(eg - dh)]xy. \quad (8)$$

This last yields a conic unless all its coefficients are equal to 0, in which case the locus is degenerate. The other cases are treated similarly. This establishes Theorem 1, apart from analysing fully the degenerate case which we shall return to later.

For Theorem 2, we start by supposing that A A_2, A_3, C_1, C_2, C_3 are on a proper conic $\mathcal{C}_1$. We define B_1, B_2, B_3 by (3) and then (2) holds. Here $A_3 \notin B_1B_2$, so we obtain (7) and (8). Now (8) cannot degenerate to having all its coefficients equal to 0, as *e.g.* $B_1 \notin A_2A_3$, $A_3 \notin B_2B_3$ imply

$$a \neq 0,\ dh - eg \neq 0.$$

Thus (8) gives the equation of a conic through A_1, A_2, A_3, C_1, C_2, C_3, and hence of $\mathcal{C}_1$. This establishes Theorem 2. We note that in it, the roles of (A_1, A_2, A_3) and (C_1, C_2, C_3) are interchangeable.

Continuing so as to cover the case where B_1, B_2, B_3 are not collinear, we suppose that a_1, a_2, a_3, A_1, A_2, A_3, B_1, B_2, B_3, C_1, C_2, C_3, P, Q_1, Q_2, Q_3 are as before, except that now we take a_1, a_2, a_3 to be any three distinct lines (so that they may be concurrent and then $A_3 = A_2 = A_1$), and B_1, B_2, B_3 to be any distinct points (and thus not confined to being collinear), such that (1) is satisfied and so C_1, C_2, C_3 are well-defined.

When a_1, a_2, a_3 are not concurrent, we choose coordinates as before and the calculations above show that $\mathcal{E}_1$ has the equation (6). When a_1, a_2, a_3 are concurrent we take the triangle of reference so that these lines have the equations

$$y + z = 0,\ y = 0,\ z = 0,$$

respectively. With (4) as before, instead of (5) we find that

$$\begin{aligned}Q_1 &= ((b+c)x - ay - az, cy - bz, -cy + bz),\\ Q_2 &= (ex - dy, 0, ez - fy),\\ Q_3 &= (kx - gz, ky - hz, 0).\end{aligned}$$

Then these points are collinear if and only if

$$\det\begin{pmatrix}(b+c)x - ay - az & cy - bz & -cy + bz\\ ex - dy & 0 & ez - fy\\ kx - gz & ky - hz & 0\end{pmatrix} = 0,$$

which expands to

$$\begin{aligned}&k(cd - af)y^3 + e(bg - ah)z^3 + e(ch - bk)z^2x\\ &+ \{a[ek + f(h-k)] - bdk + c(fg - dh)\}y^2z\\ &- \{a[e(h-k) - fh] + b(fg - dh) + ceg\}yz^2\\ &+ k(bf - ce)xy^2 - [bf(h-k) + ch(f-e)]xyz = 0. \qquad (9)\end{aligned}$$

Thus $\mathcal{E}_1$ has this as equation.

Checking the cases in which $\mathcal{E}_1$ degenerates to the whole plane is rather detailed. It is convenient to denote by capital letters the cofactors of the elements in Δ. When a_1, a_2, a_3 are non-concurrent, by (6) degeneracy occurs only if all of

$$\begin{aligned}&aB = 0, aC = 0, eF = 0, eD = 0, kG = 0, kH = 0,\\ &aA + eE + kK - \Delta = 0, \qquad (10)\end{aligned}$$

hold. We divide into the cases

(i) all three of a, e, k are equal to 0;

(ii) exactly two of a, e, k are equal to 0, and by symmetry we can take $e = k = 0, a \neq 0$;

(iii) exactly one of a, e, k is equal to 0, and we can take $a = 0, e \neq 0, k \neq 0$;

(iv) none of a, e, k is equal to 0.

In (i), as $a = 0$, we have $B_1 \in A_2A_3$ and similarly $B_2 \in A_3A_1$, $B_3 \in A_1A_2$. As $\Delta = 0$, B_1, B_2 and B_3 are collinear. In this case $\mathcal{E}_1$ degenerates. In (ii), as $e = k = 0$, we have $B_2 \in A_3A_1$, $B_3 \in A_1A_2$. As $B = C = 0$ we have $A_2 \in B_2B_3$, $A_3 \in B_2B_3$. Thus $B_2 = A_3, B_3 = A_2$, which is incompatible with (1). Similarly we find that (iii) and (iv) are incompatible with (1).

Similarly when a_1, a_2, a_3 are concurrent, by (9) $\mathcal{E}_1$ can degenerate to being the whole plane only when

$$\begin{aligned}&eD = 0, eF = 0, kG = 0, kH = 0, fD + hG = 0,\\ &-fE - hH + kK = 0, -eE + fF + hK = 0. \qquad (11)\end{aligned}$$

Now $C_1 = C_2 = C_3 = A_1$ and (1) implies that none of the triples

$$\{A_1, B_2, B_3\}, \{A_1, B_3, B_1\}, \{A_1, B_1, B_2\} \text{ is collinear.} \qquad (12)$$

We divide into the cases

(v) $e = k = 0$;

(vi) $e = 0, k \neq 0$;

(vii) $e \neq 0, k \neq 0$.

In (v), as $e = k = 0$, we have $B_2 \in a_2$, $B_3 \in a_3$ and so

$$fD + hG = 0,\ fE + hH = 0,\ fF + hK = 0.$$

If we had $f = g = 0$, then we would have $B_2 \in a_3$, $B_3 \in a_2$ and so

$$B_2 = B_3 = A_1,$$

which is ruled out as $B_2 \neq B_3$. We then have $(f, h) \neq (0, 0)$ and so

$$DH - GE = 0,\ EK - FH = 0,\ FG - DK = 0,$$

that is $c\Delta = a\Delta = b\Delta = 0$. Now $\Delta \neq 0$ would imply that $(a, b, c) = (0, 0, 0)$, which is impossible as these are homogeneous coordinates for B_1. Thus $\Delta = 0$, and so B_1, B_2, B_3 are collinear. Here $Q_2 = B_2$, $Q_3 = B_3$ and so we need $Q_1 \in B_2B_3$; this makes $Q_1 = B_1$ and so $B_1 \in a_1$. In this case $\mathcal{E}_1$ degenerates. In (vi) $e = 0$ implies $B_2 \in a_2$, and $k \neq 0$ implies $G = 0$ and $A_1 \in B_1B_2$.

These conflict with (12). Similarly (vii) conflicts with (12). These combined cases establish Theorem 3.

By considering the dual of Theorem 3, it can be deduced that the set $\mathcal{E}_2$ of lines p that are a line of collinearity $Q_1Q_2Q_3$ in Theorem 3, is either a line cubic or the set of all lines in the plane. If a_1, a_2, a_3 are concurrent, then the lines on A_1 form part of $\mathcal{E}_2$, and in the non-degenerate case $\mathcal{E}_2$ consists of a line conic and the lines on one of its Brianchon points.

It is evident that we do not obtain all cubics in Theorem 3, as $\mathcal{E}_1$ there is determined by the six points A_1, A_2, A_3, B_1, B_2 and B_3. Nonetheless, it yields a large class of cubics with a geometrical property. This class is closed under projective transformations.

An example

The equation (6) does not suit taking $z = 1$ to obtain Cartesian coordinates, as A_1 and A_2 would be points at infinity. Because of this we introduce Cartesian coordinates (X, Y) for P by applying the transformation

$$x = 1 - X - Y,\ y = X,\ z = Y.$$

In this way A_1, A_2, A_3 have Cartesian coordinates (0,0), (1,0), (0,1), respectively. Taking for an example, B_1, B_2, B_3 to have Cartesian coordinates (3,1), (3,2), (2,2), respectively, we have

$$B_1 = (-3, 3, 1),\ B_2 = (-4, 3, 2),\ B_3 = (-3, 2, 2).$$

Then we find that (6) becomes

$$2X^3 - 8X^2 - 2X(Y^2 - Y - 3) - 3Y(Y - 1)(Y - 4) = 0.$$

The graph of this is shown in Figure 2.

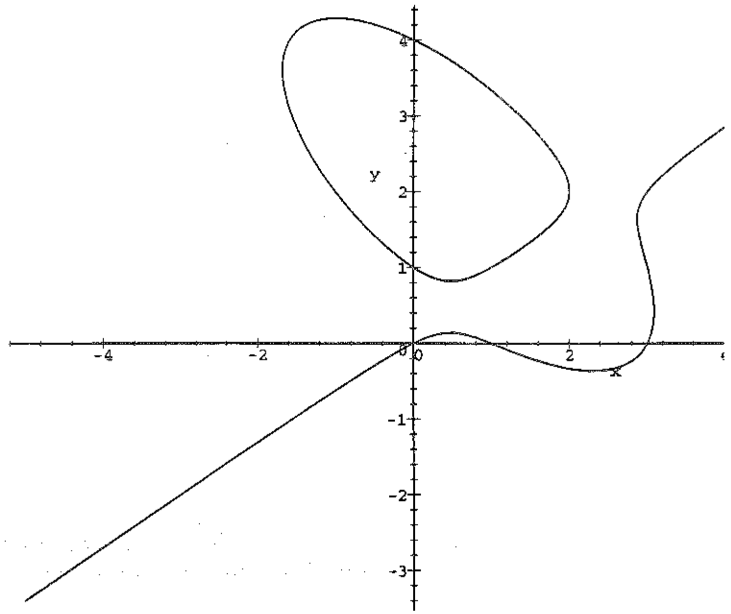


Figure 2

References

[1] E. A. Maxwell, The Methods of Plane Coordinate Geometry based on the Use of General Homogeneous Coordinates. Cambridge University Press: Cambridge, 1946

P. D. Barry
Department of Mathematics,
University College,
Cork.

STOKES PARAMETERS AND GIBBS BIVECTORS

Michael Hayes

Abstract For a single monochromatic wave train, it is shown that the use of Gibbs bivectors leads in a natural and economical way to the introduction of Stokes parameters.

Introduction

Stokes, in a study of light waves published [1] in 1852, introduced what are now called 'Stokes parameters.' These are functions only of the electromagnetic wave. The polarization state of a beam of light (either natural, totally or partially polarized) can be described in terms of these four parameters [2, 3]. The purpose of this note is to show how the use of Gibbs bivectors [4, 5] leads to a direct and economical way of introducing Stokes parameters.

First, a simple observation. Any vector $\mathbf{a}$ (say) lying in a plane may be represented in an infinity of ways as a linear combination of two arbitrary vectors, $\mathbf{b}$ and $\mathbf{c}$ (say), in the plane, provided of course that $\mathbf{b}$ and $\mathbf{c}$ are not parallel. Thus $\mathbf{a} = \beta\mathbf{b} + \gamma\mathbf{c}$, for some scalars β and γ. Provided the vectors $\mathbf{b}$ and $\mathbf{c}$ are chosen to be orthogonal, then the squared length of $\mathbf{a}$, namely $a^2 = \mathbf{a}\cdot\mathbf{a}$, may be written simply as $a^2 = \beta^2 b^2 + \gamma^2 c^2$.

It is the generalization of this simple observation to the case of complex vectors, or bivectors, which leads naturally to Stokes parameters.

Here, Gibbs bivectors are introduced and some of their properties presented. Then a single monochromatic train of elliptically polarized plane transverse waves is considered.

Background

In 1853, the year following the publication of Stokes' paper [1], Hamilton, [6], in the context of quaternions, coined the word "bivector" for the combination $\mathbf{a}+i\mathbf{b}$, where $\mathbf{a}$ and $\mathbf{b}$ are real vectors. Complex numbers $\alpha+i\beta$ had been called biscalars! Hamilton seems not to have ever used bivectors. The theory was developed by Gibbs, [4], in 1881, 1884. He presented seven pages on bivectors in his seventy page pamphlet "Elements of Vector Analysis," which laid the modern foundations of vector algebra. Gibbs printed and circulated this privately. The work on bivectors was generally ignored, possibly because in parts it is difficult to read. The phrase "too condensed and too difficult" which was used by Lord Rayleigh, [7, page xiv], in writing to Gibbs about his famous paper "Equilibrium of Heterogeneous Substances" is apposite here also.

Gibbs recognized that an ellipse could be associated with a bivector. He naturally used bivectors in the description of elliptically polarized electromagnetic waves. It is here that the connection with Stokes parameters is made.

Bivectors

A pair of orthogonal radii to a circle are said to be 'conjugate.' If the circle is drawn on a sheet of rubber which is then stretched uniformly, the circle becomes an ellipse and pairs of conjugate radii of the circle become conjugate radii to the ellipse. The property that the tangent to the circle at the tip of the radius is parallel to the conjugate carries over to the ellipse. If $\mathbf{i}$ and $\mathbf{j}$ are parallel unit vectors then the position vector $\mathbf{r}$ given by

$$\mathbf{r} = a(\mathbf{i}\cos\theta + \mathbf{j}\sin\theta)$$

describes a circle of radius a. Also, if $\mathbf{a}$ and $\mathbf{b}$ is any pair of non-parallel vectors, then

$$\mathbf{r} = \mathbf{a}\cos\theta + \mathbf{b}\sin\theta$$

describes an ellipse in which $\mathbf{a}$ and $\mathbf{b}$ are conjugate radii. The tangent $d\mathbf{r}/d\theta$ at $\theta = 0$ $(\pi/2)$ is parallel to $\mathbf{a}$ $(\mathbf{b})$. The pair $\mathbf{r}(\theta)$ and $\mathbf{r}(\theta+\pi/2)$ are conjugate, [5].

The combination $\mathbf{D} = \mathbf{a} + i\mathbf{b}$ is said to be a bivector. Throughout capital bold face letters $\mathbf{D}$, $\mathbf{E}$, $\ldots$, are used to denote bivectors. The real and imaginary parts of the bivector $\mathbf{D}$ are denoted by $(\mathbf{D})^+$ and $(\mathbf{D})^-$, respectively. Associated with $\mathbf{D}$ is a unique ellipse, $\mathbf{r} = \mathbf{a}\cos\theta + \mathbf{b}\sin\theta$, $(0 \leq \theta \leq 2\pi)$ and a sense of description, from $(\mathbf{D})^+ = \mathbf{a}$ to $(\mathbf{D})^- = \mathbf{b}$. The complex conjugate of $\mathbf{D}$ is $\bar{\mathbf{D}} = \mathbf{a} - i\mathbf{b}$. The bivectors $\mathbf{D}$ and $\bar{\mathbf{D}}$ have the same ellipse associated with them, but in the case of $\bar{\mathbf{D}}$ the sense of description is from $(\bar{\mathbf{D}})^+ = \mathbf{a}$ to $(\bar{\mathbf{D}})^- = -\mathbf{b}$, which is opposite to that of the ellipse of $\mathbf{D}$.

Two bivectors $\mathbf{D}$ and $\mathbf{E}$ are said to be **parallel** if there exists a scalar, λ, such that $\mathbf{D} = \lambda\mathbf{E}$. Otherwise they are linearly independent.

The dot product of the bivectors $\mathbf{D} = \mathbf{a} + i\mathbf{b}$ and $\mathbf{E} = \mathbf{p} + i\mathbf{q}$ is defined in the usual way:

$$\mathbf{D}\cdot\mathbf{E} = \mathbf{a}\cdot\mathbf{p} - \mathbf{b}\cdot\mathbf{q} + i(\mathbf{b}\cdot\mathbf{p} + \mathbf{a}\cdot\mathbf{q}).$$

If $\mathbf{D}\cdot\mathbf{E} = 0$, then $\mathbf{D}$ and $\mathbf{E}$ are said to be **orthogonal**.

If $\mathbf{D}\cdot\mathbf{D} = 0$, then $\mathbf{a}\cdot\mathbf{a} = \mathbf{b}\cdot\mathbf{b}$, $\mathbf{a}\cdot\mathbf{b} = 0$ so that in this case the ellipse of $\mathbf{D}$ is a circle. For example, if $\mathbf{D} = \mathbf{i} + i\mathbf{j}$, then $\mathbf{D}\cdot\mathbf{D} = 0$.

The "intensity" of $\mathbf{D}$ is defined to be $\mathbf{D}\cdot\bar{\mathbf{D}}$. A bivector $\mathbf{D}$ of unit intensity may be represented by

$$\mathbf{D} = \cos\beta\,\mathbf{r} + i\sin\beta\,\mathbf{s}, \tag{1}$$

where $\mathbf{r}$, $\mathbf{s}$ are orthogonal unit vectors along the principal axes of the ellipse of $\mathbf{D}$.

If the bivector $\mathbf{H}$ is defined by $\mathbf{H} = e^{i\phi}\mathbf{D}$ with $\mathbf{D} = \mathbf{a} + i\mathbf{b}$, then

$$\mathbf{H} = (\cos\phi\,\mathbf{a} - \sin\phi\,\mathbf{b}) + i(\sin\phi\,\mathbf{a} + \cos\phi\,\mathbf{b}), \tag{2}$$

so that the ellipse associated with $\mathbf{H}$ is

$$\begin{aligned}\mathbf{r} &= (\cos\phi\,\mathbf{a} - \sin\phi\,\mathbf{b})\cos\theta + (\sin\phi\,\mathbf{a} + \cos\phi\,\mathbf{b})\sin\theta \\ &= \mathbf{a}\cos(\theta - \phi) + \mathbf{b}\sin(\theta - \phi).\end{aligned} \tag{3}$$

This is precisely the ellipse associated with $\mathbf{D}$. Note that here ϕ is a given quantity and θ is a variable. This result is due to MacCullagh, [8], who set its equivalent as an examination question in Trinity College in 1847.

MacCullagh's theorem, described by Hamilton as "a remarkable use of the symbol i," is central to the use of bivectors in the description of wave propagation.

MacCullagh's theorem means that beginning with the pair $(\mathbf{a}, \mathbf{b})$ which defines an ellipse, then $e^{i\phi}(\mathbf{a} + i\mathbf{b})$ gives another pair of conjugate radii of the same ellipse. Now taking $\phi = \omega t$ where ω is a real constant and t denotes time, $e^{i\omega t}(\mathbf{a} + i\mathbf{b})$ gives at any time t a pair of conjugate radii of the ellipse. The tip of the real vector $\cos\omega t\,\mathbf{a} - \sin\omega t\,\mathbf{b}$ moves on the ellipse. Its period of oscillation is $2\pi/\omega$. The pair $(\mathbf{a}, \mathbf{b})$ is rotated, but not rigidly, into another pair of conjugate radii.

Let two bivectors $\mathbf{D}$ and $\mathbf{E}$ be coplanar and orthogonal: $\mathbf{D}\cdot\mathbf{E} = 0$. Now $\mathbf{D}$ may be written

$$\mathbf{D} = e^{i\phi}(\mathbf{a} + i\mathbf{b}) = e^{i\phi}(a\mathbf{i} + ib\mathbf{j}),$$

where $\mathbf{a}$ and $\mathbf{b}$ are along the principal semi-axes of the ellipse of $\mathbf{D}$ and $\mathbf{i}$, $\mathbf{j}$ are unit vectors. Because $\mathbf{E}$ is coplanar with $\mathbf{D}$, it may be written $\mathbf{D} = \alpha\mathbf{i} + \beta\mathbf{j}$ for some scalars α, β. Then $\mathbf{D}\cdot\mathbf{E} = 0$ gives $\alpha a + i\beta b = 0$ so that $\mathbf{E} = \lambda(a\mathbf{j} - ib\mathbf{i})$ for some λ. Hence the major and minor axes of the ellipse of $\mathbf{E}$ are respectively along the minor and major axes of the ellipse of $\mathbf{D}$. Also the ellipses of $\mathbf{E}$ and $\mathbf{D}$ are similar – they have the same aspect ratio (a/b) and they are described in the same sense. Hence Gibbs' result [4] follows: if $\mathbf{D}\cdot\mathbf{E} = 0$ with $\mathbf{D}$ and $\mathbf{E}$ coplanar, the ellipse of $\mathbf{E}$ is similar and similarly situated to the ellipse of $\mathbf{D}$ rotated through a quadrant in its plane. Both ellipses are described in the same sense. (See also [5].)

If two coplanar bivectors $\mathbf{D}$ and $\mathbf{E}$ are such that $\mathbf{D}\cdot\bar{\mathbf{E}} = 0$, then the ellipse of $\mathbf{E}$ is similar and similarly situated to the ellipse of $\mathbf{D}$ when rotated through a quadrant. However the ellipses are described in opposite senses. Then $\mathbf{D}$ and $\mathbf{E}$ are said to be **oppositely polarized**. For example, $\mathbf{D}$ and $\mathbf{E}$ given by

$$\mathbf{D} = \mathbf{i} + i\mathbf{j}, \quad \mathbf{E} = \mathbf{i} - i\mathbf{j}$$

and by

$$\mathbf{D} = \mathbf{i} + im\mathbf{j}, \quad \mathbf{E} = m\mathbf{i} - i\mathbf{j},$$

where $m = \bar{m}$, are oppositely polarized.

Waves

Using rectangular Cartesian coordinate axes $Oxyz$, with the z-axis along the propagation direction, plane transverse homogeneous waves are described by a vector field $\mathbf{u}(z,t)$ of the form

$$\mathbf{u}(z,t) = \{\mathbf{A}e^{i\tau}\}^{+}, \quad \tau = \kappa z - \omega t. \tag{4}$$

Here $\mathbf{A}$ is called the "amplitude bivector" and is constant. It lies in the x-y plane:

$$\mathbf{A} = A_1\mathbf{i} + A_2\mathbf{j}. \tag{5}$$

Also κ and ω are real constants.

In general, (4) describes an infinite train of homogeneous waves, propagating in the z-direction, elliptically polarized in the x-y plane. Its period is $2\pi/(\omega)$ and its wavelength is $2\pi/(\kappa)$.

The intensity I of the wave is defined by

$$I = \mathbf{A}\cdot\bar{\mathbf{A}} = A_1\bar{A}_1 + A_2\bar{A}_2. \tag{6}$$

Writing the complex numbers A_1, A_2 in terms of their moduli and arguments,

$$A_1 = a_1 e^{i\delta_1}, \quad A_2 = a_2 e^{i\delta_2}, \tag{7}$$

then

$$\mathbf{A} = \mathbf{c} + i\mathbf{d}, \quad \mathbf{c} = a_1\cos\delta_1\mathbf{i} + a_2\cos\delta_2\mathbf{j}, \quad \mathbf{d} = a_1\sin\delta_1\mathbf{i} + a_2\sin\delta_2\mathbf{j}. \tag{8}$$

The components u_1 and u_2 of the vector field $\mathbf{u}(z,t)$ along the x and y axes, respectively, are given by

$$u_1 = a_1\cos(\tau + \delta_1), \quad u_2 = a_2\cos(\tau + \delta_2). \tag{9}$$

The polarization ellipse is contained within a rectangular box whose sides are parallel to the x and y axes, and have lengths $2a_1$ and $2a_2$, respectively. The amplitudes a_1 and a_2, and the phase difference $\delta = \delta_1 - \delta_2$ of the orthogonal field components (9) may be obtained from observations. The polarization ellipse may be constructed if a_1, a_2, δ are known, [3, 5].

Stokes Parameters

Following Stokes, [1], consider the possibility of resolving the given wave (4) into two given elliptically polarized waves of the same period and wavelength. This amounts to asking whether it is possible to decompose $\mathbf{A}$ in the form

$$\mathbf{A} = \lambda\mathbf{C} + \mu\mathbf{D}, \tag{10}$$

where $\mathbf{C}$ and $\mathbf{D}$ are any two given bivectors coplanar with $\mathbf{A}$ such that $\mathbf{C}\cdot\bar{\mathbf{C}} = \mathbf{D}\cdot\bar{\mathbf{D}} = 1$ and λ, μ are to be determined. Now choosing $\mathbf{C}^{\star}$ and $\mathbf{D}^{\star}$ so that $\mathbf{C}\cdot\mathbf{C}^{\star} = \mathbf{D}\cdot\mathbf{D}^{\star} = 0$, it follows that

$$\lambda\mathbf{C}\cdot\mathbf{D}^{\star} = \mathbf{A}\cdot\mathbf{D}^{\star}, \quad \mu\mathbf{D}\cdot\mathbf{C}^{\star} = \mathbf{A}\cdot\mathbf{C}^{\star}. \tag{11}$$

Hence λ, μ do not exist if $\mathbf{C}\cdot\mathbf{D}^{\star} = 0$, or equivalently in this case $\mathbf{D}\cdot\mathbf{C}^{\star} = 0$. This means that the bivectors $\mathbf{C}$ and $\mathbf{D}$ are parallel: $\mathbf{D} = \gamma\mathbf{C}$ for some γ. Indeed, suppose, without loss, that

$$\mathbf{C} = (\mathbf{i} + im\mathbf{j})/(1+m^2)^{\frac{1}{2}}, \quad \mathbf{D} = (p\mathbf{i} + q\mathbf{j})/(p\bar{p} + q\bar{q})^{\frac{1}{2}}, \tag{12}$$

with $m = \bar{m}$, so that

$$\mathbf{C}^{\star} = (m\mathbf{i} + i\mathbf{j})/(1+m^2)^{\frac{1}{2}}, \quad \mathbf{D}^{\star} = (q\mathbf{i} - p\mathbf{j})/(p\bar{p} + q\bar{q})^{\frac{1}{2}}. \tag{13}$$

Then $\mathbf{C}\cdot\mathbf{D}^{\star} = 0$ leads to $q = ipm$, which leads to $\mathbf{C}^{\star}\cdot\mathbf{D} = 0$ and $\mathbf{D} = \{p/(p\bar{p})^{\frac{1}{2}}\}\mathbf{C}$.

If $\mathbf{C}$ and $\mathbf{D}$ are not parallel, then λ, μ are determined and using $\mathbf{C}\cdot\bar{\mathbf{C}} = \mathbf{D}\cdot\bar{\mathbf{D}} = 1$, it follows that

$$I = \mathbf{A}\cdot\bar{\mathbf{A}} = \lambda\bar{\lambda} + \mu\bar{\mu} + \lambda\bar{\mu}\mathbf{C}\cdot\bar{\mathbf{D}} + \bar{\lambda}\mu\bar{\mathbf{C}}\cdot\mathbf{D}. \tag{14}$$

Now choose $\mathbf{C}$ and $\mathbf{D}$ so that their ellipses are oppositely polarized: $\mathbf{C}\cdot\bar{\mathbf{D}} = 0$. Then

$$I = \lambda\bar{\lambda} + \mu\bar{\mu}, \tag{15}$$

which is just the sum of the intensities of the component waves.

In the Introduction it was noted that the real vectors $\mathbf{b}$ and $\mathbf{c}$ were chosen to be orthogonal. Here the bivectors $\mathbf{C}$ and $\mathbf{D}$ are chosen so that $\mathbf{C}\cdot\bar{\mathbf{D}} = 0$–the ellipse of $\mathbf{C}$ is similar and similarly situated to that of $\mathbf{D}$ when rotated through a quadrant, but the ellipses of $\mathbf{C}$ and $\mathbf{D}$ are described in opposite senses.

Now if $\mathbf{r}$ and $\mathbf{s}$ are unit vectors along the major and minor axes, respectively, of the ellipse of $\mathbf{C}$, then $\mathbf{C}$ and $\mathbf{D}$ may be written

$$\mathbf{C} = \cos\beta'\mathbf{r} + i\sin\beta'\mathbf{s}\ ,\ \ \mathbf{D} = \sin\beta'\mathbf{r} - i\cos\beta'\mathbf{s}. \qquad (16)$$

Let χ' be the azimuth of the major axis of the ellipse of $\mathbf{C}$ with respect to the x-axis. Then $\cos\chi' = \mathbf{r}\cdot\mathbf{i} = \mathbf{s}\cdot\mathbf{j}$.

Using (10) and $\mathbf{C}\cdot\bar{\mathbf{D}} = 0$, it follows that

$$\lambda\bar{\lambda} = (\mathbf{A}\cdot\bar{\mathbf{C}})(\bar{\mathbf{A}}\cdot\mathbf{C}), \qquad (17)$$

where

$$\mathbf{A}\cdot\bar{\mathbf{C}} = (A_1\mathbf{i} + A_2\mathbf{j})\cdot(\cos\beta'\mathbf{r} - i\sin\beta'\mathbf{s}).$$

Hence

$$2\lambda\bar{\lambda} = I + Q\cos 2\beta'\cos 2\chi' + U\cos 2\beta'\sin 2\chi' + V\sin 2\beta' \ (18)$$

and similarly

$$2\mu\bar{\mu} = I - Q\cos 2\beta'\cos 2\chi' - U\cos 2\beta'\sin 2\chi' - U\sin 2\beta', (19)$$

where

$$\begin{aligned} I &= A_1\bar{A}_1 + A_2\bar{A}_2, & Q &= A_1\bar{A}_1 - A_2\bar{A}_2, \\ U &= A_1\bar{A}_2 + \bar{A}_1A_2, & V &= i(A_1\bar{A}_2 - \bar{A}_1A_2). \end{aligned} \qquad (20)$$

The four quantities I, Q, U, V involve only the components A_1, A_2 of $\mathbf{A}$. They are the Stokes parameters. They all have the same dimensions and are such that

$$I^2 = Q^2 + U^2 + V^2. \qquad (21)$$

For every decomposition of the wave with amplitude bivector $\mathbf{A}$ into two oppositely polarized waves, the intensities of the two component waves are given as linear combinations of the four Stokes parameters. There is an infinity of such decompositions–a particular decomposition corresponds to a choice of the polarization form of the bivector $\mathbf{C}$, that is, to a choice of the angles β' and χ'.

If β' and χ' are altered to β'' and χ'' (say), then λ and μ are altered to λ'' and μ'' (say). The intensities $\lambda''\bar{\lambda}''$ and $\mu''\bar{\mu}''$ of the two oppositely polarized waves are given by (18) and (19) respectively, with β', χ' replaced by β'', χ'', **but the coefficients I, Q, U, V remain unchanged.**

If $\tan\beta$ is the aspect ratio of the ellipse of $\mathbf{A}$ and χ is its azimuth, it may be shown, [2, 3, 5], that

$$\begin{aligned} I &= \mathbf{A}\cdot\bar{\mathbf{A}}, & Q &= I\cos 2\beta\cos 2\chi, \\ V &= I\sin 2\beta, & U &= \cos 2\beta\sin 2\chi. \end{aligned}$$

This and (21) immediately suggest representation on a sphere–the Poincaré sphere. But that is another story.

References

[1] G. G. Stokes, *On the composition and resolution of streams of polarized light from different sources.* Trans. Cambridge Phil. Soc. **9** (1852), 399-416.

[2] R. M. A. Azzam and N. M. Bashara, Ellipsometry and Polarised Light. North-Holland: Amsterdam (1977).

[3] M. Born and E. Wolf, Principles of Optics (sixth edition). Pergamon: Oxford (1980).

[4] J. W. Gibbs, Elements of Vector Analysis. Privately printed (1881, 1884). (Published in Scientific Papers, Vol. 2, pp. 17-90. Dover: New York (1961).)

[5] Ph. Boulanger and M. Hayes, Bivectors and Waves in Mechanics and Optics. Chapman and Hall: London (1993).

[6] W. R. Hamilton, Lectures on Quaternions. Hodges and Smith: Dublin (1853).

[7] R. J. Strutt (Fourth Baron Rayleigh), Life of John William Strutt, Third Baron Rayleigh. The University of Wisconsin Press: Madison (1968).

[8] J. MacCullagh, *On total reflexion*, Proc. Royal Irish Acad. **3** (1847), 49-51.

Acknowledgement I am very grateful to T. J. Laffey for his comments.

M. Hayes,
Mathematical Physics Department,
University College,
Belfield,
Dublin 4.

WRITING COMMUTATORS OF GROUP COMMUTATORS AS PRODUCTS OF CUBES

Peter V. Hegarty

Abstract We derive an upper bound for the number of cubes needed to write a commutator of group commutators as a product of cubes.

1. Introduction

If a and b are elements of a group G, we define their commutator $[a,b]$ to be the group element $a^{-1}b^{-1}ab$. It is well known that groups of exponent 3 are metabelian–for a proof see [2], pp. 382-3. Consequently, in the free group F_4 on four generators x, y, z and w, the "commutator of commutators" $[[x,y],[z,w]]$ can be expressed as a product of cubes of elements of F_4. In the survey article [1], R. Lyndon poses the problem of finding such an expression which contains the smallest possible number of cubes. At this point it is instructive to recall, by way of analogy, the simple and well known fact that, in the free group F_2 on two generators x and y, the commutator $[x,y]$ can be written as a product of 3 squares, but of no fewer:

$$[x,y]=(x^{-1})^2(xy^{-1})^2y^2.$$

Lyndon's problem, by contrast, seems to be more difficult. In this note, I will show that $[[x,y],[z,w]]$ can be expressed as a product of 85 cubes. This will, I hope, provide a benchmark for future progress on the problem. Following my proof, one could write down an explicit expression, but in the interests of saving space I shall not do so here.

2. Notation

From now on, all work takes place in the free group F_4 on the four generators x, y, z, w. To simplify the presentation of the proof to follow, let me introduce some unorthodox notation. The symbol π_n will be used to denote a generic product of n cubes of elements of F_4. It is important to understand that π_n does not denote a group element, but rather a type of group element. Hence, for example, given $a \in F_4$ we will write the equation

$$a = \pi_n \tag{1}$$

to denote the fact that a can be expressed as a product of some (unspecified) n cubes of elements of F_4. Next, for a and b in F_4, the equation

$$a = b\pi_n \tag{2}$$

will be written instead of $b^{-1}a = \pi_n$. An elementary but important fact is that, for any $a \in F_4$ and any n, we have

$$a\pi_n = \pi_n a \tag{3}$$

or, in words, right-multiplying a by a product of n cubes is the same as left-multiplying a by some other product of n cubes. The verification of this fact is trivial. More generally, for $a_1, \ldots a_k$ in F_4 and positive integers $n_1, \ldots, n_k$ we have

$$\begin{aligned} a_1\pi_{n_1}a_2\pi_{n_2}...a_k\pi_{n_k} &= a_1a_2...a_k\pi_{n_1+n_2+...+n_k} \\ &= \pi_{n_1+n_2+...+n_k}a_1a_2...a_k. \end{aligned} \tag{4}$$

3. Main Result

We begin with a lemma.

Lemma. *For a and b in F_4, the following hold:*

(i) $[a,b] = [b^{-1},a]\,\pi_3$;
(ii) $[a,b] = [b,a^{-1}]\,\pi_3$;
(iii) $[a,b] = [a^{-1},b^{-1}]\pi_3$.

Proof: For (i), we have

$$\begin{aligned} [a,b^{-1}][a,b] &= a^{-1}ba(b^{-1}a^{-1}b^{-1})ab \\ &= a^{-1}ba(b^{-1}a^{-1})^3aba^2b \\ &= a^{-1}(ba^2)^2b\,\pi_1 \\ &= a^{-1}(ba^2)^3a^{-2}\,\pi_1 = \pi_3, \end{aligned}$$

as required. Part (ii) follows from (i) simply by inverting both sides and interchanging the symbols a and b.

For (iii), we have

$$\begin{aligned} [a,b] &= a^{-1}b^{-1}ab = a^{-1}(b^{-1}a)^3a^{-1}ba^{-1}b^2 \\ &= \pi_1(a^{-2}ba^{-1}b^2) = \pi_1(aa^{-3}ba^{-1}b^{-1}b^3) \\ &= \pi_3(aba^{-1}b^{-1}) = \pi_3\,[a^{-1},b^{-1}], \end{aligned}$$

as required.

The rest of the paper is devoted to proving the following result.

Theorem. *In $F_4 = \langle x,y,z,w\rangle$ we have that $[[x,y],[z,w]] = \pi_{85}$.*

Proof: Our strategy is to adapt the proof in [1], pp 382-3, which the reader may profitably consult, that groups of exponent 3 are metabelian. So let us begin.

For a, b and d in F_4 we have

$$\begin{aligned} d^{-1}b^{-1}a^{-1}b^{-1}ada^{-1}d &= d^{-1}(b^{-1}a^{-1})^2a^3(a^{-1}d)^2 \\ &= (d^{-1}abd^{-1}a)\pi_3 \\ &= (d^{-1}ab)^3b^{-1}a^{-1}db^{-1}\pi_3 \\ &= (b^{-1}a^{-1}db^{-1})\pi_4. \end{aligned}$$

So, by equating the first and last terms we get

$$a^{-1}b^{-1}ada^{-1} = (bdb^{-1}a^{-1}db^{-1}d^{-1})\pi_4 \tag{5}$$

Now substitute bcb^{-1} for d in (5) and derive easily that

$$\begin{aligned} c^{-1}a^{-1}b^{-1}abcb^{-1}a^{-1}ba &= (c^{-1}b^2cb^{-2}a^{-1}bcb^{-1}c^{-1}a)\pi_4 \\ &= (c^{-1}b^{-1}cba^{-1}bcb^{-1}c^{-1}a)\pi_6 \end{aligned} \tag{6}$$

Using part (iii) of the lemma, we can obtain from (6) that

$$[c,[b,a]] = [[b,c],a]\pi_9 \tag{7}$$

Now set $u = [[x,y],[z,w]]$ and $g = [z,w]$. Then

$$\begin{aligned} u = [[x,y],g] &= [y,[x,g]]\pi_9 \text{ by (7)} \\ &= [y,[x,[z,w]]]\pi_9 \\ &= [y,[[z,x],w]]\pi_9]\pi_9 \text{ by (7)} \\ &= [y,[[z,x],w]]\pi_{27} \\ &= [y,[w,[x,z]]\pi_3]\pi_{27} \text{ by part (ii) of the lemma} \\ &= [y,[w,[x,z]]]\pi_{33} \\ &= [[w,y],[x,z]]\pi_{42} \text{ by (7) again.} \end{aligned}$$

Equating the first and last terms, we have

$$[[x,y],[z,w]] = [[w,y],[x,z]]\pi_{42} \tag{8}$$

Similarly,

$$\begin{aligned} u = [[x,y],g] &= [g,[y,x]]\pi_3 \text{ by part (ii) of the lemma} \\ &= [[y,g],x]\pi_{12} \text{ by (7)} \\ &= [[y,[z,w]],x]\pi_{12} \\ &= [[[z,y],w]\pi_9,x]\pi_{12} \text{ by (7)} \\ &= [[[z,y],w],x]\pi_{30} \\ &= [x,[w,[z,y]]]\pi_{33} \text{ by part (ii) of the lemma} \\ &= [[w,x],[z,y]]\pi_{42} \text{ by (7) again.} \end{aligned}$$

Equating the first and the last terms, we have

$$[[x,y],[z,w]] = [[w,x],[z,y]]\pi_{42} \tag{9}$$

Combining (8) and (9) we obtain easily that

$$u = u^{-1}\pi_{84} \Rightarrow u^2 = \pi_{84} = u^3u^{-1} \Rightarrow u = \pi_{85},$$

which completes the proof of the theorem.

Remark Let me elucidate the idea of the proof above. Equation (8) says, informally, that the permutation $x \to w \to z$ of the symbols x, y, z, w in the commutator u corresponds to multiplication of u by some 42 cubes. Equation (9) says the same for the permutation $x \to w \to y$. The product of these permutations is '$x \leftrightarrow z$, $y \leftrightarrow w$', which takes u to u^{-1}. Now, though I have not checked it, I would conjecture that any 3-cyclic permutation of x, y, z, w corresponds to multiplication of u by some 42 cubes. An obvious question to ask is whether 42 is best possible. And one may ask the same question for other types of permutations, in particular for transpositions. In this way, it may be possible to improve on the number 85 in our theorem simply by pure luck and without introducing any essentially new ideas. It seems an entirely more complicated matter, however, to obtain optimal results.

Acknowledgement I wish to thank Professor Desmond MacHale of University College, Cork, for pointing out this problem to me, and for some helpful suggestions regarding the preparation of the manuscript.

References

[1] R. C. Lyndon, *Equations in groups*, Bol. Soc. Bras. Mat. **11** (1980), 79-102.

[2] W. Magnus, A. Karrass and D. Solitar, Combinatorial Group Theory. Interscience Publishers: New York, 1966.

P. V. Hegarty
Department of Mathematics,
Princeton University,
Princeton, NJ 08544,
USA.

COMMUTATORS IN RINGS

T. Creedon

Abstract We exhibit with proof a ring of minimal order in which the commutator subset is not a subring.

Introduction

It is well known that the product of two commutators in a group need not be a commutator. However the smallest order of a group in which this occurs is 96. We produce an example of a ring of order 16 in which the subset of all commutators is not a subring. We prove that this example is minimal by showing that in all rings of order less than 16 the subset of all commutators is an ideal and therefore also a subring. Throughout this paper $\mathbf{Z}_2$ denotes the field of integers modulo 2, C_p denotes the cyclic group of order p and $\langle a \rangle$ denotes the additive group generated by an element a. The commutator of two elements a and b in a ring is denoted $[a, b] = ab - ba$. A presentation for a finite ring R consists of a set of generators $g_1, \ldots, g_k$ of the additive group of R together with relations which specify the additive order of the generators and the multiplication with which R is endowed. For example $\langle a : 2a = 0, a^2 = a \rangle$ is a presentation for Z_2 and we write $\mathbf{Z}_2 = \langle a : 2a = 0, a^2 = a \rangle$.

Example

Consider the ring R of order 16 consisting of all 2×2 matrices with entries in $\mathbf{Z}_2$,

$$R = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where a, b, c and d run over the elements of $\mathbf{Z}_2$. By direct calculation, we find that the commutator subset C of R consists of the

following eight matrices

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

We remark that C is an additive subgroup of R. However, since

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \notin C,$$

we see that C is not closed under multiplication and so C is not a subring of R and hence not an ideal of R.

We now prove that for all rings of order less than 16, the commutator subset is an ideal. We do this by examining the structure of these rings. Note that any commutative ring has commutator subset $\{0\}$, which is an ideal. Since all abelian groups of orders 1, 2, 3, 5, 6, 7, 10, 11, 13, 14 and 15 are cyclic, the rings of these orders must be commutative and therefore in all these rings the commutator subset is an ideal. The rings of order p^2, where p is a prime number, have been classified (see [1], [2]). There are only two non-commutative rings of order p^2. These are rings with additive group $C_p \oplus C_p = \langle a \rangle \oplus \langle b \rangle$, where $pa = pb = 0$. When $p = 2$, the two rings are given by

$$R_1 = \langle a, b : 2a = 2b = 0, a^2 = a, b^2 = b, ab = a, ba = b \rangle$$

and

$$R_2 = \langle a, b : 2a = 2b = 0, a^2 = a, b^2 = b, ab = b, ba = a \rangle.$$

The commutator subset of R_1 is $\{0, a + b\}$ and this is an ideal of R_1. The commutator subset of R_2 is also $\{0, a + b\}$ and this is an ideal of R_2. When $p = 3$, the two rings are given by

$$R_3 = \langle a, b : 3a = 3b = 0, a^2 = a, b^2 = b, ab = a, ba = b \rangle$$

and

$$R_4 = \langle a, b : 3a = 3b = 0, a^2 = a, b^2 = b, ab = b, ba = a\rangle.$$

The commutator subset of R_3 is $\{0, a+2b, 2a+b\}$ and this is an ideal of R_3. The commutator subset of R_4 is also $\{0, a+2b, 2a+b\}$ and this is an ideal of R_4. Therefore in all rings of orders 4 and 9, the commutator subset is an ideal.

It is well known that any ring can be decomposed into a direct sum of rings of prime power order. Therefore the only non-commutative rings of order 12 are of the form $R_1 \oplus R_2$, where S_1 is a non-commutative ring of order 4 and S_2 is of order 3. Clearly S_2 is commutative and as we mentioned above there are only two non-commutative rings of order 4 and the commutator subset of each of these rings is an ideal. Hence the commutator subset of a ring of order 12 is an ideal.

The only remaining case to be considered is where the ring R has order 8. In this case R must have additive group C_8 (in which case R is commutative), $C_4 \oplus C_2$ or $C_2 \oplus C_2 \oplus C_2$.

Suppose first that R has additive group $C_4 \oplus C_2 = \langle a\rangle \oplus \langle b\rangle$, where $4a = 2b = 0$. Since $2b = 0$, we see that $2[a,b] = 0$ and the commutator subset of R is $C = \{0, [a,b]\}$. Therefore C is an additive subgroup of R. Every element of R is of the form $ma + nb$, where $m = 0$, 1, 2, or 3 and $n = 0$ or 1. It follows from the identities

$$a[a,b] = [a,ab],\ [a,b]a = [a,ba],\ b[a,b] = [ba,b],\ [a,b]b = [ab,b]$$

that C is an ideal of R.

Finally, suppose that R has additive group

$$C_2 \oplus C_2 \oplus C_2 = \langle a\rangle \oplus \langle b\rangle \oplus \langle c\rangle,$$

where $2a = 2b = 2c = 0$. It is easily seen that the commutator subset C of R is an additive group. By considering different cases we shall show that C must be an ideal of R.

Case1 Suppose that $[a,b] = 0$. Then the commutator subset is $\{0, [a,c], [b,c], [a+b,c]\}$. Any element of R is of the form $ka+lb+mc$, where each of k,l and m is either 0 or 1. We have

$$\begin{aligned}(ka+lb+mc)[a,c] &= kaac - kaca + lbac - lbca + mcac - mcca\\ &= k[a,ca] + l[a,bc] + m[ca,c] \in C.\end{aligned}$$

Also, since $[a,b] = 0$, we have

$$\begin{aligned}[a,c](ka+lb+mc) &= kaca - kcaa + lacb - lcab + macc - mcac\\ &= k[a,ca] + lacb - lcba + macc - mcac\\ &= k[a,ca] + l[a,cb] + m[ac,c] \in C.\end{aligned}$$

Similarly $(ka+lb+mc)[b,c] \in C$ and $[b,c](ka+lb+mc) \in C$. So C is an ideal. Similarly if $[b,c] = 0$ or $[a,c] = 0$, then C is an ideal. So we can suppose $[a,b], [b,c]$ and $[a,c]$ are all non-zero.

Case 2 Suppose that $[a,b] + [b,c] = 0$. Now $[a+c,b] = 0$ and

$$C = \{0, [a,c], [a,b], [a,b+c]\}.$$

We have

$$\begin{aligned}(ka+lb+mc)[a,c] &= k(aac-aca) + l(bac-bca) + m(cac-cca)\\ &= k[a,ac] + l(b(a+c)c - bc(a+c)) + m[ca,c]\\ &= k[a,ac] + l((a+cbc - bc(a+c)) + m[ca,c]\\ &= k[a,ac] + l[(a+c),bc] + m[ca,c] \in C.\end{aligned}$$

Similarly

$$\begin{aligned}&[a,c](ka+lb+mc) \in C,\\ &(ka+lb+mc)[a,b] \in C\end{aligned}$$

and

$$[a,b](ka+lb+mc) \in C,$$

also. Therefore C is an ideal.

Case 3 Suppose that $[a,b]+[b,c]+[a,c] = 0$. Then $[b,c] = [a,b+c]$ and

$$C = \{0, [a,b], [a,c], [a,b+c]\}.$$

As above we can easily show that C must be an ideal.

We can finally suppose that all of the cases above do not occur. Thus it follows that if $k[a,b] + l[b,c] + m[a,c] = 0$, then

$k = l = m = 0$. Therefore C has order 8, in which case $C = R$. Therefore the commutator subset of a ring of order 8 is an ideal. We conclude that 16 is the smallest order of a ring in which the commutator subset is not an ideal.

Acknowledgement The author is grateful to P. D. MacHale for several discussions on the topic of this note.

References

[1] B. Fine, *Classification of finite rings of order p^2*, Mathematics Magazine **66** (1993), 248-252.

[2] C. R. Fletcher, Rings of small order, Mathematical Gazette **64** (1980), 9-22.

T. Creedon,
Department of Mathematics,
University College,
Cork.

WHEN IS A FINITE RING A FIELD?

Des MacHale

When I was an undergraduate, there were two theorems in algebra that took my fancy. The first was

Theorem 1. *A finite integral domain is a field.*

The second was the beautiful theorem of Wedderburn (1905).

Theorem 2. *A finite division ring is a field.*

I often wondered why the standard proof of Theorem 1 was relatively easy and why all of the proofs of Theorem 2 are relatively difficult. I wondered too if it might be possible to prove a single theorem that would include both Theorem 1 and Theorem 2 as special cases. The following is an attempt in that direction.

Theorem 3. *Let $\{R, +, \cdot\}$ be a finite non-zero ring with the property that if a and b in R satisfy $ab = 0$, then either $a = 0$ or $b = 0$. Then $\{R, +, \cdot\}$ is a field.*

Recall that $\{R, +, \cdot\}$ is an integral domain if $\{R, +, \cdot\}$ is a commutative ring with unity $1 \neq 0$ with the property that $ab = 0$ implies either $a = 0$ or $b = 0$. Clearly, a finite integral domain satisfies the hypothesis of Theorem 3.

Recall too that a division ring $\{R, +, \cdot\}$ is a ring in which the non-zero elements of R form a multiplicative group with unity 1. A finite division ring $\{R, +, \cdot\}$ also satisfies the hypothesis of Theorem 3. To see this, suppose that for elements a and b of R, we have $ab = 0$. If $a = 0$, we are finished, so suppose that $a \neq 0$. Then a^{-1} exists in R. Hence $b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$, as required. Note finally that in the hypothesis of Theorem 3, we are assuming neither commutativity of multiplication, nor the existence of inverses. These have all to be established.

Proof of Theorem 3: Since $R \neq \{0\}$, we can choose a fixed non-zero element a of R. Let

$$R = \{r_1, r_2, \ldots, r_n\}.$$

Define a function $\alpha : R \to R$ by

$$(r_i)\alpha = r_i a$$

for all i. Now if $(r_i)\alpha = (r_j)\alpha$, then $r_i a = r_j a$ and hence $(r_i - r_j)a = 0$. Since $a \neq 0$, this forces $r_i = r_j$, so α is one-to-one, and since R is finite, α is onto. Thus there exist elements t and t^* in R such that

$$ta = a \text{ and } t^*a = t.$$

Now define a function $\beta : R \to R$ by

$$(r_i)\beta = ar_i$$

for all i. Again, if $(r_i)\beta = (r_j)\beta$, then $ar_i - ar_j = 0 = a(r_i - r_j)$, so $r_i = r_j$. Thus β is one-to-one, hence onto, and there exist elements s and s^* in R such that

$$as = a \text{ and } as^* = s.$$

Now let x be any element of R. Since α and β are onto, there exist elements b and c in R such that

$$x = ba = ac.$$

We now have

$$tx = t(ac) = (ta)c = ac = x,$$

so t is a left unity for $\{R, +, \cdot\}$. Similarly,

$$xs = (ba)s = b(as) = ba = x,$$

so s is a right unity for $\{R, +, \cdot\}$. Thus $t = ts = s = 1$ is a unity for R.

Now as $as^* = s = 1 = t = t^*a$, it follows that a has a right inverse s^* and a left inverse t^*. Thus

$$s^* = 1s^* = (t^*a)s^* = t^*(as^*) = t^*1 = t^*,$$

so $s^* = t^* = a^{-1}$ and we see that each non-zero element a in R is invertible in R. Thus R is a finite division ring and hence by Wedderburn's theorem, R is a field. This completes the proof. ∎

Of course, the theory now proceeds to show that $|R| = p^n$ for some prime p and positive integer n and if $R_1 = |R_2| = p^n$, then R_1 and R_2 are both isomorphic to the unique Galois field $\mathrm{GF}(p^n)$, a rather remarkable result given the innocent looking hypothesis of Theorem 3.

Finally, we mention three other directions in which Wedderburn's theorem can be strengthened.

Theorem 4. [1] *Let $\{R, +, \cdot\}$ be a finite ring with unity $1 \neq 0$ such that more than $|R| - \sqrt{|R|}$ elements of R are invertible. Then $\{R, +, \cdot\}$ is a field.*

The example $\{\mathbf{Z}_{p^2}, \oplus, \odot\}$ for a prime p shows that this result is best possible.

Theorem 5. [2] *Let $\{R, +, \cdot\}$ be a finite ring with unity $1 \neq 0$ in which every non-zero ring commutator $xy - yx$ is invertible. Then $\{R, +, \cdot\}$ is commutative.*

Of course, $\{R, +, \cdot\}$ need not be a field, as $\{\mathbf{Z}_4, \oplus, \odot\}$ shows.

Theorem 6. [3] *Let $\{R, +, \cdot\}$ be a finite non-zero ring and suppose that for each $a \neq 0$ there exists a unique b with $aba = a$. Then $\{R, +, \cdot\}$ is a field.*

References

[1] D. MacHale, *Wedderburn's theorem revisited*, Bull. IMS **17** (1986), 44-46.

[2] D. MacHale, *Wedderburn's theorem revisited (again)*, Bull. IMS **20** (1988), 49-50.

[3] N. H. McCoy, The Theory of Rings. Macmillan: New York, 1964.

D. MacHale,
Department of Mathematics,
University College,
Cork.

A RE-ANALYSIS OF BESSEL'S ERROR DATA

A. Kinsella

Introduction

The Gaussian (Normal) probability model

$$f(x;\mu,\sigma)=\frac{\exp(-(x-\mu)^2/2\sigma^2)}{\sigma(2\pi)^{1/2}}$$

is, arguably, the most widely used probability model because of

1. the fact that it is found as a limiting form of other common probability models;

2. the operation of the Central Limit Theorem which gives rise to the Gaussian form;

3. the intuitive appeal of the model as a description of measurement errors in that it postulates that, in the long run, measurements will zone in on the "true but unknown" quantity of interest, μ, and will be close to this value, lying between $(\mu-\sigma)$ and $(\mu+\sigma)$ some 68% of the time;

4. the mathematical tractability of linear and quadratic functions of Gaussian random variables which are used in Student's t and F ratio tests;

5. the ability of the model to readily change location and shape because of the independence of μ, the location parameter, and σ, the shape parameter.

A simple transformation of the random variable, namely,

$$y=|x|$$

gives rise to the Folded Normal probability model

$$g(y;\mu,\sigma) = \frac{\exp(-(y-\mu)^2/2\sigma^2) + \exp(+(y-\mu)^2/2\sigma^2)}{\sigma(2\pi)^{1/2}}$$

which can arise when empirical observational data are recorded without regard to the sign. If the signed data are postulated to conform to the Gaussian probability model, the unsigned data will conform to the Folded Normal model. An example of the possible use of this model is provided by the data set given by Topping, [1], in his discussion of "Normal error distributions". The data, which are displayed in the first two columns of Table 1, are the "much discussed example of observational data satisfying the normal error law (which) was given by Bessel". This data set tabulates "the errors involved in measuring the right ascension of stars.", the magnitude of the error of observation, in seconds, being shown in the first column of Table 1 with the corresponding frequency in the second column. In his subsequent analysis of this data set Topping assumes that since "positive and negative errors are grouped together, ... so we can only assume that they are equally divided". This assumption is the basis of the subsequent analysis in terms of a Gaussian model. This note analyses the data set on the assumption that the Folded Normal model is appropriate.

Table 1: Right Ascension Error Data Set

Limits of Error	Observed Frequency (n)	Predicted Frequency (e)	Pearson Residual (r)
0.0 – 0.1	114	102.1	+1.174
0.1 – 0.2	84	84.4	−0.041
0.2 – 0.3	53	57.6	−0.005
0.3 – 0.4	24	32.5	−1.487
0.4 – 0.5	14	15.1	−0.290
0.5 – 0.6	6	5.8	+0.074
0.6 – 0.7	3	1.9	+0.845
0.7 – 0.8	1	0.5	+0.737
0.8 – 0.9	1	0.1	+2.756

Parameter Estimation

The Maximum Likelihood method of parameter estimation was used to extract numerical estimates of the unknown parameters, μ and σ, from the data set. In general, if the data set is a random sample of size n, denoted by $(x_1, x_2, \ldots, x_n)$, the Likelihood Function is

$$L(\theta) = f(x_1;\theta)f(x_2;\theta)\ldots f(x_n;\theta),$$

where $f(x;\theta)$ denotes the probability model of interest and θ denotes the set of parameters of the model. Since the data are, or will be, known, the Likelihood Function is a function of the elements of the set of parameters, namely, θ, which are continuous *nonrandom* variables. The Maximum Likelihood Estimator(s) of the parameter(s) are the value(s) which maximize the Likelihood Function, namely, the "most likely" value(s) which can be found using the data set. In simpler cases exact functions of the data are found to be the Maximum Likelihood Estimators, these being the solutions(s) to the equation(s)

$$\frac{\delta L(\theta)}{\delta\theta} = 0 \text{ or } \frac{\delta \mathrm{Log}(L(\theta))}{\delta\theta} = 0.$$

A complication arises in the case of the data set in Table 1 because the observational data, the error, is censored in that the number of occasions on which an error lies within an interval of length 0.1 seconds is recorded rather than the actual value of the error. This means that the Likelihood Function has to be rewritten as

$$L(\mu,\sigma) = \frac{N!}{n_1!n_2!\ldots n_9!}(F_1)^{n_1}(F_2)^{n_2}\ldots(F_9)^{n_9}$$

which is a multinomial probability model. In this Likelihood Function, N denotes the total number of observations,

$$N = \sum_{i=1}^{9} n_i = 300,$$

$$n_1 = 114, n_2 = 84, \ldots, n_9 = 1,$$

and F_i denotes the integral of the Folded Normal probability model over the i^{th} interval,

$$F_1 = \int_{0.0}^{0.1} g(y; \mu, \sigma) dy, \ldots, F_9 = \int_{0.8}^{0.9} g(y; \mu, \sigma) dy.$$

These integrals give the probability that a randomly chosen observation will fall in any given interval.

Because of the necessity of numerically integrating the Folded Normal probability model, it is necessary to use a search method to find the values of μ and σ which maximize the Likelihood Function, the Maximum Likelihood estimates. A simple "trial and error" search of the two dimensional parameter space was used in this case. The values of the negative of the natural logarithm of the Likelihood Function, excluding the constant factor involving $N!$ and $n_i!$, are shown for a wide grid of values in Table 2.

Table 2: Logarithm of Likelihood Function

μ/σ	0.10	0.15	0.20	0.25	0.30	0.35	0.40
−0.2	566.2	492.4	487.7	499.6	517.3	537.5	558.8
−0.1	615.4	489.4	466.3	473.5	492.1	515.1	539.3
0.0	805.3	529.9	470.2	468.0	484.7	507.9	533.0
0.1	615.4	489.4	466.3	473.5	492.1	515.1	539.3
0.2	566.2	492.4	487.7	499.6	517.3	537.5	558.8

This function is chosen because the Maximum Likelihood estimate will minimize its value so that, in general, a function minimization algorithm can be used to obtain the required values. The use of a more refined grid in the region

$$-0.1 < \mu < +0.1, \quad 0.20 < \sigma < 0.30$$

indicated that the logarithm of the Likelihood Function was more sensitive to changes in σ than in μ. The final values which were chosen were $\mu = 0.0$ and $\sigma = 0.227$. The changes in the value of the logarithm of the Likelihood Function were of the order of 0.001 for corresponding changes in the magnitudes of μ and σ.

Model Evaluation

The "goodness of fit" of the Folded Normal probability model to the data set was judged by Pearson residual, [2, pp.37-39], which is defined as

$$r_i = (n_i - e_i)/(e_i)^{1/2},$$

where e_i is the expected frequency in the i-th censoring interval, being equal to

$$N \int g(y; \hat{\mu}, \hat{\sigma})\, dy,$$

the integral being over the appropriate interval. Here $\hat{\mu}$ and $\hat{\sigma}$ denote the Maximum Likelihood estimates. The square of the Pearson residual is the the i-th component of the familiar Chi-squared test statistic

$$X^2 = \sum_{i=1}^{9} (n_i - e_i)^2 / e_i$$

and is useful in indicating which components of the overall test are making the largest contributions. On the basis that the Pearson residual has, approximately, a Standard Gaussian distribution ($\mu = 0$, $\sigma = 1$) one value of r_i, namely, +2.76, is sufficiently large to warrant some attention. This arises because the expected frequency is approximately one tenth of the observed frequency but since this apparent problem arises in a low frequency tail it is of no practical significance.

On the basis of this analysis the claim that the error has a Gaussian distribution would appear to be vindicated in view of the connection of that probability model with the Folded Normal Probability model.

References

[1] J. Topping, Errors of Observation and their Treatment. Chapman and Hall: London, 1971.

[2] P. McCullagh and J. A. Nelder, Generalized Linear Models, 2nd ed. Chapman and Hall: London, 1990.

A. Kinsella,
Department of Mathematics, Statistics and Computer Science
Dublin Institute of Technology,
Kevin Street,
Dublin 8.

SOME MATHEMATICAL ASPECTS OF INFORMATION TECHNOLOGY: FIXED POINTS AND THE FORMAL SEMANTICS OF PROGRAMMING LANGUAGES

Anthony Karel Seda

1. Introduction

> "It is reasonable to hope that the relationship between computation and mathematical logic will be as fruitful in the next century as that between analysis and physics in the last. The development of this relationship demands a concern for both applications and for mathematical elegance." John McCarthy[1], 1967.

In describing Information Technology, the Web page of the recently formed Information Technology Centre at University College, Galway says this: "During the past decade Information Technology (IT) has transformed business life, from the boardroom to the shopfloor. As we generally understand it, Information Technology is an outgrowth from the computer, microelectronics, and telecommunications industries, and now comprises: computer processors and data storage devices, telecommunications, software, microprocessors, automation technologies and user interface media."

Generally speaking, users of IT need not be expert in, nor even familiar with, the technologies which support it. If this is true, it is even more true that these same users need have no knowledge of the *theory* which supports the technologies which support IT. Nevertheless, the issue of the theories underlying IT and, in particular, which areas of mathematics are important in

[1] Inventor of the programming language Lisp and pioneer of AI.

it, is itself important and interesting. At the moment, the vehicle moving all the activity in IT is the electronic digital computer, and this state of affairs is likely to persist for some time into the future. Therefore, questions concerning the relationship of mathematics to IT are often really questions concerning some more or less theoretical issue in computer science, and indeed such issues are raised in this Bulletin from time to time, sometimes in an educational context, see [16], for example. So, just which areas of mathematics are currently of importance in research and teaching in theoretical computer science and IT, and which of these areas will prove to be of enduring importance in this context? But before addressing this question, it will be helpful to say a few words about the recent history of IT.

Much of the recent and ongoing work in IT has as its focus new generation computing and is the direct result of the efforts of the Alvey and ESPRIT programmes in Europe, ICOT in Japan and the consortium known as the Microelectronics and Computer Technology Corporation in the U.S.A. Indeed, all this was directly inspired by ICOT's announcement in 1982 of its intention to build the so called fifth generation computer, prompting a global race from about 1985 onwards to build such machinery. It was found necessary within these projects, see [1, 2], to broadly divide the whole of IT into, initially, four *enabling technologies*: VLSI (Very Large Scale Integration, which is concerned with chip fabrication and computer architecture); MMI (Man-Machine Interface, or human factors in computing); SE (Software Engineering, which is concerned with putting the production of software on a scientific basis (in particular, the development and use of formal methods of verification in the manufacture of software and hardware)); IKBS (Intelligent Knowledge Based Systems, i.e. Artificial Intelligence (AI)). As a matter of fact, communications and networks quickly came to be seen as so important that they were taken to be the fifth enabling technology.

The classification just described is useful as a means of organizing the applications of mathematics to IT, and can help determine which are central and which are of lesser importance. As one would expect, all five of these enabling technologies use mathematics, to a greater or lesser extent, in the way that it is used in other sciences, that is, as a precise language in which to formulate problems and results and as a tool with which to solve these problems (even MMI uses mathematics in problems concerned with pattern recognition). Returning to our main question, and taking a glance at, say, the thirteen volumes which collectively make up [3, 13, 40], and which cover several thousand pages, shows that even the first part of our question is by no means easy to answer (and the volumes just cited cover mainly the mathematics relevant to SE and IKBS and say little about the other three areas). However, such a glance does make it clear that the answer "discrete mathematics" which is sometimes proposed in response to this question is only a small part of the story, at least when this term is interpreted to mean graph theory and combinatorics, as is often the case. Important as graph theory and combinatorics undoubtedly are, they do not explain, for example, the many uses of category theory and topology in connection with domain theory and the formal semantics of programming languages. Much less do they explain the many uses of mathematical logic in connection with program verification and within machine intelligence and robotics. Still less do they explain the use of real and complex analysis in the analysis of algorithms, and the use, say, of measure and integration in connection with probabilistic powerdomains on the one hand, and in connection with uncertainty in reasoning systems on the other (where fuzzy logic is also important). Indeed, one can continue in this vein citing seemingly endless applications of different branches of mathematics to various aspects of the theory of computation and IT, and some of these are indicated in the References at the end of this article. On the other hand, many others are not mentioned at all, and there is indeed an immense literature covering the various topics of which our bibliography is but a tiny fraction.

Devising a complete classification of all the areas of mathematics which are of importance in IT would be an interesting and valuable project in its own right, though time consuming and beyond the abilities of the author, and in any case is not the objective of this article. Instead, we propose to take one concept, that of *fixed point*, and attempt to relate it to two of the main areas, SE and IKBS, which were identified earlier. The notion of fixed point is, of course, of great importance within mathematics, and it turns out also to be central in the areas we intend to consider in the context of programming language semantics. There may well be applications of ideas concerning fixed points elsewhere within IT, but they will not fall within our scope. Thus, specifically, we consider the use of fixed points in relation to the problem of giving formal, machine independent meaning (a formal semantics) to computer programs. To do such is fundamental to the problem of formal verification of software, or the use of formal methods as it is known in industry, and we take up this issue for procedural programs in §2. In §3 we briefly consider basic ideas of formal systems and mathematical logic preparatory to the discussion, in §4, of the role of fixed points in computational logic (the declarative style of programming). Again, fixed points are fundamental in this area in order to both give meaning to programs and to gain deep insight into the computation process itself, necessary if advanced machine reasoning features are to be developed such as time dependent logics, the ability for machines to learn and so on. Such questions are themselves of importance of course given the extent to which computers control complex and important systems in modern society. Finally, in §5 we discuss briefly the uses of topology, some due to the author, which unite the two themes just described. Given space limitations, not to mention those of the writer, it is not possible to do much more here than touch on the main issues. Nevertheless, it is hoped to show, en route, that the simple concept of fixed point links in a coherent fashion a wealth of important ideas drawn from mathematical logic, recursive function theory, topology, category theory and abstract algebra in an effort to resolve the apparently simple question of what a program means. Indeed, far from being simply a matter of pressing keys on a computer keyboard, which is the end user's perception, IT has behind it a rich and fascinating theory which makes use of many fundamental ideas drawn from many parts of mathematics. That at any rate has been the experience of the author over the first decade of IT, a subject which by all accounts

is set to become one of the two or three dominant forces which shape the next century.

2. Fixed-point semantics of procedural programs

No matter what programming language it is written in, a program P computes a function f. By suitably coding data structures (lists, arrays etc.) and by a simple conjugacy, we can suppose without loss of generality (though not necessarily without loss of convenience) that f is defined on vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in N^n$, for some natural number n, and takes values in N, where N denotes the set $\{0, 1, 2, \ldots\}$ of natural numbers together with zero. The essence, of course, of computer science is the translation of formal or informal algorithm into (high level program) code. It is therefore eminently reasonable from the point of view of the computer scientist to impose some resource bounds on the notion of *algorithm* that one adopts, see [15]. We shall not, however, do this here so that we employ this term in the manner familiar in mathematics and in particular in the usual sense of recursive function theory, see [21, 26]. This means that f is a partial recursive function (a *computable* function) and that its domain is a possibly strict subset of N^n; if the domain of f is all of N^n, then f will be called *total*. Let us therefore denote by $\mathcal{F}_n$ the collection of all partial functions from N^n to N and write dom(f) for the domain of f. Given two functions $f, g \in \mathcal{F}_n$, we write $f(\mathbf{x}) \simeq g(\mathbf{x})$ to mean that if one of $f(\mathbf{x})$ or $g(\mathbf{x})$ is defined, then both are defined and equal. With this notation, we may define the graph of f, graph(f), by graph$(f) = \{(\mathbf{x}, y); f(\mathbf{x}) \simeq y\}$, and as usual graph$(f)$ will be identified with f. This notion permits us to partially order $\mathcal{F}_n$ by: $f \leq g$ iff graph$(f) \subseteq$ graph(g), and we note the following two facts. (i) The nowhere defined function f_ϕ, whose graph is the empty set, satisfies $f_\phi \leq f$ for all $f \in \mathcal{F}_n$, and therefore is the *bottom element* of $\mathcal{F}_n$. (ii) $\mathcal{F}_n$ is an ω-complete partial order in that any chain $f_\phi \leq f_1 \leq f_2 \leq \ldots$ has a supremum $f = \bigcup_{m=1}^{\infty} f_m$, where f satisfies (and is well defined by) $f(\mathbf{x}) \simeq \mathbf{y}$ iff $f_m(\mathbf{x}) \simeq \mathbf{y}$ for some m.

The main theorem we will need in this section is the following, known as Kleene's first recursion theorem, see [11, 21, 26].

Theorem 1. *Suppose that $\Phi : \mathcal{F}_n \to \mathcal{F}_n$ is a recursive operator. Then Φ has a least fixed point h which is a computable function. Thus, there is a computable function h satisfying*
a) $\Phi(h) = h$,
b) if $\Phi(g) = g$, then $h \leq g$.
Hence, if h is total, then it is the only fixed point of Φ. ■

We will not give a formal definition of the term *recursive* used here, but the essence of the idea is that whenever $\Phi(f)(\mathbf{x})$ is defined, its value depends only on finitely many values of f and these values can be chosen in a computable fashion. Note that Φ is itself totally defined, that is, defined on all of $\mathcal{F}_n$, but of course $\Phi(f)$ may be a partial function. It will be convenient to write $\Phi(f;\mathbf{x})$ in place of $\Phi(f)(\mathbf{x})$.

We also will not give details of the proof of this theorem, other than those which we will need later on, and they are as follows. We define inductively the following chain (f_n) of elements of $\mathcal{F}_n$: $f_0 = f_\phi$ and $f_{m+1} = \Phi(f_m)$, and now let $h = \bigcup_{m=0}^{\infty} f_m$. The continuity of Φ, implied by recursiveness and defined later, shows that h is a fixed point; the construction shows it to be the least such; recursiveness of Φ is used to show that h is in fact a computable function.

To show how this theorem is used, we consider the following simple example which is an adaptation, in some of the detail, of an example to be found in [37]. It will serve to make clear the central problem under discussion and the manner of its solution.

Example 1 Consider the problem of finding the greatest common divisor, $\gcd(a,b)$, of the two positive natural numbers a and b. The usual way to do this is to apply the Euclidean algorithm and write $a = q(a,b)b + r(a,b)$ for unique choice of natural numbers $q(a,b)$ and $r(a,b)$, where the remainder $r(a,b)$ satisfies $0 \leq r(a,b) < b$. It is then noted that $\gcd(a,b) = \gcd(b, r(a,b))$, if $r(a,b) > 0$, and that the pair $(b, r(a,b))$ is "smaller" than the pair (a,b), so that repeated application of this technique is bound to terminate (in the required gcd). It will be convenient to regard r as totally defined by setting $r(a,0) = a$ for all a, and $r(0,b) = 0$ for all b. Then, with similar, suitably chosen exceptional values for q, we see that the identity $a = q(a,b)b + r(a,b)$ is satisfied for all a and b. Now, a procedural-language implementation P of the algorithm just described, say in PASCAL, will contain a program statement of the form "gcd := gcd(y,z)", and a mathematical formulation of the algorithm is given by

$$\gcd(a,b) = \begin{cases} b, & \text{if } r(a,b) = 0; \\ \gcd(b, r(a,b)), & \text{otherwise.} \end{cases}$$

The program, and the formulation just given, recursively or implicitly define gcd in terms of itself, and the question which naturally arises now is "What is the meaning or interpretation of such a definition?" From the point of view of computation, that is, from the point of view of *operational* or *procedural semantics*, the answer is simply that we are given an iterative procedure to calculate the function gcd. Such a meaning, closely related to the behaviour of P when running on a machine, is not in general satisfactory for purposes of formal verification, and a machine independent explicit definition is needed. The standard way to obtain this, in general, is to pass to an associated operator Φ and take the function which P is intended to compute to be the least fixed point of Φ. To see how this works for the problem in question, we define $\Phi : \mathcal{F}_2 \to \mathcal{F}_2$ by

$$\Phi(f;a,b) \simeq \begin{cases} b, & \text{if } r(a,b) = 0; \\ f(b, r(a,b)), & \text{otherwise.} \end{cases}$$

It is important to note that the definition of Φ is explicit i.e. does not involve recursion. Moreover, because $\Phi(f;a,b)$ depends only on the one value $f(b, r(a,b))$ of f, for any f and (a,b), it follows that Φ is a recursive operator. Applying Kleene's theorem, we obtain the least fixed point h of Φ, and h is a computable function. By reference to the synopsis of the proof of Kleene's theorem, given above, we note the following:
1) $f_1(0,b) = b$ for all b, and $f_1(a,0)$ is undefined for $a > 0$.
2) $f_2(0,b) = b$ for all b necessarily, and $f_2(a,0) = f_1(0,a) = a$ for all $a > 0$. It follows that $h(0,b) = b$ for all b and $h(a,0) = a$ for all a.

3) If h_1 is any fixed point of Φ, and thus satisfies the equation

$$h_1(a,b) \simeq \begin{cases} b, & \text{if } r(a,b)=0; \\ h_1(b,r(a,b)), & \text{otherwise.} \end{cases}$$

then it is easy to check that $h_1(a,b)$ coincides with $\gcd(a,b)$ for positive a and b.

It follows from these observations that $h(a,b)$ coincides with $\gcd(a,b)$ for positive a and b and therefore that h is totally defined. Hence, h is the unique fixed point of Φ, and so we recover gcd as the unique fixed point of Φ provided we are willing to accept that $\gcd(a,0)=a$ for all a and $\gcd(0,b)=b$ for all b, which is reasonable, and in particular $\gcd(0,0)=0$, which is not unreasonable.

The discussion of this example, even though a little accelerated, identifies many of the main points of the theory, and these points can be summarized as follows.

- There is a need for abstract models of computation. Usually these are ordered spaces (such as Scott domains, see [37], and indeed much of this theory has been heavily influenced by the work of Dana Scott and Gordon Plotkin, see [28, 29, 30, 36]) but sometimes are metric spaces or even quasi-metric spaces, see [35]. Such spaces should permit one to model the computation process itself perhaps by better and better (increasing) approximations to a limit or supremum, and should incorporate a certain finiteness, known as algebraicity, which we will not identify, again see [37]. At the very least, the domains chosen must permit the construction of fixed points of certain operators. Moreover, to model features of real programming languages they must be closed under the formation of products, sums, function space, power domain (to model non-determinism) and must permit the solution of so called recursive domain equations. One is therefore looking for a Cartesian closed category of domains. The (ongoing) search for such categories is a beautiful example of pure mathematics, with the satisfaction that at all times it is closely related to genuine problems in the design of advanced programming languages.
- Fixed points can be used, via fixed point induction, to verify programs and their properties, see [22, 23]. They also can force suitable choices of exceptional values and, more importantly, eliminate problems involving choice where computation rules are used in evaluating recursive definitions.

Whilst this is only the start of the theory, we can take it no further for we want to turn now to consideration of the other main strand of this article, namely, the use of mathematical logic in IT and the role of fixed points in that context.

3. Logic, computability and formal systems

Ever since the early discoveries made by the Ancient Greeks, there has been a strong interplay between mathematics and logic, leading to the specific area of *mathematical logic*. This subject is concerned with both analysing the reasoning used in mathematics and also contributing to that subject, especially to its foundations, by examining the limits to mathematical reasoning and to what is possible. In addition, mathematical logic is proving to be indispensable in the theory of computation and in IT for several reasons, including its use in formal verification of software and as a computational medium. We will not discuss the first mentioned, in this section, other than to give references to appropriate literature; the latter we will discuss in more detail in the next section. It will be convenient to assume that the reader is familiar with elementary notions concerned with syntax: formation of terms and well formed formulae (usually abbreviated to wff, whether in the singular or the plural) from an alphabet, and the corresponding first order language. We also assume that the reader is similarly familiar with elementary notions of semantics: interpretations, formal assignment of truth values to wff, models, logical consequence and validity, for details see [7, Chapter 1].

In modern terminology, what the Greeks conceived of is the concept of a *formal system* or *formal deductive system* in which, within a theory, one reasons from axioms (distinguished wff in the underlying first order language) by applying formal rules of inference to obtain new "truths" or theorems (this process being inductive of course). Roughly speaking, this concept is defined as follows, and a useful general reference is again [7, Chapter 1].

Definition 1 A *formal system* $\mathcal{S}(\mathcal{L},\mathcal{A},\mathcal{R})$ or just $\mathcal{S}$ consists of:

1) A first order language $\mathcal{L}$ called the *underlying first order language*, whose alphabet is chosen so that $\mathcal{L}$ is adequate to describe the theory one has in mind.
2) A distinguished set $\mathcal{A}$ of wff in $\mathcal{L}$ called the *axioms*; usually some computability restriction is imposed here such as "it is decidable which wff are axioms" (the set of axioms therefore forms what is known as a *recursive set* and the system is said to be *recursively axiomatizable*).
3) A set $\mathcal{R}$ of *rules of inference*.

Rules of inference take the following general form: $\frac{\text{Input}}{\text{Output}}$ where Input and Output are both sets of wff of a specific syntactic form. For example, one well known rule is *Modus Ponens* which has the form:

$$\frac{\begin{array}{l}A \to B\\ A\end{array}}{B}$$

where A and B are *syntactic variables* i.e. vary over wff. Thus, for example, if the wff $(\forall x\, p(f(x))) \to q(g(a,b))$ and $\forall x\, p(f(x))$ are taken as Input, then the Output is $q(g(a,b))$.

Other examples of rules of inference can be found in [7, Chapter 1].

Definition 2 A *proof* in a formal system $\mathcal{S}$ consists of a finite string $A_1A_2\ldots A_n$ of wff A_i in $\mathcal{L}$ where each A_i is either an axiom or follows from earlier A_j by application of a rule of inference. The end term A_n in a proof is called a *theorem*. If a wff A in $\mathcal{L}$ is the end term of some proof (i.e. if A is a theorem), we say that A is *derivable* or *provable* and write $\mathcal{S} \vdash A$ or $\mathcal{A} \vdash A$.

This definition encapsulates a formalist or mechanical view of reasoning in which there is no meaning or semantics (it is purely syntactic): one keeps on mechanically applying rules of inference generating more and more proofs and therefore more and more theorems without regard to whether or not the theorems are "true". Nevertheless, certain immediate questions arise about formal systems for which a satisfactory answer requires truth values:

Correctness of rules of inference
This is easy to answer: a rule of inference is *correct* or *sound* provided that its Output is a logical consequence of its Input. For example, since a wff B is always a logical consequence of wff $A \to B$ and A, Modus Ponens is a correct rule of inference.
Completeness of a formal system Roughly speaking this is a question about the power of a formal system to prove anything which could reasonably be expected to be provable and it depends mainly on the choice of the set $\mathcal{R}$ of rules of inference. There are several styles of formal system in use and two in particular are the *Hilbert style* formal system and the *Gentzen style* formal system. These are described in detail in [7, Chapter 1] where the exact form of the rules of inference is given in order to handle substitutions and quantifiers. The main result concerning completeness for both these styles of formal system is Gödel's well known completeness theorem, where $\models$ is the symbol for logical consequence.

Theorem 2. *In a Hilbert style or Gentzen style formal system $\mathcal{S}$, a well formed formula A is derivable iff it is a logical consequence of $\mathcal{A}$. Thus, in symbols $\mathcal{A} \vdash A$ iff $\mathcal{A} \models A$.* ■

Incompleteness in formal systems
Recall that $\mathcal{A} \models A$ means that A is true in *every* model of $\mathcal{A}$. So, if a wff A is true in some models of $\mathcal{A}$ but false in others, then A cannot be provable by Theorem 1, and conversely. The main question which arises is whether or not in a given theory (in particular this question arose in relation to Peano Arithmetic $\mathcal{PA}$) there is a closed wff, or sentence, A which is true in the intended interpretation of that theory which is not provable. In the case of $\mathcal{PA}$ the intended interpretation is the expected one in which the domain is the set of natural numbers and the function symbols there are interpreted as addition and multiplication. The shocking answer to this question for $\mathcal{PA}$ that there are such wff is the content of Gödel's famous first incompleteness theorem, a simple, but useful, form of which is as follows, see [11].

Theorem 3. *Suppose $\mathcal{S}$ is any recursively axiomatized formal system for Peano Arithmetic $\mathcal{PA}$ in which every provable sentence* *is true in the intended interpretation. Then there is a sentence σ in $\mathcal{PA}$ which is true in the intended interpretation but not provable. Consequently, $\neg\sigma$ is not provable either (since $\neg\sigma$ is not true), and σ is called an undecidable sentence.* ■

This theorem together with Gödel's second incompleteness theorem (which roughly stated says that it is impossible to prove consistency of $\mathcal{PA}$ within $\mathcal{PA}$, where consistency means absence of contradictions), effectively destroyed Hilbert's plan to mechanize mathematics. This plan, of course, grew out of attempts to overcome paradoxes in the foundations of mathematics resulting from Cantor's theory of cardinals and the unrestricted use of power set operations, and from the desire for a proof of consistency of $\mathcal{PA}$ by finitary means. A good discussion of these results can be found in [34].

The basic reason for incompleteness in $\mathcal{PA}$ is the following, and it depends on concepts to do with computability. Suppose $\gamma : L \to N$ is a coding of the wff in $\mathcal{PA}$, so that γ is bijective, effectively computable and such that γ^{-1} is effectively computable, where L denotes the set of all wff in $\mathcal{PA}$ (Gödel's original coding was not actually bijective but simply injective, but it was decidable whether or not a given natural number n belonged to the image set of γ). Thus, given a wff A in L, we can effectively find its unique *code number* or *Gödel number* $\gamma(A)$; conversely, given a natural number n we can effectively find the unique wff $A = \gamma^{-1}(n)$ from which it came–the effectiveness of these operations is crucial. There are now two sets of interest here: one is the set $\mathcal{P}$ of all provable sentences in $\mathcal{PA}$ and its image $\gamma(\mathcal{P})$, and the other is the set $\mathcal{T}$ of all true sentences in $\mathcal{PA}$ and its image $\gamma(\mathcal{T})$. What Theorem 3 says is that $\mathcal{P} \subset \mathcal{T}$ and clearly this is iff $\gamma(\mathcal{P}) \subset \gamma(\mathcal{T})$. The heart of the matter is that the set $\gamma(\mathcal{P})$ *is* the image set of a computable function i.e. can be listed by a machine (such a set is called *recursively enumerable* or usually just r.e.) whilst the set $\gamma(\mathcal{T})$ is *not* listable by any machine; the two sets therefore cannot be equal. Indeed, the set $\mathcal{T}$ or rather $\gamma(\mathcal{T})$ is highly intractable and this fact is a deep issue with far reaching consequences.

These ideas concerning formal systems are of great importance in computing and in particular in connection with formal verification of software, see [23, 42]. However, the direction we want to pursue, in the next section, is the use of deduction as an actual computational medium, rather than as a tool of verification, and to investigate the use of fixed points in the corresponding theory.

4. Formal systems and computational logic

> "From hardware design to the development of new programming languages and the construction of artificial intelligence programs, Logic is the major mathematical tool. Logic will perform the function in IT that calculus performs in other areas of engineering. It will provide IT with a rigorous theoretical foundation," see [2].

The desire to mechanize reasoning and the related notion of building robots can probably be traced back a very long way in history. Certainly Descartes dreamt of a calculus with which one could perform reasoning by algebraic manipulation, a dream which was to be fulfilled by George Boole in *The Laws of Thought* with respect to propositional logic, leading to the concept of Boolean Algebra and its great use in analysing logic circuits in the hands of Claude Shannon. Perhaps, too, Blaise Pascal, Charles Babbage and Ada Byron, Countess of Lovelace, were thinking beyond mere arithmetical calculation when designing their calculating machines; certainly Babbage and Byron appear to have encountered the main concern of SE: proving that a program does what is intended.

Coming forward in time to the early years of this century, we encounter Hilbert's plan, mentioned earlier, to mechanize mathematics. As already noted, this plan came to a dead halt due to Theorem 3 and related results. Nevertheless, there is a positive side to this provided by Theorem 2. Just because some formal systems such as $\mathcal{PA}$ contain some unprovable true statements does not mean that reasoning suddenly becomes worthless. Perhaps we can make do with the theorems or logical consequences of a theory rather than deal with the larger set of all the statements true in some particular interpretation, especially if we can automate the reasoning process itself.

Following the point just made, the landmark result came in 1965 with J. A. Robinson's Unification Algorithm and his Unification Theorem, see [24, 25]. Robinson showed that there is a single rule of inference, called *resolution*, which is sound and complete in that Theorem 2 holds for formal systems using resolution as their sole rule of inference, and moreover resolution turns out to be easy to automate. To see how this works, it has first to be shown that *any* closed wff can be cast into a syntactically different but equivalent form called *conjunctive normal form CNF* (*closed* here means that there are no free variables i.e. all variable symbols in the wff are existentially or universally quantified; *equivalent* means that the new form is a logical consequence of the given wff and vice versa). We assume that this is so; as a matter of fact, not only can it be done but it can be done by an algorithm and hence is an effective operation. A wff written in CNF takes the form of a universally quantified conjunction $\forall (C_1 \wedge C_2 \wedge \ldots \wedge C_n)$, where each C_i is a *clause*, thus C_i has the general form $L_1^i \vee L_2^i \vee \ldots \vee L_{m_i}^i$, wherein each L_j^i is a *literal*, that is, either an atom A_j^i (a propositional formula) or a negated atom $\neg A_j^i$; it is usual to understand the universal quantifier $\forall$ to be present and to omit writing it. The resolution rule of inference can now be explained, at least in its simplest form, as follows. Suppose given two clauses, the *parent* clauses, $L_1^1 \vee L_2^1 \vee \ldots L_n^1$ and $L_1^2 \vee L_2^2 \vee \ldots \vee L_m^2$ the first of which contains the literal L, say, and the second $\neg L$ (the literals L and $\neg L$ are said to *clash*). Reordering and letting C^1 and C^2 denote the disjunctions of the obvious respective remaining literals, we can write the two given clauses as $C^1 \vee L$ and $C^2 \vee \neg L$. The resolution rule says that if we take these clauses as Input, then the Output is $C^1 \vee C^2$ (i.e. we simply "cancel" the clashing literals L and $\neg L$ and disjoin what remains). In the symbolism of a rule of inference, we have

$$\begin{array}{c} C^1 \vee L \\ C^2 \vee \neg L \\ \hline C^1 \vee C^2 \end{array}$$

This simple form is not adequate and a more general form is needed involving certain substitutions called *most general unifiers (mgus)*. In this more general form, clashing literals are still cancelled, but after unification has brought them into syntactic identity. Furthermore, Robinson's algorithm for finding mgus can be implemented with reasonable efficiency, giving the means of feasibly constructing automated theorem provers. Such devices have been extensively examined in the context of mathematics, see [20], and a number of new results have been established in various areas in addition to verifying old results (in classical analysis for example). The drawback, however, in using resolution is that it involves an immense amount of searching for clashing literals and hence automated theorem provers using it run slowly in comparison with modern procedural languages such as PASCAL or C.

Interesting as these applications to mathematics are, they are a little peripheral to the main thrust of this work. Developments made by Colmerauer et al. in Marseilles, [10], Kowalski and van Emden in Imperial College, [6, 39], and Warren in Edinburgh and Manchester, [41], identified a significant fragment of first order predicate logic (the Horn clause subset) relative to which a restricted form of resolution (SLD-resolution) ran as fast as conventional languages. Note that by grouping all positive atoms in a clause to one end, and all negative ones to the other, we can write an arbitrary clause in the form $A_1 \vee A_2 \vee \ldots \vee A_m \vee \neg B_1 \vee \neg B_2 \vee \ldots \vee \neg B_n$. In turn this can be written as $A_1 \vee A_2 \vee \ldots \vee A_m \leftarrow B_1 \wedge B_2 \wedge \ldots \wedge B_n$, where $\leftarrow$ denotes the connective "material implication." The relative slowness of resolution can now be traced to the presence, in general, of more than one atom in the "head" of this clause, that is, to $m > 1$, which causes a combinatorial explosion in search. Restricting syntax to allow only the case $m = 1$ results in so called (definite) program clauses of the type $A \leftarrow B_1, B_2, \ldots, B_n$, where A and all the B_i are atoms and the commas in the "body" denote conjunction. It also results in SLD-resolution running very fast. It is convenient to abuse notation and allow n to be zero to indicate that the body of a clause is empty, so that the clause in question is a *unit* clause $A \leftarrow$ or a "fact". This is in contrast to the conditional statement represented by a clause whose body is not empty.

Thus, in this paradigm (logic programming), a program is thought of as a finite set of axioms (each program clause being an axiom) in a formal system whose only rule of inference is SLD-resolution. Computation is thus (controlled) deduction. Moreover, soundness and completeness were both established for such systems and, in addition, it was shown that given any partial recursive function, there is a logic program that computes it. Thus, logic programming systems have as much power as conventional procedural languages despite the restricted syntax. This work led to the programming languages PROLOG and PARLOG (a parallel implementation), see [4, 19] for theoretical foundations and [9] for programming practice. Whilst not especially suited for numerical computation, logic programming languages are ideal for work in deductive databases, AI, and natural language processing in which first order predicate logic is viewed as a knowledge representation language. Current work which aims to incorporate λ-terms in clause bodies, and hence to amalgamate logic and functional programming styles, should result in increased flexibility. Here is an example of a PROLOG program (not quite in PROLOG syntax) which is a quick-sorting program intended to sort lists of non-negative integers and has two built-in predicates *le* and *gr*:

$$
\begin{aligned}
&qsort(nil, nil) \leftarrow \\
&qsort(H.T, S) \leftarrow part(H, T, P, Q), qsort(P, P1), qsort(Q, Q1), \\
&\qquad\qquad\qquad append(P1, H.Q1, S) \\
&part(R, H.T, H.X, Q) \leftarrow le(H, R), part(R, T, X, Q) \\
&part(R, H.T, X, H.Q) \leftarrow gr(H, R), part(R, T, X, Q) \\
&part(X, nil, nil, nil) \leftarrow \\
&append(nil, X, X) \leftarrow \\
&append(H.T, X, H.Y) \leftarrow append(T, X, Y)
\end{aligned}
$$

It should be observed that in addition to the operational semantics and the fixed point semantics (or *denotational semantics* as it is often termed) that exist for procedural programs, logic programs P have a third semantics, the *declarative semantics*. This term simply refers to the model-theoretic meaning P has when viewed as a first order theory, namely, the set of all logical consequences of P. The completeness alluded to earlier, when properly formulated, says that the set M_P of those ground atoms (i.e. those atoms containing no variable symbols) which are derivable or provable from the clauses in P via SLD-resolution coincides precisely with the set of ground atoms which are logical consequences of P, that is, those ground atoms true in every model of P. Unfortunately, this set M_P (which can be thought of as the set of things which P computes) is not easy to get hold of when considered in these terms. It is at this point that the fixed point semantics of P enters the picture, for it is a major result of the theory, Theorem 4 below, that M_P coincides with the least fixed point of an operator T_P which can be associated with P and is analogous to the operator Φ discussed in Example 1; moreover T_P provides a relatively simple way of obtaining M_P. Again, we will consider these issues by reference to a simple example as follows.

Example 2 Consider the program P:

$$
\begin{gathered}
q(b) \leftarrow \\
q(s(y)) \leftarrow q(y) \\
p(s(s(x))) \leftarrow p(a), q(x)
\end{gathered}
$$

which does not compute anything significant but is manageable and illustrates the main ideas. We start by observing that the underlying first order language $\mathcal{L}$ for this example contains just the following: constant symbols a, b; variable symbols x, y; a unary function symbol s; unary predicate symbols p, q. Let

$$U_P = \{s^m(a), s^n(b); m, n \in N\}$$

denote the set of all ground terms which can be formed using the symbols s, a, b, where s^n is informal shorthand for n occurrences of s; U_P is called the *Herbrand universe* for $\mathcal{L}$. Similarly, let

$$B_P = \{p(t), q(t'); t, t' \in U_P\}$$

denote the set of all ground atoms which can be formed using the symbols p, q and ground terms from U_P; B_P is called the *Herbrand base* for $\mathcal{L}$. There are canonical interpretations for $\mathcal{L}$, called *Herbrand interpretations*, which can be constructed out of the elements of $\mathcal{L}$ as follows: the constant symbols a, b in $\mathcal{L}$ are assigned to themselves in U_P; the mapping $U_P \to U_P$ defined by $t \mapsto s(t)$ of arity one is assigned to the unary function symbol s; since we are working in classical two valued logic, we assign a unary relation I^p on B_P (i.e. a subset of B_P) to the unary predicate symbol p and likewise a unary relation I^q to q to obtain the interpretation $I^p \cup I^q$. Since the assignment to constant symbols and function symbols is fixed, Herbrand interpretations I can be identified with subsets I of B_P by: ground atom $p(t)$ is *true* relative to I, written $I \models p(t)$, iff $p(t) \in I$; ground atom $q(t')$ is *true* relative to I, again written $I \models q(t')$, iff $q(t') \in I$. In this way, the set of all Herbrand interpretations for $\mathcal{L}$ can be identified with the power set $\mathcal{P}(B_P)$ which we will henceforth write as I_P. The set I_P we will regard as a complete lattice relative to the partial order of set inclusion whose bottom element is the empty set, and in which the infimum and supremum of an arbitrary collection of elements (subsets of B_P) are the intersection and union respectively of the collection. It is this complete lattice which is the domain of the operator T_P and is the usual domain on which fixed-point semantics is carried out for logic programs. Let us note therefore that, in general, this operator is defined by $T_P : I_P \longrightarrow I_P$ where

$$T_P(I) =$$
$$\{A \in B_P;\ \text{there is a ground instance } A \leftarrow B_1, B_2, \ldots, B_n$$
$$\text{of a clause in } P \text{ satisfying} I \models B_1 \wedge B_2 \wedge \ldots \wedge B_n\}$$

(a ground instance of a program clause is simply a clause containing no variable symbols, so that elements of U_P have been assigned to each variable symbol). In practice, $T_P(I)$ is obtained by matching all the atoms in a given clause body with elements of I and collecting up corresponding clause heads. For example, with

$$I = \{p(a), p(s(a)), q(a), q(s(a)), q(b)\}$$

in our present example, we get

$$T_P(I) = \{p(s^2(a)), p(s^3(a)), p(s^2(b)), q(s(a)), q(s^2(a)), q(b), q(s(b))\}.$$

All the ideas presented in this example carry over completely to the case of an arbitrary program P in which all clauses are definite, a *definite* program. Now, a central fact emerges concerning T_P, *the immediate consequence operator* to give it its name, which is that T_P is *lattice-continuous* in the sense that $T_P(\sup(X_\alpha)) = \sup(T_P(X_\alpha))$ for every directed family (X_α) of subsets of I_P, where $\sup(X_\alpha)$ denotes the supremum of (X_α); this property of T_P is the analogue of recursiveness in the case of the operator Φ in Example 1. Once more, least fixed points of such operators play a fundamental role and the facts in brief are as follows. We inductively form the chain (I_n) in I_P by: $I_0 = \phi$ and $I_{n+1} = T_P(I_n)$, just as for Kleene's theorem, and take $\sup(I_n)$, which is often denoted $T_P \uparrow \omega$. This time we apply an abstract form of Kleene's first recursion theorem, due to Tarski, see [38] and also [18]. We obtain that $T_P \uparrow \omega$ is the least fixed point, $\mathrm{lfp}(T_P)$, and the following theorem due to van Emden and Kowalski, see [19, 39], shows the importance of this fixed point.

Theorem 4. *For any definite logic program P, we have $M_P = T_P \uparrow \omega = lfp(T_P)$.* ■

Carrying out the construction described above in the case of Example 2 shows that

$$M_P = T_P \uparrow \omega = \{q(b), q(s(b)), q(s^2(b)), \ldots\},$$

as is readily checked, and the elements of this set are exactly those ground atoms which P computes.

5. The topological viewpoint

Despite the fact that definite logic programs T_P can compute all computable functions, there is a need to extend syntax to make them more expressive. This means that we want to allow negative literals in the bodies of clauses (and hence arbitrary first order formulae). Once that is done, however, T_P fails to be monotonic and hence fails to be lattice-continuous (monotonicity is an easy consequence of lattice continuity of T_P or of recursiveness in the case of the operator Φ) so that the standard approach discussed in §4 does not apply. A partial remedy is to consider syntactic devices such as stratification and local stratification, see [5]. Nevertheless, the problem arises of finding fixed points of non-monotonic operators on I_P, and in this section we sketch methods being developed by us in [31, 32, 33] to solve this problem using topological notions and in particular quasi-metrics.

The following definition can be found in [27, 35].

Definition 3 Let X be a non-empty set. A *quasi-metric* on X is a map from $X \times X$ to the non-negative real numbers including $+\infty$ satisfying:
1. $d(x,x) = 0$;
2. $d(x,y) \le d(x,z) + d(z,y)$;
3. if $d(x,y) = d(y,x) = 0$, then $x = y$.
A quasi-metric d is called an *ultra*-quasi-metric if it satisfies the strong triangle inequality
2′. $d(x,y) \le \max\{d(x,z), d(z,y)\}$.

Notice that $d(x,y)$ and $d(y,x)$ are different in general. Quasi-metrics have been used in program semantics (for procedural programs) to reconcile the two standard approaches (Scott domains and metric spaces) to solving recursive domain equations. They can be viewed as categories enriched over the unit interval $[0,1]$, see [8], and this observation permits the development of many of their basic properties following ideas of W. Lawvere.

Given a quasi-metric d on X, there is an associated metric $d^\star$ defined on X by $d^\star(x,y) = \max\{d(x,y), d(y,x)\}$. One then says that (X,d) is *totally bounded* if the metric space $(X,d^\star)$ is totally bounded. Moreover, d *induces* a natural topology on X in which a set O is called *open* if, for every $x \in O$, some ϵ-ball $B(\epsilon,x)$ (where $B_\epsilon = \{y \in X; d(x,y) < \epsilon\}$) is contained in O.

The two examples which follow are taken from [35].

Example 3 Let $(D,\le)$ be an arbitrary partially ordered set and define d on $D \times D$ by

$$d(x,y) = \begin{cases} 0 & \text{if } x \le y; \\ 1 & \text{otherwise.} \end{cases}$$

Then d is an ultra-quasi-metric, called the *discrete quasi-metric*, which induces the Alexandroff topology and moreover (D,d) is totally bounded iff D is finite.

Example 4 Let $(D,\le)$ be any Scott domain, let B_D denote the set of compact elements of D and let $r : B_D \to N$ be a map (a rank function) such that $r^{-1}(n)$ is a finite set for each $n \in N$. Define d on $D \times D$ by

$$d(x,y) = \inf\{2^{-n}; e \le x \Rightarrow e \le y \text{ holds for every } e \text{ of rank } \le n\}.$$

Then d is an ultra-quasi-metric which induces the Scott topology of D and (D,d) is totally bounded.

Definition 4 A sequence (x_n) in the quasi-metric space (X,d) is said to be *forward Cauchy* if, for each $\epsilon > 0$, there is a natural number k such that $d(x_l, x_m) \le \epsilon$ whenever $k \le l \le m$.

Definition 5 Let (x_n) be a forward Cauchy sequence in a quasi-metric space (X,d). A point $x \in X$ is a *Limit* of (x_n), written $x = \operatorname{Lim} x_n$, if, for every $y \in X$, we have $d(x,y) = \lim_{n\to\infty} d(x_n,y)$. The space X is said to be *complete* if every forward Cauchy sequence in X has a Limit.

The forward Cauchy property of the sequence (x_n) implies that the sequence $d(x_n,y)$ is itself Cauchy in the real line, so that the definition just given is meaningful. Moreover, Limits of forward Cauchy sequences are unique when they exist.

Definition 6 Let (X,d) be a quasi-metric space and suppose $f : X \to X$ is a mapping.
1. f is *non-expansive* if, for all $x,y \in X$, we have $d(f(x),f(y)) \le d(x,y)$.
2. f is *contractive* if there exists a positive number $c < 1$ such that, for all $x,y \in X$, we have $d(f(x),f(y)) \le c.d(x,y)$.
3. f is *Continuous* if, for all forward Cauchy sequences (x_n) and x in X, we have $\operatorname{Lim} f(x_n) = f(x)$ whenever $\operatorname{Lim} x_n = x$.

The following theorem is due to Jan Rutten, [27, Theorem 3.7].

Theorem 5. *Let (X,d) be a complete ultra-quasi-metric space and suppose $f : X \to X$ is non-expansive.*

1. If f is Continuous and there is an x in X with the property that $d(x,f(x)) = 0$, then f has a fixed point which is the least fixed point above x in the order $\le_X$ defined by $y \le_X z$ iff $d(y,z) = 0$.

2. If f is Continuous and contractive, then f has a unique fixed point. ■

Attempts to use the Banach contraction mapping theorem in logic programming have been made with some success in [12], and in [17] where problems arising out of attempts to formalize common sense reasoning are considered. Nevertheless, it is our claim that it is quasi-metrics that should be used instead, in conjunction with theorems such as Theorem 5. This point of view is substantiated by the following two observations: (i) The topology underlying the declarative semantics of definite programs is the Scott topology, see [32], which is not metrizable. This means that it is impossible to recover the classical theory of §4 with metrics. (ii) It is not usual for T_P to have unique fixed points (rather, the set of such forms a complete lattice) and this means that in general T_P is not a contraction relative to any metric. To finish this paper, we therefore briefly indicate how quasi-metrics can be used in logic programming.

First, consider an arbitrary definite logic program P and view I_P as a partially ordered set, under set inclusion, endowed with the discrete quasi-metric defined in Example 3. The following facts are established in [33]:

1) A sequence (I_n) in I_P is forward Cauchy iff it is eventually increasing.

2) (I_P, d) is complete.

3) The following are equivalent for any forward Cauchy sequence (I_n) in (I_P, d)

a) $\mathrm{Lim}\, I_n = I$.

b) $I_n \to I$ in the Scott topology and I is the greatest limit (in the Scott topology) of (I_n).

4) If (I_n) is a forward Cauchy sequence in (I_P, d), then $(T_P(I_n))$ is also a forward Cauchy sequence.

5) T_P is Continuous relative to d.

6) T_P is non-expansive relative to d.

Noting that the empty set ϕ satisfies $d(\phi, T_P(\phi)) = 0$, we can apply Rutten's theorem and, on examining its proof, we conclude that T_P has a fixed point equal to $\mathrm{Lim}\, T_P^n(\phi)$. This fixed point is, by Observation 3 above, equal to $gl(T_P^n(\phi))$ as defined in [32] and this, in turn is equal to $\bigcup T_P^n(\phi)$, by [32, Proposition 8]. In this way, we recover the classical least fixed point of T_P and Theorem 4 follows immediately from this. ■

For our second and final application let P denote an arbitrary, not necessarily definite, program. This time we will think of I_P as a Scott domain (i.e. a bounded-complete ω-algebraic cpo) under set inclusion whose compact elements are the finite sets, the collection of which we will denote by B_D. We define a *level mapping* for P to be a function $l : B_P \to N$, and we assume that $l^{-1}(n)$ is a finite set for every n. Such mappings have found application in several places in logic programming including uses in defining stratification, in questions of termination of logic programs, and in treating completeness issues. Given a level mapping l we define the function $r : B_D \to N$ by $r(I) = \max_{A \in I}(l(A))$, for nonempty I, and set $r(\phi) = 0$. We will call r the *rank* function determined by l. Now let d denote the quasi-metric defined as in Example 4 so that (I_P, d) is complete and totally bounded, and d induces the Scott topology on I_P. The central facts we need, established in [33], concern the connection between quasi-metric notions and corresponding ones in the Cantor topology on I_P (this latter topology is denoted by Q in [32]) and are as follows:

1) For a sequence (I_n) in I_P and $I \in I_P$, the following statements are equivalent.

a) $I_n \to I$ in the topology Q.

b) (I_n) is forward Cauchy, $I_n \to I$ in the Scott topology and $I = gl(I_n)$, the greatest limit of (I_n).

2) Let (I_n) be a forward Cauchy sequence in (I_P, d). Then $\mathrm{Lim}\, I_n = I$ iff $I_n \to I$ in Q.

3) If T_P is non-expansive relative to d, then it is continuous in the topology Q.

4) T_P is Continuous relative to d iff it is continuous in the topology Q.

Once again it will be best to illustrate these ideas by considering them in relation to a simple example, as follows.

Example 5 Let P be the program:

$$p(o) \leftarrow$$

$$p(s(x)) \leftarrow \neg p(x)$$

This program is perhaps "intended" to compute the even natural numbers ($p(x)$ can be interpreted to mean "x is even", s can be interpreted to be the successor function). This program is not definite and is neither stratified nor locally stratified, so that the standard approach does not apply. Define the level mapping l on B_P by $l(p(s^n(o))) = n$ for each n. We note that in this case T_P is not non-expansive for if we take

$$I_1 = \{p(o), p(s(o))\}$$

and

$$I_2 = \{p(o), p(s(o)), p(s^2(o))\},$$

then

$$T_P(I_1) = \{p(o), p(s^3(o)), p(s^4(o)), p(s^5(o)), \ldots\}$$

and

$$T_P(I_2) = \{p(o), p(s^4(o)), p(s^5(o)), \ldots\}.$$

Thus, we have $d(I_1, I_2) = 0$ and yet $d(T_P(I_1), T_P(I_2)) = 2^{-2}$. Consider powers $I_n = T_P^n(\phi)$, the first few of which are as follows: $I_1 = B_P$, $I_2 = \{p(o)\}$, $I_3 = B_P \setminus \{p(s(o))\}$, $I_4 = \{p(o), p(s^2(o))\}$, $I_5 = B_P \setminus \{p(s(o)), p(s^3(o))\}$, etc. Using [33, Proposition 7] we obtain that $d(I_n. I_{n+1})$ takes value 0 if n is even and takes value 2^{-n+1} if n is odd. This is enough to show that the sequence (I_n) is forward Cauchy and therefore converges to I, say, in Q. By [32, Proposition 4] it is clear that (I_n) converges in Q to the set $\{p(o), p(s^2(o)), p(s^4(o)), \ldots\}$ which therefore coincides with I. Since T_P is continuous in Q by [32, Corollary 6], it follows that I is a fixed point of T_P by a simple argument using the uniqueness of limits in Q. Thus, the set I of "even natural numbers" is a model of P. In fact, it is not hard to see that I is the only fixed point of T_P. ■

References

[1] The Alvey Programme of Advanced Information Technology. Alvey Directorate: Millbank Tower, Millbank, London SW1P 4QV, U.K.

[2] Research in Logic for Information Technology: Logic for IT. Science and Engineering Research Council: Polaris House, North Star Avenue, Swindon, Wiltshire, U.K.

[3] S. Abramsky, D. M. Gabbay and T. S. E. Maibaum (eds.), Handbook of Logic in Computer Science, Volumes 1 to 6. Oxford Science Publications, Oxford University Press: Oxford, 1994.

[4] K. R. Apt, *Logic programming*, *in* Handbook of Theoretical Computer Science, Volume B: Formal Models and Semantics, (ed.) J. van Leeuwen, 493-574. Elsevier Science Publishers: Amsterdam, 1990.

[5] K. R. Apt, H. A. Blair and A. Walker, *Towards a theory of declarative knowledge*, *in* Foundations of Deductive Databases and Logic Programming, (ed.) J. Minker, 89-148. Morgan Kaufmann Publishers Inc.: Los Altos, 1988.

[6] K. R. Apt and M. H. van Emden, *Contributions to the theory of logic programming*, J. ACM **29** (1982), 841-862.

[7] J. Barwise (ed.), Handbook of Mathematical Logic. North-Holland: Amsterdam, 1977.

[8] M. M. Bonsangue, F. van Breugel and J. J. J. M. Rutten, Generalized ultrametric spaces: completion, topology, and powerdomains via the Yoneda embedding, Technical Report CS-R9560, Centrum voor Wiskunde en Informatica, Amsterdam, 1995.

[9] I. Bratko, Prolog Programming for Artificial Intelligence. International Computer Science Series, Addison-Wesley Publishing Company: 1988.

[10] A. Colmerauer, H. Kanoui, P. Roussel and R. Pasero, Un système de communication homme-machine en franąis, Groupe de recherche en intelligence artificielle, Université d'Aix-Marseille, 1973.

[11] N. Cutland, Computability: An Introduction to Recursive Function Theory. Cambridge University Press: Cambridge, 1980.

[12] M. C. Fitting, *Metric methods: three examples and a theorem*, J. Logic Programming **21** (1994), 113-127.

[13] D. M. Gabbay, C. J. Hogger and J. A. Robinson (eds.), Handbook of Logic in Artificial Intelligence and Logic Programming, Volumes 1 to 5. Oxford Science Publications, Oxford University Press: Oxford, 1994.

[14] M. Gelfond and V. Lifschitz, *Classical negation in logic programs and disjunctive databases*, New Generation Computing **9** (1991), 365-385.

[15] Y. Gurevich, *The value, if any, of decidability*, Bull. European Association for Theoretical Computer Science **55** (1995), 129-135.

[16] T. C. Hurley, *Benefits and advantages of an integrated mathematics and computer science degree*, Irish Math. Soc. Bulletin **32** (1994), 63-72.

[17] M. A. Khamsi, V. Kreinovich and D. Misane, *A new method of proving the existence of answer sets for disjunctive logic programs: a metric fixed point theorem for multi-valued mappings*, *in* Proceedings of the Workshop on Logic Programming with Incomplete Information, Vancouver, B.C., Canada, October 1993, pp. 58-73.

[18] J-L. Lassez, V. L. Nguyen and E. A. Sonenberg, *Fixed point theorems and semantics: a folk tale*, Information Processing Letters **14** (1982), 112-116.

[19] J. W. Lloyd, Foundations of Logic Programming (second edition). Springer-Verlag: Berlin, 1988.

[20] D. W. Loveland, Automated Theorem Proving: A Logical Basis. North Holland: New York, 1978.

[21] P. Odifreddi, Classical Recursion Theory. North-Holland: Amsterdam, 1992.

[22] D. Park, *Fixpoint induction and proof of program properties*, *in* Machine Intelligence Volume 5, (eds.) B. Meltzer and D. Michie, 59-78. Edinburgh University Press: Edinburgh, 1970.

[23] L. C. Paulson, Logic and Computation. Cambridge Tracts in Theoretical Computer Science No. 2, Cambridge University Press: Cambridge, 1987.

[24] J. A. Robinson, *A machine oriented logic based on the resolution principle*, J. ACM **12** (1965), 23-41.

[25] J. A. Robinson, Logic, Form and Function: The Mechanization of Deductive Reasoning. Edinburgh University Press: 1979.

[26] H. Rogers, Theory of Recursive Functions and Effective Computability. MIT Press: Cambridge, Mass., 1987.

[27] J. J. M. M. Rutten, Elements of generalized ultrametric domain theory, Technical Report CS-R9507, Centrum voor Wiskunde en Informatica, Amsterdam, 1995.

[28] D. S. Scott, *Data types as lattices*, SIAM J. Computing **5** (1976), 522-587.

[29] D. S. Scott, *Lectures on a mathematical theory of computation*, *in* Theoretical Foundations of Programming Methodology, (eds.) M. Broy and G. Schmidt, 145-292. Reidel: Dordrecht, 1982.

[30] D. S. Scott, *Domains for denotational semantics*, *in* Proceedings 9th International Colloquium on Automata, Languages and Programming, (eds.) M. Nielsen and E. M. Schmidt, 577-613. Lecture Notes in Computer Science Volume 140, Springer-Verlag: Berlin-Heidelberg-New York, 1982.

[31] A. K. Seda, *Some applications of general topology to the semantics of logic programs*, Bull. European Association for Theoretical Computer Science **52** (1994), 279-292.

[32] A. K. Seda, *Topology and the semantics of logic programs*, Fundamenta Informaticae **24** (1995), 359-386.

[33] A. K. Seda, Quasi-metrics and the semantics of logic programs, Fundamenta Informaticae, to appear.

[34] S. G. Shanker (ed.), Gödel's Theorem in Focus. Croom Helm Ltd.: Kent, 1988.

[35] M. B. Smyth, *Totally bounded spaces and compact ordered spaces as domains of computation*, *in* Topology and Category Theory in Computer Science, (eds.) G. M. Reed, A. W. Roscoe and R. F. Wachter, 207-229. Oxford University Press: Oxford, 1991.

[36] M. B. Smyth and G. D. Plotkin, *The category-theoretic solution of recursive domain equations*, SIAM J. Computing **11** (1982), 761-783.

[37] V. Stoltenberg-Hansen, I. Lindström and E. R. Griffor, Mathematical Theory of Domains. Cambridge Tracts in Theoretical Computer Science No. 22, Cambridge University Press: Cambridge, 1994.

[38] A. Tarski, *A lattice-theoretical fixed point theorem and its applications*, Pacific J. Math. **5** (1955), 285-309.

[39] M. H. van Emden and R. A. Kowalski, *The semantics of predicate logic as a programming language*, J. ACM **23** (1976), 733-742.

[40] J. van Leeuwen (ed.), Handbook of Theoretical Computer Science, Volumes A & B. Elsevier Science Publishers: Amsterdam, 1990.

[41] D. H. D. Warren and F. C. N. Pereira, An efficient easily adaptable system for interpreting natural language queries, DAI Research Paper No. 155, Department of Artificial Intelligence, University of Edinburgh, 1981.

[42] J. Woodcock and M. Loomes, Software Engineering Mathematics. Pitman Publishing: London, 1988.

A. K. Seda
Department of Mathematics,
University College,
Cork,
Ireland.
email:aks@bureau.ucc.ie

Book Review

Groups '93
Galway/ St Andrews

London Mathematical Society Lecture Note Series,
vols. 211 & 212

Ed. by C. M. Campbell, T. C. Hurley, E. F. Robertson,
S. J. Tobin & J. J. Ward

Cambridge University Press 1995
xii+304pp (vol. 1), xii+305pp (vol. 2)
ISBN 0-521-47749-2 (vol. 1), 0-521-47750-6 (vol. 2)

Reviewed by Rod Gow

The volumes under review contain selected papers from a conference on group theory held at University College Galway during the period 1-14 August 1993. This conference was the continuation of a series of conferences on group theory held at the University of St Andrews in 1981, 1985 and 1989, with the next conference to be held in Bath in 1997. There were 285 participants at the conference, with numerous principal lectures, invited lectures, research talks and workshops on computational group theory to entertain them.

It seems to the reviewer that large scale conferences devoted to a rather broad theme are less common these days than once they were. In group theory, conferences on groups of Lie type, representation theory of algebraic and related finite groups, groups and geometry, or computational group theory are dominant. This probably reflects the fact that researchers' interests are more narrowly focused on their specialities and they may imagine that there is a better chance of a pay-off in terms of a publication by attending conferences offering a concentrated diet of specialized material. Looking through the papers under review, I noticed that many topics popular 25 years ago are no longer represented. These include finite simple groups, ordinary character theory and permutation groups. This is predictable, given the success of the the classification of finite simple groups, although a revisionist school of mathematicians, devoted to improved and more convincing proofs of theorems and constructions in these areas, has come into existence.

I would always expect to find some novelties of an unexpected nature among the contributed papers and, in this case, I was not disappointed. Obviously, different people will respond to different themes but I enjoyed finding out about the existence of a group G that is a non-split extension of a free abelian group of rank 3 by $\mathrm{SL}_3(\mathbf{Z})$ which is not residually finite and for which the associated 2-cocycle has infinite order. The relevant paper is *An army of cohomology against residual finiteness* by P. R. Hewitt (pp 305-313). Another paper that interested me was *An invitation to computational group theory* by J. Neubüser. Neubüser arranged a workshop on computational group theory (CGT) and the use of the GAP system during the second week of the conference and the paper reflects his thoughts on CGT. He describes problems that may be studied by using GAP, mentions some of the history and triumphs of CGT, and finishes by expressing his concerns about the future of CGT and the value in which it is held. It is clearly annoying to find all the hard work put into creating CAYLEY or GAP often ignored by researchers who take for granted the existence of these CGT packages. The paper includes a substantial bibliography.

Five main lecture courses, consisting of about five lectures each, were given by J. L. Alperin, M. Broué, P. H. Kropholler, A. Lubotzky and E. I. Zelmanov, and articles based on their lectures are presented in the proceedings. The article by Lubotzky, *Counting finite index subgroups*, contains a large amount of information, and should make worthwhile reading for the enthusiast or the enquiring novice. A memoir on subgroup growth, prepared by Lubotzky as a background for his lectures, was made available by the Mathematics Department in Galway. A paper by A. Shalev, *Some problems and results in the theory of pro-p groups*, relates well to Lubotzky's paper, and also to that of Zelmanov (*Lie ring methods in the theory of nilpotent groups*). Zelmanov's paper

touches briefly on his solution to the restricted Burnside problem, for which he was to receive a Field's medal in 1994.

The editors of the proceedings have worked hard to obtain a uniform format for the published papers. Often conference proceedings consist only of photocopies of manuscripts, with the end-products of various unpleasant word processing systems lying discordantly side by side. This is not the case here. I did not notice many glaring typos, although I did see the name Heisenberg rendered as Heizenberg twice. I think these proceedings are something perhaps to be browsed at by interested parties, rather than purchased outright. They are well produced and give some idea of certain current interests in group theory, without really touching on several of the leading research topics.

Rod Gow,
Department of Mathematics,
University College Dublin.

INSTRUCTIONS TO AUTHORS

The Bulletin is typeset with TEX. Authors should if possible submit articles to the Bulletin as TEX input files; if this is not possible typescripts will be accepted. Manuscripts are not acceptable.

Articles prepared with TEX

Though authors may use other versions of TEX, It is preferred that they write plain TEX files using the standard IMS layout files. These files can be received by sending an e-mail message to `listserv@irlearn.ucd.ie`. The body of the message should contain the three lines:

```
get imsform tex
get mistress tex
get original syn
```

Instructions on the use of these is contained in the article on *Directions in Typesetting* in issue number 27, December 1991.

The TEX file should be accompanied by any non-standard style or input files which have been used. Private macros, reference input files and both METAFONT and TEX source files for diagrams should also accompany submissions.

The input files can be transmitted to the Editor either on an IBM or Macintosh diskette, or by electronic mail to the following Bitnet or EARN address:

RODGOW@IRLEARN.UCD.IE

Two printed copies of the article should also be sent to the Editor.

Other Articles

Authors who prepare their articles with word processors can expedite the typesetting of their articles by submitting an ASCII input file as well as the printed copies of the article.

Typed manuscripts should be double-spaced, with wide margins, on numbered pages. Commencement of paragraphs should be clearly indicated. Hand-written symbols should be clear and unambiguous. Illustrations should be carefully prepared on separate sheets in black ink. Two copies of each illustration should be submitted: one with lettering added, the other without lettering. Two copies of the manuscript should be sent to the Editor.