IRISH MATHEMATICAL SOCIETY

NEWSLETTER

No. 4 1981

CONTENTS

NEWS

The sudden death of Dr. J.J. McMahon in September shocked the Irish mathematical community. Dr. McMahon was formerly Professor of Mathematics at Maynooth, and also spent some years teaching in Africa. His most recent position was at Thomond College Limerick, and he was currently on the committee of the Irish Mathematical Society.

Dr. Richard Aron is at present on leave of absence from T.C.D. He is spending the 1981-82 academic year at Kent State University.

Dr. J. Dudziak (Indiana) is replacing Richard Aron at T.C.D. for 1981-82. His field of interest is Spectral Theory and Functional Analysis.

Dr. M. Klimek has taken up a Dept. of Education Post-Doctoral position at T.C.D. Dr. Klimek is from Krakov (Poland) and works in Potential Theory.

Professor Sean Tobin (U.C.G.) is spending the academic year 1981-82 at the University of Freiburg (Germany).

Dr. Gareth Thomas (Bristol) has joined the Mathematical Physics Dept. at U.C.C. Dr. Thomas works in Fluid Mechanics.

Dr. Gordon Lessells has taken up a position at N.I.H.E.(Limerick). His field of interest is Analysis. Last year, Dr. Lessells was at U.C.C.

Dr. Michael Clancy has joined the Mathematics Department at N.I.H.E. (Dublin).

Mr. Paul Barry has joined the staff of the Regional Technical College, Waterford.

Dr. Ralph Saxton has left U.C.D. Mathematical Physics Dept. to take up a position at Brunel University, London.

Dr. David Reynolds has joined the Mathematical Physics Dept. at U.C.D. His field of research is Continuum Mechanics.

Dr. Brian Smyth (Notre Dame) and Dr. Benedict Seifert (I.H.E.S., Paris) have joined the Mathematics Department at U.C.D. Dr. Smyth works in Differential Geometry and Dr. Seifert works in Group Representations.

Dr. Kasia Woloszynska (Warsaw) is spending the year at U.C.D. Mathematical Physics Dept. Dr. Woloszynska works in Continuum Mechanics, and is on an N.B.S.T. Fellowship. Dr. Emmanuel Buffet (Paris) and Dr. Grainne O'Brien have taken up Department of Education Post-Doctoral Fellowships. Dr. Buffet works in Statistical Mechanics and Dr. O'Brien in General Relativity.

Dr. Norman Fenton (Sheffield) has taken up a Department of Education Post-Doctoral Fellowship at U.C.D. Mathematics Department. His field of research is Matroids and Commutative Algebra.

Professors T.J. Laffey (U.C.D.) and A.G. O'Farrell (Maynooth) were elected to membership of the Royal Irish Academy in March.

Seán Dineen

MOTION FOR CHANGE IN RULES OF IRISH MATHEMATICAL SOCIETY

(Proposed by Committee)

RULE 1

Current : Every ordinary member shall pay, on election to membership and on the first day of October in each succeeding session an annual subscription to be determined by the Committee.

Proposed : Every ordinary member shall pay, on application for membership and during the month of January in each succeeding session an annual subscription to be determined by the Committee. A change in the annual subscription shall be ratified by a meeting of the Society.

RULE 4

Current : The term of office shall be two years in the case of the President and Vice-President.

The President and Vice-President may not continue in office for more than two consecutive terms.

Proposed : The term of office of the office-bearers and of the Committee shall be two years.

RULE 5

Current : The additional members of the Committee shall be elected annually as shall the Treasurer and Secretary at the first ordinary meeting of each session.

Proposed : On alternate years, elections for the following positions will take place

(a) President, Vice-President and one half the additional members of the Committee;

(b) Secretary, Treasurer and one half the additional members of the Committee.

GALWAY GROUP THEORY CONFERENCE

The annual I.M.S. Mini-conference on Group Theory was held in U.C.G. in May. The speakers were Dr. John Lennox (Cardiff), Professor Sean Tobin, Dr. Michael Barry and Dr. Johannes Siemons. Each year, this is a most enjoyable and informative get-together of the algebraists in the country and Professor Martin Newell and his colleagues warmly deserve our gratitude for organising it (and performing the annual miracle with the weather).

DUBLIN INSTITUTE FOR ADVANCED STUDIES

CHRISTMAS SYMPOSIUM

Monday and Tuesday, 21st and 22nd December 1981

MAIN TALKS

MONDAY

Dr. A.I. Solomon (Open University) "Applications of Lie Algebras to Many-Body Problems".

TUESDAY

Dr. D. McCrea (U.C.D.) "The Structure of Singularities in Space-Time".

Prof. A.G. O'Farrell (Maynooth) "The Approximation of Functions of Two Variables by Sums of Functions of One Variable".

Dr. R.S. Ward (T.C.D.) " PDEs and Geometry: Weierstrass, Whittaker and Yang-Mills Monopoles".

COMPEL

THE INTERNATIONAL JOURNAL FOR COMPUTATION AND MATHEMATICS IN ELECTRICAL AND ELECTRONIC ENGINEERING

AIMS AND SCOPE

COMPEL exists for the discussion and dissemination of numerical and analytical methods in all areas of electrical and electronic engineering. The main emphasis of the papers is on the methods. Applications of methods to particular engineering problems may be given to illustrate their use in practice.

IRISH NATIONAL MATHEMATICS CONTEST

The contest was held in March and was very successful, the number entering having again increased, and returns were received on behalf of over 1,600 students. This year's winner, Seamus Moran, of O'Connell School, Dublin, achieved the highest mark attained in the contest here so far. The contest was supported by the Educational Company of Ireland, the Irish Mathematics Teachers Association and the Irish Mathematical Society.

IRISH NATIONAL MATHEMATICS CONTEST 1981

Individual Roll of Honour

SCORE	*STUDENT*	*SCHOOL*	*COUNTY*
114	Seamus Moran	O'Connell School	Dublin
100	Gerard Lawless	Blackrock College	Dublin
99	Terri Raftery	St. Joseph's, Glenamaddy	Galway
94	Stephen Doyle	Belvedere College	Dublin
94	Mary Garvey	St. Joseph's, Glenamaddy	Galway
91	Donal Hayes	Col. an Spioraid Naoimh	Cork
90	Deirdre Grady	St. Joseph's, Glenamaddy	Galway
89	Balfour Lambert	Newpark Comprehensive, Blackrock	Dublin
89	Michael Lynch	Col. an Spioraid Naoimh	Cork
88	Stephen Ming Tsang	Col. an Spioraid Naoimh	Cork
88	Michael Moriarty	Christian Bros. College	Cork
88	Derek O'Leary	Col. an Spioraid Naoimh	Cork
86	David Butler	Belvedere College	Dublin
86	James Cunnane	Christian Bros. College	Cork
86	Jonathan O'Connor	Blackrock College	Dublin
85	John Geoghegan	O'Connell School	Dublin
85	Naveen Goswami	Sandymount High School	Dublin
85	Aidan Kerins	O'Connell School	Dublin
85	Fintan Lucy	Presentation Bros. College	Cork
84	John Hegarty	St. Colman's College, Claremorris	Mayo
84	Rory Murray	Oatlands College, Stillorgan	Dublin
84	Brendan O'Connor	O'Connell School	Dublin
84	Padraig Quill	St. Munchin's College	Limerick
83	Joe Collins	St. Kieran's College	Kilkenny
83	Colin Hassett	Presentation Bros. College	Cork
82	Fergus Coakley	Presentation Bros. College	Cork
82	Declan Keegan	Presentation Bros. College	Cork
82	Patrick O'Brien	Presentation Bros. College	Cork
82	Brendan Walsh	Presentation Bros. College	Cork
82	Ronan Boland	Col. an Spioraid Naoimh	Cork
82	Cormac Conroy	Col. an Spioraid Naoimh	Cork
82	Sharon Reid	Sligo Grammar School	Sligo

SCORE	*STUDENT*	*SCHOOL*	*COUNTY*
81	Francis Cagney	St. Munchin's College	Limerick
81	Sean Coffey	Oatlands College, Stillorgan	Dublin
81	Martin Cosgrove	Christian Bros. School Dundalk	Louth
81	Gerard Garvey	O'Connell School	Dublin
81	Tomas Jones	Christian Bros. School Enniscorthy	Wexford
80	Paraic Begley	Christian Bros. School Dundalk	Louth
80	Sheung Ming Chu	St. Mary's College, Dundalk	Louth
80	Eugene Cosgrave	Col. Iognaid Ris, Deerpark	Cork
80	Peter Finnegan	Beneavin College, Finglas	Dublin
80	Mervyn Lang	Bandon Grammar School	Cork
80	Brian Martin	Beneavin College, Finglas	Dublin
80	Jim Quigley	Marian College, Ballsbridge	Dublin
80	Finbar Sheehy	St. Kieran's College	Kilkenny

SCHOOL ROLL OF HONOUR

SCORE	*SCHOOL*	*Team (Top 3)*
284	O'Connell School, Dublin 1	Seamus Moran John Geoghegan Aidan Kerins
283	St. Joseph's, Glenamaddy, Co. Galway	Terri Raftery Mary Garvey Deirdre Grady
268	Colaiste an Spioraid Naoimh, Cork	Donal Hayes Michael Lynch Stephen Ming Tsang/ Derek O'Leary
263	Blackrock College, Blackrock, Co. Dublin	Gerard Lawless Jonathan O'Connor John Rafter
256	Belvedere College, Dublin 1	Stephen Doyle David Butler David Boushel/ Michael Higgins/ Paul Timmons

INTERNATIONAL MATHEMATICAL OLYMPIAD

The 1981 International Mathematical Olympiad was held in the U.S. in July. This is the first time the event has been held in the Western Hemisphere. Twenty-seven nations competed. The U.S.A. won, four of their team (of eight) actually achieved perfect scores. Ireland has yet to compete in the olympiad. Many countries use their National Mathematics Contest as a qualification for their olympiad team. This could easily be done here also, the difficulty being to obtain sponsorship to then pay for the team's transportation to the olympiad venue, etc. Hopefully, when the recession ends such sponsorship will be forthcoming.

1981 Olympiad Questions

1. P is a point inside a given triangle ABC. D,E,F are the feet of the perpendiculars from P to the lines BC,CA,AB, respectively. Find all P for which

$$\frac{BC}{PD} + \frac{CA}{PE} + \frac{AB}{PF} \quad \text{is least.}$$

2. Let $1 \leq r \leq n$ and consider all subsets of r elements of the set $\{1,2,\ldots,n\}$. Also consider the least number in each of these subsets. $F(n,r)$ denotes the arithmetic mean of these least numbers; prove that

$$F(n,r) = \frac{n+1}{r+1} .$$

3. Determine the maximum value of m^2+n^2, where m and n are integers satisfying $m,n \in \{1,2,\ldots,1981\}$ and $(n^2 - mn - m^2)^2 = 1$.

4. (a) For which values of $n>2$ is there a set of n consecutive positive integers such that the largest number in the set is a divisor of the least common multiple of the remaining $n-1$ numbers?

(b) For which values of $n>2$ is there exactly one set having the stated property?

5. Three congruent circles have a common point O and lie inside a given triangle. Each circle touches a pair of sides of the triangle. Prove that the incentre and the circumcentre of the triangle, and the point O are collinear.

6. The function $f(x,y)$ satisfies

(1) $f(0,y) = y+1$,

(2) $f(x+1,0) = f(x,1)$,

(3) $f(x+1,y+1) = f(x,f(x+1,y))$,

for all non-negative integers x,y. Determine $f(4,1981)$.

LEAVING CERTIFICATE COURSES

The statistics on the next page concerning the number of students who attempted the Honours Leaving Certificate Course in Mathematics, Applied Mathematics, Physics and Chemistry have been compiled by Professor M.A. Hayes. They should form an interesting basis for analysis, conjecture, etc. In this connection we include here the pertinent part of the recommendation of the conferences held in April 1980 and January 1981 (organised by The Royal Irish Academy, The Manpower Consultative Committee, The National Board for Science and Technology and the Institute of Engineers of Ireland) on "Engineering Manpower for Economic Development".

SUPPLY OF STUDENTS – Implications for Second Level Education

The availability of students willing and able to undertake the necessary courses of study is an essential prerequisite to achieving the increased output of engineering manpower. As far as professional engineers are concerned it is widely accepted that the minimum necessary entrance qualification is a standard in mathematics equivalent to achieving a grade C in an honours Leaving Certificate mathematics paper of the present standard. The number achieving this qualification in 1980 was 2,504 while the number attempting the paper was 3,332. Corresponding figures for 1979 were 1,558 and 3,801. Of these 655 entered engineering courses in 1980 and 418 entered in 1979. It is clear, therefore, that to achieve an output of about 1,000, as envisaged, a considerable increase in the number of qualified applicants will be essential.

To achieve this end the Conference recommended that a programme should be initiated to double the number of boys and quadruple the number of girls taking higher mathematics and physics in the Leaving Certificate over the next ten years. This will involve definite plans to make the subjects available to a wider range of pupils particularly to girls and the removal of institutional and administrative barriers to achievement of these goals. It will also be necessary to take steps to revise and update the curricula to make the subjects more attractive while maintaining the necessary depth and rigour of treatment. In order to increase the level of understanding of technology among second level students the Conference proposed the introduction of a new Technology subject on a pilot basis.

If these goals for increased supply of suitably qualified school leavers are to be attained then the shortage of mathematics and physics teachers must be urgently examined, and resolved. It is clear that without an adequate supply of properly qualified teachers in these areas, the increased numbers will not be achieved.

It is important in the introduction of new material to the Leaving Certificate course that teachers be provided with the opportunity to undertake in-career updating courses. This is not only important in relation to providing the increased numbers required with the higher level mathematics and physics qualification, but is equally important in educating and motivating those students who will be required to undertake technician courses to meet the increased demand in that area.

Proper career guidance in schools is an important requirement if able students are to be in a position to evaluate their prospects in engineering courses. It is necessary that third level institutions and both employers and the professional bodies should ensure that career guidance teachers are in full possession of up to date information and close liaison must be maintained.

As it is inevitable that time will be required to produce increased numbers of school leavers with the necessary qualifications for engineering degree courses through developments in the second level school system, the Conference recommended that the feasibility of mounting one-year post Leaving Certificate courses to qualify for entry be investigated. Such courses already exist to a limited extent but the question to be examined is whether a course with an agreed syllabus and examination could be mounted, from which successful students could generally be admitted to third level institutions. This would obviously require agreement on content and standards in advance. Such courses would mainly be intended for students having the necessary ability in mathematics who have not had the opportunity to study the subject at higher level in the Leaving Certificate.

HONOURS	YEAR 1959		1960		1961		1962		1963		1964	
	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS
MATHEMATICS	952	38	1,115	40	1,215	56	1,364	87	1,474	71	1,740	90
APPLIED MATHEMATICS	159	0	156	0	197	0	256	3	382	2	499	1
PHYSICS	543	0	563	3	659	19	657	15	700	9	1,016	39
CHEMISTRY	545	23	624	60	715	57	796	99	934	111	960	83

HONOURS	YEAR 1965		1966		1967		1968		1969		1970	
	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS
MATHEMATICS	1,802	128	2,037	172	1,998	176	1,815	161	1,770	181	1,857	277
APPLIED MATHEMATICS	505	3	500	8	575	4	532	11	650	8	634	6
PHYSICS	1,028	31	1,225	47	1,359	60	1,452	91	2,462	108	1,509	117
CHEMISTRY	1,014	127	1,154	145	1,309	240	1,501	275	2,446	354	2,113	566

HONOURS	YEAR 1971		1972		1973		1974		1975		1976	
	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS
MATHEMATICS	1,803	314	1,925	361	1,975	389	2,046	468	2,375	558	2,727	799
APPLIED MATHEMATICS	242	0	215	4	242	1	241	3	317	14	346	9
PHYSICS	1,345	135	1,258	131	1,353	152	1,514	200	1,693	263	2,092	363
CHEMISTRY	1,813	518	1,965	637	1,883	642	2,057	770	2,251	933	2,633	1,188

	YEAR 1977		1978		1979		1980*		1981	
	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS	BOYS	GIRLS
MATHEMATICS	3,062	1,030	2,870	991	2,583	924	2,461	847		
APPLIED MATHEMATICS	392	0	322	7	319	9	362	12		
PHYSICS	2,328	398	2,286	430	2,501	482	2,478	490		
CHEMISTRY	2,898	1,396	2,778	1,588	2,827	1,519	2,982	1,868		

* By telephone from Dept. of Education

AN INTRODUCTION TO THE COMPUTATIONAL COMPLEXITY OF MATRIX OPERATIONS

by Derek O'Connor, U.C.D.

1. INTRODUCTION

Computational complexity is the study of algorithms to determine the amount of 'effort' or 'work' they require in solving problems. We associate with every problem an integer (or set of parameters) called the size of the problem. The time needed by an algorithm for solving a problem, expressed as a function of the size of the problem, is called the time complexity of the algorithm. The limiting behavior of this complexity, as the size increases, is called the asymptotic time complexity of the algorithm. There are similar definition for space complexity, the storage space needed by the algorithm. In this paper we will be concerned only with time complexity and for the remainder of the paper the word 'time' is omitted.

We need to distinguish between the inherent complexity of a problem and the complexity of an algorithm used to solve the problem. The inherent complexity of a problem of size n is the amount of time that is both necessary and sufficient to solve the problem. This time, $T^*(n)$, is usually difficult to determine and we have to be content with $T'(n)$, a lower bound on $T^*(n)$. The complexity of an algorithm, $T''(n)$, is sufficient to solve the problem and is an upper bound on $T^*(n)$. The algorithm is optimal if $T''(n) = T^*(n)$.

In this paper we concentrate on the asymptotic complexity of algorithms for matrix operations. If an algorithm solves a problem of sized n in a time $T(n) = cn^2+n$ for some constant c, we say the complexity is $O(n^2)$. hence we are interested only in the functional form of $T(n)$ for large values of n. In general a function $g(n)$ is said to be $O(f(n))$ if there exists a constant c such that $g(n) < cf(n)$ for all but some finite set of non-negative values for n.

We consider only square matrices, but many of the results hold for non-square matrices. The size of an $n \times n$ matrix is n and we wish to determine the amounts of time needed to perform the familiar operations of addition, multiplication, inversion, equation solving and determinant evaluation, with time for each operation expressed as a function of n. We assume that our computer has the usual repertoire of operators (+, -, *, /) for reals and integers and that each operator is performed in a fixed amount of time. Hence we can view the time complexity of an algorithm as the number of basic arithmetic operations it performs.

2. LOWER BOUNDS ON MATRIX OPERATIONS

A general $n \times n$ matrix has n^2 elements. Hence, any operation that involves all elements requires at least $O(n^2)$ time. The usual algorithm for matrix addition/subtraction requires n^2 additions/subtractions and is therefore optimal. The ordinary algorithm for matrix multiplication requires n^3 multiplications and $n^2(n-1)$ additions. Surprisingly, the best-known lower bound is $O(n^2)$.

3. ORDINARY MATRIX MULTIPLICATION, INVERSION AND EQUATION SOLVING ARE $O(N^3)$ OPERATIONS

Multiplication: $C = AB$ where $c_{ij} = \sum_k a_{ik} * a_{kj}$

Each c_{ij} requires n multiplications and $n-1$ additions. The total number of operations is n^3 multiplications n^3-n^2 additions. Hence the complexity of multiplication is $O(n^3)$.

Equation solving: $Ax = b$

Triangularize A using Gaussian elimination. This gives $Ux = \hat{b}$ which can be solved by Back-Substitution because U is upper-triangular. Gaussian Elimination is $O(n^3)$ and Back-Substitution is $O(n^2)$. Hence the complexity of Equation Solving is $O(n^3)$.

Inversion: $AA^{-1} = I$

This is equivalent to solving the n sets of equations $Ax_j = e_j$, $j=1,2,\ldots n$ where x_j and e_j are the j^{th} columns of A^{-1} and I respectively. This, in turn, is equivalent to solving the n sets of equations $Ux_j = \hat{e}_j$. U is computed once using Gaussian Elimination in $O(n^3)$ time, each $\hat{e}_j$ can be computed in $O(n^2)$ time, and each set of equations is solved by backsubstitution in $O(n^2)$ time. The total time is $O(n^3) + 2nO(n^2)$. Hence, Inversion is $O(n^3)$.

4. IMPROVED UPPER BOUNDS FOR MATRIX MULTIPLICATION

Lemma 1: $(M_n, +_n, \cdot_n, 0_n, I_n)$ is a ring, where M_n is the set of all $n \times n$ matrices whose elements are chosen from arbitrary ring R.

Lemma 2: Let f be a partition of an $n \times n$ matrix into four $n/2 \times n/2$ matrices, assuming n is even,

$$\text{i.e.} \quad f(a) = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$$

Then, for any matrices A and B in M_n,

$$f(A+B) = f(A) + f(B) \quad \text{and} \quad f(AB) = f(A)f(B)$$

The above lemma allows us to transform an $n \times n$ matrix with elements from source ring R into a 2×2 matrix with elements from the ring of $n/2 \times n/2$ matrices.

Strassens Algorithm for Matrix Multiplication

The product $C = AB$ of two $n \times n$ matrices can be transformed into the product of two 2×2 matrices whose elements are $n/2 \times n/2$ matrices. Thus we have

$$\begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix} = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}$$

where elements of C are defined as follows

$$\begin{aligned} C_{11} &= A_{11}B_{11} + A_{12}B_{21} \\ C_{12} &= A_{11}B_{12} + A_{12}B_{22} \\ C_{21} &= A_{21}B_{11} + A_{22}B_{21} \\ C_{22} &= A_{21}B_{12} + A_{22}B_{22} \end{aligned}$$

If we have an algorithm that computes the elements of C using m multiplications and a additions then we apply the algorithm recursively to smaller and smaller partitions until we are reduced to multiplying the elements of the underlying ring R. If the algorithm multiplies two n x n matrices in time $T_m(n)$ and n is a power of 2 ($=2^p$) then we have

$$T_m(n) \leq mT_m(n/2) + an^2/4, \quad n > 2.$$

This inequality can be used to show that $T_m(n) < kn^q$, $q = \log_2 m$, i.e., the complexity of the algorithm is $O(n^{\log m})$ and is independent of a. If $m = 8$ then the algorithm is $O(n^3)$, which is the same as ordinary matrix multiplication.

Strassen's Lemma: The product of two 2x2 matrices with elements from an arbitrary ring can be computed with 7 multiplications and 18 additions/subtractions.

Proof: Compute the elements of C = AB as follows:

Compute the products

$$\begin{aligned}
m_1 &= (a_{12} - a_{22})(b_{21} + b_{22}) \\
m_2 &= (a_{11} + a_{22})(b_{11} + b_{22}) \\
m_3 &= (a_{11} + a_{22})(b_{11} + b_{12}) \\
m_4 &= (a_{11} + a_{12} - b_{11}) \\
m_5 &= a_{11}(b_{12} - b_{22}) \\
m_6 &= a_{22}(b_{21} - b_{11}) \\
m_7 &= (a_{21} + a_{22})b_{11}
\end{aligned}$$

With these seven products compute

$$\begin{aligned}
c_{11} &= m_1 + m_2 - m_4 + m_6 \\
c_{12} &= m_4 + m_5 \\
c_{21} &= m_6 + m_7 \\
c_{22} &= m_2 - m_3 + m_5 - m_7
\end{aligned}$$

There are obviously 7 multiplications and 18 additions/subtractions. Simple algebraic manipulation, using only the ring axioms, shows that the c_{ij}'s are those required by the definition of multiplication.

This lemma leads to the following theorem.

Theorem1: Two $n \times n$ matrices with elements from an arbitrary ring can be multiplied in $O(n^{\log 7})$ arithmetic operations.

Proof: Assume $n = 2^p$, for some integer p. If T(n) is the number of arithmetic operations needed to multiply two $n \times n$ matrices, then using Strassen's Lemma on the matrices partitioned into four $n/2 \times n/2$ blocks we get the recurrence

$$T(n) = 7T(n/2) + 18(n/2)^2 \quad \text{for } n \geq 2 .$$

The first term on the right is the time required to multiply a 2×2 matrix whose elements are $n/2 \times n/2$ matrices, while the second term is the time required for the addition/subtraction of these matrices. By induction we get

$$T(n) = O(7^{\log n}) = O(n^{\log 7}) .$$

If n is not a power of 2, i.e., $2^p < n < 2^{p+1}$, then augment the matrices with enough rows and columns of zeroes to make $n = 2^{p+1}$. This will increase the size of the matrix by a factor of 2, at most. This in turn will increase T(n) by a factor of 7, and so T(n) is still $O(n^{\log 7})$.

It can be shown (see [AHU74]) that equation - solving, inversion, determinant evaluation, etc., are computationally equivalent. This implies that each of these operations can be performed in $O(n^{\log 7})$ time.

5. PRACTICAL CONSIDERATIONS

Although Strassen's improvement is theoretically significant it is not better than classical $O(n^3)$ multiplication, unless n is large (> 150). This is because of the many hidden, non-arithmetic operations that must be performed during the multiplication operation. Additional storage, for intermediate results, is also needed because the algorithm is recursive.

Nonetheless, Strassen's Algorithm has opened up a large new area of research (see below) whose results will have great practical significance as computers increase in size and speed.

6. RECENT IMPROVEMENTS

Strassen's work [Str69] stimulated a great deal of research into matrix multiplication and related operations. We give here a chronology of the improvements since 1969, taken from a recent paper [Pan81].

Exponent	Author	Date of Publication
2.8074	Strassen	1969
2.7950	Pan	1978
2.7804	Pan	1979
2.7801	Pan	1979
2.7799	Bini, et al.	1979
2.6088	Schonhage	1979
2.6054	Pan	1979
2.5480	Schonhage	To appear
2.5220	Pan & Winograd	To appear

7. A SHORT REFERENCE LIST

1. [AHU74] Aho, A., Hopcroft, J., & Ullman, J. : The Design and Analysis of Computer Algorithms, Addison Wesley, 1974.

2. [Pan81] Pan, V. : New Combinations of Methods for the Acceleration of Matrix Multiplication, Computers and Mathematics with Applications, Vol. 7, No.1, 1981.

3. [Str69] Strassen,V. : Gaussian Elimination is not Optimal, Numer. Math., Vol. 13, 354 - 356, 1969.

Roots of Real Polynomials

W.J. Kirk

and

A.G. O'Farrell

The simplest sure-fire way to approximate the real zeros of a real polynomial is to use Sturm's theorem. Horner's method misses double zeros, and Newton's method does not always work. The method based on Vincent's theorem [1] is very elaborate.

Sturm's theorem is not usually covered in basic algebra courses, even though it is in van der Waerden [2, p. 284] . Consequently, it is not as well-known as it should be. It provides a straight-forward, computationally effective method for approximating the real zeros (without multiplicities) of a real polynomial. It goes as follows.

Let $f(x)$ be a polynomial with real coefficients. Let $F_0 = f$, and $F_1 = f'$ (the derivative of f). Carry out the following variant of the Euclidean algorithm:

$$F_0 = F_1 Q_1 - F_2$$

$$F_1 = F_2 Q_2 - F_3$$

$$\cdots\cdot$$

$$F_{m-2} = F_{m-1} Q_{m-1} - F_m$$

$$F_{m-1} = F_m Q_m .$$

Note that the customary plus sign has been replaced by a minus sign. Equivalently, carry out the usual Euclidean algorithm, and change the sign of the $j-th$ remainder whenever j is congruent to 2 or 3 modulo 4. For any real number x, let $n(x)$ denote the number of sign changes in the sequence

$$F_0(x), F_1(x), \ldots, F_m(x)$$

(where terms equal to zero are omitted, thus $+,0,+$ is not a sign change, and $+,0,-$ is). This sequence is called the Sturm chain. Sturm's theorem states that if $a < b$, then the number of zeros of f in the closed interval $[a,b]$ is $n(a) - n(b)$.

This algorithm is easily programmed. Polynomials can be treated as vectors (with the coefficients as components), and one can write simple routines to carry out polynomial arithmetic (additon, multiplication, division, and Euclidean algorithm). Once the Euclidean algorithm is programmed, it is easy to write a routine to calculate $n(x)$, for any given x (since there is an algorithm for differentiating polynomials). A routine to find all the roots in the interval $[a,b]$ proceeds by checking $n(a) - n(b)$, then bisecting the interval, checking n at the endpoints, and continuing. At the $n-th$ step, the positions of the roots are known to within $|a-b|/2^n$.

To find all the roots on the line, use the (obvious) fact that all the roots of

$$f(x) = a_n x^n + \ldots + a_0$$

lie in the interval $[-s,s]$, where

$$s = 1 + \max_{0 \le j < n-1} \left| \frac{n a_j}{a_n} \right|^{1/(n-j)} .$$

To detect multiple roots, examine the zeros of f'.

We wrote a BASIC program to perform the Sturm algorithm. Apart from solving equations, it is useful for demonstrating the Euclidean algorithm for polynomials. It uses about 8k words of core on the DEC PDP 11/34. If necessary, it can be pruned considerably to fit in smaller workspaces. Copies of the listing may be had by writing to the authors.

On our time-sharing system, the program finds the total number of roots in a few seconds. The time taken to locate r roots with error less than h is roughly proportional to $r \log_2 h$. The constant of proportionality is less than 6 seconds.

References

1. D.ROSEN & J. SHALLIT, A continued fraction algorithm for approximating all real polynomial roots, Math. Mag. 51(1978)112-116.

2. B.L. van der WAERDEN, Algebra I, 8th ed., Springer, 1971.

CODING THEORY

Thomas J. Laffey

Coding Theory deals with the accurate transmission of information tthrough an imperfect (or "noisy") communication channel. The idea is to encode the message (thus enabling one to introduce several redundant (or "check" symbols), transmit the coded message and decode the received message. If the code is constructed sufficiently cleverly, then one is able to deduce from the received message, even if a "small" number of errors have occurred in transmission, what the transmitted message was.

An ALPHABET F is a set of symbols in which our messages are written. Usually F is taken to be a finite field and more particularly, the field Z_2 of two elements 0,1 (binary case) or Z_3 of three elements 0,1,2, (ternary case). [We recall that if F is a finite field, then F has q elements for some prime-power q and conversely for such q, there is essentially one field with q elements.] We denote by F^k the set of all k-tuples $u_1 \ldots u_k$ where $u_1,\ldots,u_k$ belong to F.

An (n,k) code is a (one,one) function $\mathcal{C}$ from a subset $\mathcal{M}$ of F^k to F^n. The image of $\mathcal{C}$ (that is $\{\mathcal{C}(m) \mid m \in \mathcal{M}\}$) is called the set of code-words and is also denoted by $\mathcal{C}$, and also referred to as the code. [$\mathcal{M}$ is the set of messages, given a message $m = u_1 \ldots u_k$ $\mathcal{C}(m) = x_1 \ldots x_n$ is the code-word corresponding to m.] Here n is called the length of the code.

This is the text of a lecture delivered at the Workshop on "Current Developments in Operations Research" in the College of Commerce, Dublin Institute of Technology, June 1981.

Example 1

$F = Z_2$, $\mathcal{M} = F^2$ and

$\mathcal{C}$ ↓	0 0	0 1	1 0	1 1
	0 0 0	0 1 1	1 0 1	1 1 0

$\mathcal{C}(u_1u_2) = u_1\ u_2\ u_3$ where $u_3 \in F$ is such that $u_1+u_2+u_3 = 0$ (in F). $\mathcal{C}$ introduces a parity-check.

Given two n-tuples c_1, c_2, the (Hamming) distance $d(c_1,c_2)$ is the number of places where c_1, c_2 differ. For example, if $c_1 = 10101$, $c_2 = 11011$, $d(c_1,c_2) = 3$. The weight $w(c)$ of an n-tuple c is the number of non-zero entries in c. Above $w(c_1) = 3$, $w(c_2) = 4$. We call an (n,k) code $\mathcal{C}$ an (n,k,d) code if d is the least distance between distinct elements of $\mathcal{C}$.

The most studied types of codes are linear codes. A (n,k) code is linear if F is a field and the set of code-words is a vector space over F (i.e. if c_1, c_2 are code-words, so is c_1+c_2 and ac_1 for $a \in F$ where code-words are added by adding corresponding entries and ac is obtained from c by multiplying all the entries of c by a). The dimension of this vector-space is called the dimension of the code. Usually in considering linear codes, we assume $\mathcal{M} = F^k$ in which case k is the dimension of $\mathcal{C}$.

Suppose $\mathcal{C}$ is a linear (n,k) code (of dimension k). Then $\mathcal{C}$ can be described by matrices in two ways. There exists a kxn matrix G such that

$$\mathcal{C}(w) = wG$$

for all $w = u_1 \ldots u_k \in F^k$. The dimension condition means that G has rank k. G is called the generating matrix for $\mathcal{C}$. We can also describe $\mathcal{C}$, the set of code-words, as $\{x = x_1 \ldots x_n \in F^n \mid Hx^T = 0\}$ (where T denotes transpose) and H is an $(n-k) \times n$ matrix of rank $n-k$. H is called the parity-check matrix of the code. The code $\mathcal{C}$ is called systematic if $\mathcal{C}(u_1 \ldots u_k) = u_1 \ldots u_k\, u_{k+1} \ldots u_n$, $(u_i \in F)$, that is the first k entries in the code-word corresponding to the message $m = u_1 \ldots u_k$ from m itself. If $\mathcal{C}$ is linear and systematic, then H is of the form

$$H = (X \mid I_{n-k})$$

where X is an $(n-k) \times k$ matrix. In this case,

$$G = (I_k \mid -X^T).$$

Example 1 is an example of a linear systematic $(3,2)$ code, $H = (1\ 1\ 1)$, $G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ (since we are working over Z_2 in this example $-1 = 1$).

Let u be a message, $\mathcal{C}$ a code, $x = \mathcal{C}(u)$ the code word corresponding to x. Suppose that x is transmitted and that y is received. Note that $d(x,y)$ counts the number of errors. Let $e = x-y$. Then e is called the error-vector. Given y we use the code to recover x. Choose $x_0 \in \mathcal{C}$ such that $d(y,x_0)$ is least possible. We decode y as x_0. If $w(e) = t$ (say), we necessarily get $x_0 = x$ provided that $d(y,x') > t$ for all $x' \in \mathcal{C}$, $x' \neq x$. A sufficient condition for this to happen is that $d(c_1,c_2) \geq 2t+1$ for all $c_1, c_2 \in \mathcal{C}$, $(c_1 \neq c_2)$. So $\mathcal{C}$ can "correct" t errors if its minimum distance is at least $2t+1$.

Suppose that $\mathcal{C}$ is a linear code of length n and dimension k and that F has q elements. Suppose that $\mathcal{C}$ can correct t errors. For each $c \in \mathcal{C}$, the "sphere" $S(c,t) = \{x \in F^n \mid d(c,x) \leq t\}$ contains

$$\binom{n}{0} + \binom{n}{1}(q-1) + \ldots + \binom{n}{t}(q-1)^t$$

elements and these spheres must be disjoint. Hence

$$(*) \qquad q^n \geq q^k\left[\binom{n}{0} + \binom{n}{1}(q-1) + \ldots + \binom{n}{t}(q-1)^t\right]$$

[This is known as the Hamming or sphere-packing bound).

If equality holds, the code is called <u>perfect</u>. We now give some examples of perfect codes.

<u>Example 2</u> Let F be the field of q elements and let $H(n,q)$ be the linear code of length $\frac{q^n-1}{q-1}$, dimension $k = \frac{q^n-1}{q-1} - n$ whose parity check matrix is the $n \times \left(\frac{q^n-1}{q-1}\right)$ matrix whose columns are the distinct non-zero n-tuples whose first non-zero entry is 1. It is easy to check that $H(n,q)$ has minimum distance 3 and that $(*)$ holds with $t=1$. So $H(n,q)$ is a <u>perfect</u> single error-correcting code. $H(n,q)$ is called a Hamming code.

<u>Example 3</u> Let F be a finite field and let $F[x]$ be the set of all polynomials $a_0+a_1x + \ldots + a_{n-1}x^{n-1}$. Let $g(x)$ be a divisor of x^n-1 and let $V(n,g)$ be the set of all polynomials $g(x)f(x)$ $(f(x) \in F[x])$ where we set $x^n = 1$, $x^{n+1} = x$, etc. We think of the elements $v_0+v_1x + \ldots + v_{n-1}x^{n-1} \in V(n,g)$ as n-tuples $v_0v_1 \ldots v_{n-1}$. Then the set $V(n,g)$ becomes a linear code of length n over F. This code is called a cyclic code. By judiciously choosing F,n,g, we get many

interesting codes.

For example, if $F=Z_3$, $n=11, x^{11}-1 = (x-1)g_1(x)g_2(x)$ where $g_1(x)$, $g_2(x)$ are irreducible of degree 5 over F, and taking $g(x) = g_1(x)$, we get a linear code $\mathcal{G}_{11}$ of length 11, dimension 6 and minimum distance 5. An easy calculation shows that $\mathcal{G}_{11}$ is a perfect 2-error correcting code.

If $F=Z_2$, $n=23$, $x^{23}-1 = (x-1)f_1(x)f_2(x)$ where $f_1(x), f_2(x)$ are irreducible of degree 11, and taking $g(x) = f_1(x)$ we get a linear code $\mathcal{G}_{23}$ of length 23, dimension 12 and minimum distance 7. Again, it is easy to check that $\mathcal{G}_{23}$ is a perfect 3-error correcting code. The codes $\mathcal{G}_{11}, \mathcal{G}_{23}$ by introducing a parity check are the famous Golay codes. These are the most remarkable of all codes. They arise in many combinatorial investiagations, and have intimate connections with the Conway simple groups and the recent construction of the Fischer-Griess Monster, etc. Efficient coding and de-coding procedures have been constructed for them and they are used in many communication networks.

Despite the ad-hoc nature of the construction of the perfect codes above (done initially in the 1940's) the following amazing result holds:

Theorem (van Lint, Tietavainen) Let $\mathcal{C}$ be a perfect t-error correcting code over an alphabet F of a prime-power q number of elements. Then $\mathcal{C}$ has the same parameters as H(n,q), $\mathcal{G}_{11}$ or $\mathcal{G}_{23}$.

[Note: Thus t=1,2, or 3. If t = 2 or 3, then $\mathcal{C}$ is in fact a linear code isomorphic to $\mathcal{G}_{11}$ or $\mathcal{G}_{23}$. However, if t=1, $\mathcal{C}$ need not be linear, though it must have length $\frac{q^n-1}{q-1}$,

minimum distance 3 and have the same number of elements as $H(n,q)$.]

Let $\mathcal{C}$ be a linear code of length n and dimension k over a field F with q elements. The dual code $\mathcal{C}^{\perp}$ is the set of all n-tuples $y = y_1 \ldots y_n$ such that $x.y = x_1y_1 + \ldots + x_ny_n = 0$ for all $x = x_1 \ldots x_n \in \mathcal{C}$. Then $\mathcal{C}^{\perp}$ is a linear code of length n and dimension $n-k$.

Example 4 If $\mathcal{C}$ is the Hamming code $H(n,q)$ of Example 2, then $\mathcal{C}^{\perp}$ is a linear code of length $(q^n-1)/(q-1)$ and length n. It is called a first order Reed-Muller code. In particular, the case $q=2$, $n=5$, gives the $(31,5)$ code which was used in transmitting information back to Earth from the Mariner space-craft to Mars.

Let $\mathcal{C}$ be a code of length n and for each $i = 0,1,\ldots,n$, let w_i = number of elements $c \in \mathcal{C}$ of weight i. The polynomial

$$W(x,y) = \sum_{i=0}^{n} w_i x^i y^{n-i}$$

is called the weight-enumerator of the code. MacWilliams discovered a beautiful connection between the weight-enumerators of $\mathcal{C}$ and its dual $\mathcal{C}^{\perp}$ for a linear code $\mathcal{C}$. We state the result for the case of a binary code.

MacWilliams' Theorem If $\mathcal{C}$ is a binary linear code, then

$$W_{\mathcal{C}^{\perp}}(x,y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(x+y,x-y)$$

(where $|\mathcal{C}|$ denotes the number of elements in $\mathcal{C}$).

An elementary proof of this can be obtained using the finite Fourier transform.

$\mathcal{C}$ is called <u>self-dual</u> if $\mathcal{C} = \mathcal{C}^{\perp}$.

<u>Example 5</u> $\mathcal{G}_{12}, \mathcal{G}_{24}$ are self-dual.

MacWilliams' theorem enables one to get information on the weight distribution of a self-dual code. Namely, for $\mathcal{C}$ a self-dual binary code, we have

$$W_{\mathcal{C}}(x,y) = W_{\mathcal{C}}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right).$$

By considering the group G which leaves W(x,y) invariant and the classical theory of invariants of finite groups, Gleason (and others) have found very detailed information on the structure of self-dual codes, and in particular, were able to prove the non-existence of certain codes.

<u>Example 6</u> The weight enumerator of $\mathcal{G}_{24}$ is

$$x^{24} + 759x^{16}y^{8} + 2576x^{12}y^{12} + 759x^{8}y^{16} + y^{24}.$$

There are many methods by which interesting codes are constructed and we describe here a couple of these.

A nxn matrix H, all of whose entries are ±1 is called a Hadamard <u>matrix</u> if $HH^{T} = nI$. It is easy to show that if H exists for n>2, then n must be a multiple of 4 and it is conjectured that a Hadamard matrix exists for all such n. The smallest n still in doubt is n=268. If H_n is a Hadamard matrix of size nxn, multiplying it on left and right

by suitable diagonal matrices with entries 1 we get a Hadamard matrix with first row and first column all ones. Such a Hadamard matrix is called normalized.

Suppose H_n is a normalized Hadamard matrix. Deleting the first column of H_n and replacing all its 1's by 0's and its -1's by 1's we get a code A_n of length n-1, minimum distance n/2 and containing n codewords. Several other codes can be constructed from H_n.

A well-known result on codes is

Plotkin Bound Let m,d be given with $2d>m$ and let $\mathcal{C}$ be a code of length m and minimum distance d. Then $\mathcal{C}$ has at most $2\left[\frac{d}{2d-m}\right]$ code-words.

Note that the code A_n achieves this bound for m=n, d=n/2 and a result of Levensthein shows more strongly that the Plotkin bound is attainable in general if Hadamard matrices H_n exist for all n which are multiples of 4.

We now consider briefly the construction of Hadamard matrices. If H is an nxn Hadamard matrix, then $\begin{bmatrix} H & H \\ H & -H \end{bmatrix}$ is a $2n \times 2n$ Hadamard matrix. Starting with (1) we can thus construct Hadamard matrices of size $2^k x 2^k$ $(k \geq 1)$.

Suppose n is a multiple of 4 and that $n = q+1$ where q is a prime power. Denote the non-zero elements of the finite field F with q elements by $1,2,\ldots,q-1$.

Let Q be the qxq matrix (indexed by the elements 0,1,...,q-1 of F) whose (i,j) entry

q_{ij} = 0 if i=j

= 1 if $i \neq j$ and i-j is a square in F

= -1 if $i \neq j$ and i-j is not a square in F.

Let H be the nxn matrix

$$\begin{bmatrix} 1 & 1 & . & . & . & 1 \\ 1 & & & & & \\ . & & & & & \\ . & & & Q-I_q & & \\ . & & & & & \\ 1 & & & & & \end{bmatrix}$$

Then H is a Hadamard nxn matrix. This is called the Paley construction. If we take n=12, the matrix obtained in this way is related to the generating matrix of the Golay code $\mathcal{G}_{24}$.

Recently, work of Goethals-Seidel has led to a method related to the quaternions and Turyn sequences for constructing Hadamard matrices. It is conjectured that this method will work in all cases. For details (though beware the typographical errors), see M. Hall's paper in the Proceedings of the Santa Cruz Group Theory Conference (AMS 1981).

Given a Hadamard matrix H, we can replace the entries 1, -1, by 0, 1 respectively and then consider the binary code spanned by the rows. These codes have also been studied, the ones corresponding to the Paley-type Hadamard matrices are examples of quadratic residue codes.

We conclude by giving an application of coding theory to combinatorics. Suppose $\mathcal{P}$ is a finite projective plane of order 10. [The problem of whether $\mathcal{P}$ exists is a famous, (still) open question.] Then $\mathcal{P}$ consists of 111 points, 111 lines, each point lies on exactly 11 lines, each line has exactly 11 points. Each pair of points lies on a unique line and two distinct lines meet in exactly one point. Let $A = (a_{ij})$ be the incidence matrix of $\mathcal{P}$. Thus A is an 111×111 matrix and if P_i, L_i are the points, lines, resp. of $\mathcal{P}$,

$$a_{ij} = 1 \text{ if } P_i \text{ lies on } L_j,$$
$$= 0 \text{ if } P_i \text{ does not lie on } L_j.$$

Let $\mathcal{A}$ be the binary code with A as its generating matrix. It has been shown that $\mathcal{A}$ has minimum distance 11. Let $\hat{\mathcal{A}}$ be the code obtained by adding a parity check to $\mathcal{A}$. Then $\hat{\mathcal{A}}$ has minimum distance 12, length 112 and it is easy to show that $\hat{\mathcal{A}} \subseteq \hat{\mathcal{A}}^{\perp}$. Thompson has shown that in fact $\hat{\mathcal{A}}$ has dimension 56 and thus $\hat{\mathcal{A}}$ is a self-dual code. It has been shown that the weight distribution of $\hat{\mathcal{A}}$ would be known if w_{12}, w_{15} and w_{16} were known. MacWilliams, Sloane, Thompson, have shown that $w_{15} = 0$. By considering $\hat{\mathcal{A}}$ more closely, recently, Anstee, Hall, Thompson, have shown that $\mathcal{P}$ has no automorphism of order 5. This, with work of Whitesides shows that the automorphism group of $\mathcal{P}$ has order a power of 3 and is now conjectured to be trivial. So $\mathcal{P}$, if it exists, does not appear to have any of the symmetry we usually associate with a geometry.

References

For a general survey of coding theory, the best sources are the following books:

van Lint. Coding Theory (Lecture Notes in Mathematics No.201). Springer-Verlag, 1971.

McEliece. The Theory of Information and Coding (Encyclopaedia of Mathematics & its Applications, Vol.3). Addison-Wesley, 1977.

MacWilliams and Sloane. The Theory of Error-Correcting Codes. Parts I,II. North-Holland, 1977. (*This book also contains a very comprehensive set of references.*)

The book:

Shu Lin. An Introduction to Error-Correcting Codes. Prentice Hall, 1970, *discusses the problems of constructing efficient programmes to implement the various codes.*

The book:

Blake and Mullin. An Introduction to Algebraic and Combinatorial Coding Theory. Academic Press, 1976, *gives a quite concise account of coding theory with particular reference to its relation to combinatorics. It also contains a nice account of the algebraic machinery (particularly the theory of finite fields and their automorphisms) required for constructing codes.*

The work of Anstee, Hall, Thompson, *referred to above appears in* Journal of Combinatorial Theory, Series A, 29 (1980, 39-58.

The Golay Codes *are discussed at length in the* MacWilliams-Sloane *book. The material on the nonexistence of perfect codes referred to above is also available there, or in* van Lint's *paper in* Combinatorics (Proceedings of the NATO Adv. Study Institute, Breukelen, The Netherlands, 1974), Riedel Publ. Co., 1975. *This book also contains a very nice account of Gleason's and MacWilliams' theorems on weight-enumerators by* Sloane *as well as interesting papers on coding theory by* Delsarte and McEliece.

RECENT ADVANCES IN MATHEMATICS

It seems a good idea to have a section of the Newsletter devoted to informing readers of recent major break-throughs in Mathematics, which should be of interest to mathematicians in general. In this issue, we list two results of this type.

(1) The Classification of the Finite Simple Groups

A paper by G. Mason, now in the course of completion, will bring to an end the classification of the finite simple groups. This is arguably the greatest mathematical achievement of all time, the proof that the list of known simple groups is complete adding up to many thousands of pages. The classification has involved the work of many of the greatest mathematicians of our time and has involved major contributions by so many people that it is difficult to single out any aspects for special mention. However, the development of techniques by Chevalley to actually construct the simple groups of Lie type in the 1950's, the proof of the solvability of groups of odd order by Feit and Thompson (1963), the determination of the minimal simple groups by Thompson (1968) and the work of Aschbacher and Thompson on the B-conjecture in the 1970's are universally recognised as milestones along the way.

Of course, quite a lot of work has still to be done to try and shorten and simplify the work to make it comprehensible to ordinary mortals. Referring to the view among some mathematicians that finite group theory was finished now that the simple groups are known, Gorenstein (in Pittsburgh in August) reminded his audience that though the real numbers have been

classified for a long time, there are still many real analysts.

(2) The van der Waerden conjecture

Let $A = (a_{ij})$ be an nxn matrix. The permanent, per A, of A is defined by

$$\text{per } A = \sum_{\sigma \in S_n} a_{\sigma(1)1}\, a_{\sigma(2)2} \cdots a_{\sigma(n)n}$$

(where S_n denotes the symmetric group of degree n)

[per A is thus the same as det A except that sign (σ) is replaced by +1 throughout.]

A is called doubly stochastic if its entries are (real) non-negative and the sum of the entries in each row is 1 and the sum of the entries in each column is 1. Thus, in symbols

$$\sum_{i=1}^{n} a_{ij} = 1 = \sum_{i=1}^{n} a_{ji} \qquad (j = 1,\ldots,n).$$

Examples of doubly stochastic matrices are I_n and J_n where J_n is the nxn matrix all of whose entries are 1/n.

The famous van der Waerden conjecture (1925) states that the minimum of per A as A ranges through the set of all doubly stochastic nxn matrices is achieved precisely for $A = J_n$.

Many authors worked on this problem and many special cases were resolved. Of particular elegance is the solution by Marcus and Minc for the case of symmetric A. See Minc's book on Permanents or the article by Marcus and Minc in the American Mathematical Monthly Vol.75 (1965) for the history

and results on the problem.

Recently the conjecture has been proved in full generality by Egoryshev in Krasnoyarsk in the U.S.S.R. A very nice account of the solution (incorporating some simplifications due to himself and Seidel) can be found in the article by van Lint in Linear Algebra and its Applications, Vol. 1981.

T.J. Laffey

PROBLEM SECTION

(4.1) (D. McHale) Let R be a finite commutative ring with identity and let $a,b \in R$ with $aR = bR$. Show that $a = bu$ for some unit u of R. Generalise!

(4.2) (M. Hall and M. Newman) Let $Q(x_1,\ldots,x_n)$ be a positive definite real quadratic form and suppose that Q can be expressed as $L_1^2 + \ldots + L_r^2$ where $L_1,\ldots,L_r$ are linear forms with non-negative coefficients. Show that Q has such a representation with $r \leq f(n)$ for some function $f(n)$ of n^2 and find the best such function f.

(4.3) Calculate explicitly $\sum_{n=0}^{\infty} e^{-\pi n^2}$, $\sum_{n=0}^{\infty} e^{-2\pi n^2}$.

(4.4) (P. Halmos) Let A,B be positive semi-definite matrices. Let $d_1(A,B) = \|A-B\|$ and $d_2(A,B) = \sup_{\|x\|=1} \left| \|Ax\| - \|Bx\| \right|$. Prove that there exists a function $c(n)$ such that $d_2 \leq d_1 \leq c(n)d_2$ and find the best function c.

(4.5) For which natural numbers n does there exist an $n \times n$ magic square whose entries are $1,2,\ldots,n$. [According to the Evening Press, one has been constructed recently with $n = 243$.]

(4.6) (G. Myerson) Given two co-prime integer polynomials $f(x)$, $g(x)$, find a formula for the least positive integer d for which there exist integral polynomials $h(x)$, $k(x)$ with $d = f(x)h(x)+g(x)k(x)$. [Myerson points out that the standard Sylvester resultant formula does not necessarily give the smallest d.]

SOLUTIONS TO PROBLEMS

We give here outline solutions to some of the problems in Newsletter Number 3.

(3.1) Find all numbers of the form $\frac{1}{2}n(n+1)$ (triangular numbers) which are perfect squares.

Suppose first that n is even. The fact that $\frac{1}{2}n(n+1)$ is a perfect square implies that $n=2a^2$, $n+1=b^2$ where a,b are integers. But then $b^2-2a^2=1$. Conversely for such a,b, setting $n=2a^2$ gives a solution to our problem. The solutions to the equation $b^2-2a^2=\pm 1$ are given by the rational and irrational parts of the binomial expansion of $\pm(1\pm\sqrt{2})^k$ $(k=0,1,\ldots)$ (Hardy and Wright: Introduction to the Theory of Numbers). A similar analysis works in the case n odd.

(J. Kennedy)

(3.2) Let $n>1$ be a given natural number. Find a square matrix A whose entries are zeros and ones such that A^n is a matrix with all its entries equal to one. Show that 2^n is the least possible size for such a matrix A.

Let A be the $2^n \times 2^n$ matrix of the form $\begin{pmatrix} B \\ B \end{pmatrix}$ where row i of B has ones in the $(2i-1)^{st}$ and $(2i)^{th}$ positions and zeros elsewhere. Then $A^n = J(2^n)$ where $J(m)$ is the $m \times m$ matrix all of whose entries are one. On the other hand, if $A^n = J(t)$, the eigenvalues of A^n are $t,0,\ldots,0$, so the eigenvalues of A are $\sqrt[n]{t},0,\ldots,0$. So trace $(A) = \sqrt[n]{t}$. Since trace (A) is an integer,

t must be a perfect n^{th} power. So $t \geq 2^n$.

(W. Sullivan)

(3.3) (non-trivial part) Give an example of periodic functions f,g with periods $u > 0$, $v > 0$, respectively, such that (i) u/v is not rational, and (ii) $f+g$ is periodic.

Define a function $f_a : [0,a] \to \mathbb{R}$ as follows: Let $x \in [0,a]$. For each integer m, let $x_m = x+m\pi-ka$ where k is the unique integer so that $x_m \in [0,a)$. For example, when $a=1$, x_m is the decimal part of $x+m\pi$.) Let $V(x) = \{x_m \mid m \in Z\}$. Note that $V(x) \cap V(y)$ non-empty implies $V(x) = V(y)$. So $\{V(x)\}$ form a partition of $[0,a]$. Choose a distinguished element $y = y(x)$ in each distinct $V(x)$. Then $V(x) = \{y_m \mid m \in Z\}$. Define $f_a : [0,a] \to \mathbb{R}$ by $f_a(y_m) = m$. Extend f_a to be a map of $\mathbb{R}$ to $\mathbb{R}$ by the rule $f_a(x+a) = f_a(x)$. Then f_a is periodic of period $\leq a$ and f_a satisfies the equation $f_a(x+\pi) = f_a(x)+1$ for all $x \in \mathbb{R}$.

Let $f = f_1$, $g = -f_{\sqrt{2}}$. Then f is periodic of period 1 and g is periodic of period $\sqrt{2}$ (using the fact that π is not algebraic). Also $f(x+\pi) = f(x)+1$ and $g(x+\pi) = g(x)-1$ for all real x. So $f+g$ is periodic of period a (non-zero) rational multiple of π.

(3.4) Let A be a square matrix with entries in a field F. Prove that $A = D+N$ where N is nilpotent and D is diagonalizable <u>over the field</u> F.

We reduce easily to the case where A is a companion matrix, say

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ & & & & & \\ & & & & & \\ & & & & & 1 \\ a_0 & a_1 & \cdots & \cdots & a_{n-1} \end{bmatrix}$$

If $a_{n-1} \neq 0$, take N to be A with the last row replaced by zero and D to have its last row equal to the last row of A and zeros elsewhere. If $a_{n-1} = 0$, let k be the least integer with $a_{n-k-1} \neq 0$. Replace N as above except that the 1 in its $(n-k)^{th}$ row is replaced by $1-a_{n-k-1}$ and let $D = A-N$. In characteristic $\neq 2$, D is diagonalizable with non-zero eigenvalues $\pm a_{n-k-1}$. In characteristic 2, the required result may fail - try $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ over Z_2.

(3.5) This question is answered in the paper by Choi, Laurie and Radjavi in Linear & Multilinear Algebra 8, (1980).

T.J. Laffey

COMMITTEE OF THE IRISH MATHEMATICAL SOCIETY

President : Professor J.J.H. Miller (TCD)

Vice-President : Professor F. Holland (UCC)

Secretary : Professor S. Dineen (UCD)

Treasurer : Dr. R. Ryan (UCG)

Mr. C. O'Caoimh (Dept. Education)

Professor A. Jennings (QUB)

Professor J.T. Lewis (DIAS)

Dr. P. McGill (NUU)

Dr. D. Redmond (Maynooth)

Dr. M. Stynes (Waterford RTC)

Dr. R.M. Timoney (TCD)