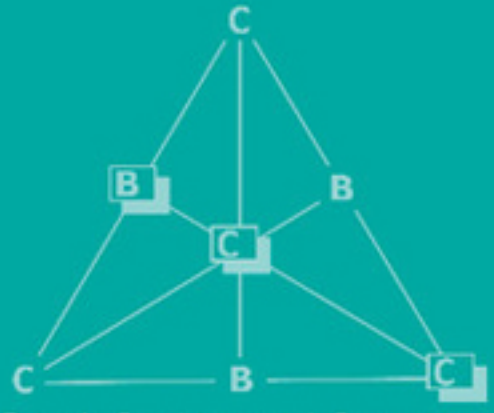
London Mathematical Society
Lecture Note Series 267

Surveys in Combinatorics, 1999

Edited by
J. D. Lamb & D. A. Preece



CAMBRIDGE
UNIVERSITY PRESS
British Combinatorial Committee

CAMBRIDGE
more information - www.cambridge.org/9780521653763

LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES

Managing Editor: Professor N.J. Hitchin, Mathematics Institute,
University of Oxford, 24–29 St Giles, Oxford OX1 3LB, United Kingdom

The titles below are available from booksellers, or, in case of difficulty, from Cambridge University Press.

46 *p*-adic Analysis: a short course on recent work, N. KOBLITZ
59 Applicable differential geometry, M. CRAMPIN & F.A.E. PIRANI
66 Several complex variables and complex manifolds II, M.J. FIELD
86 Topological topics, I.M. JAMES (ed)
87 Surveys in set theory, A.R.D. MATHIAS (ed)
88 FPF ring theory, C. FAITH & S. PAGE
89 An F-space sampler, N.J. KALTON, N.T. PECK & J.W. ROBERTS
90 Polytopes and symmetry, S.A. ROBERTSON
92 Representations of rings over skew fields, A.H. SCHOFIELD
93 Aspects of topology, I.M. JAMES & E.H. KRONHEIMER (eds)
96 Diophantine equations over function fields, R.C. MASON
97 Varieties of constructive mathematics, D.S. BRIDGES & F. RICHMAN
98 Localization in Noetherian rings, A.V. JATEGAONKAR
99 Methods of differential geometry in algebraic topology, M. KAROUBI & C. LERUSTE
100 Stopping time techniques for analysts and probabilists, L. EGGHE
104 Elliptic structures on 3-manifolds, C.B. THOMAS
105 A local spectral theory for closed operators, I. ERDELYI & WANG SHENGWANG
107 Compactification of Siegel moduli schemes, C.-L. CHAI
109 Diophantine analysis, J. LOXTON & A. VAN DER POORTEN (eds)
113 Lectures on the asymptotic theory of ideals, D. REES
114 Lectures on Bochner-Riesz means, K.M. DAVIS & Y.-C. CHANG
116 Representations of algebras, P.J. WEBB (ed)
119 Triangulated categories in the representation-theory of finite-dimensional algebras, D. HAPPEL
121 Proceedings of *Groups - St Andrews 1985*, E. ROBERTSON & C. CAMPBELL (eds)
128 Descriptive set theory and the structure of sets of uniqueness, A.S. KECHRIS & A. LOUVEAU
130 Model theory and modules, M. PREST
131 Algebraic, extremal & metric combinatorics, M.-M. DEZA, P. FRANKL & I.G. ROSENBERG (eds)
132 Whitehead groups of finite groups, ROBERT OLIVER
133 Linear algebraic monoids, MOHAN S. PUTCHA
134 Number theory and dynamical systems, M. DODSON & J. VICKERS (eds)
137 Analysis at Urbana, I, E. BERKSON, T. PECK, & J. UHL (eds)
138 Analysis at Urbana, II, E. BERKSON, T. PECK, & J. UHL (eds)
139 Advances in homotopy theory, S. SALAMON, B. STEER & W. SUTHERLAND (eds)
140 Geometric aspects of Banach spaces, E.M. PEINADOR & A. RODES (eds)
141 Surveys in combinatorics 1989, J. SIEMONS (ed)
144 Introduction to uniform spaces, I.M. JAMES
146 Cohen-Macaulay modules over Cohen-Macaulay rings, Y. YOSHINO
148 Helices and vector bundles, A.N. RUDAKOV *et al*
149 Solitons, nonlinear evolution equations and inverse scattering, M. ABLOWITZ & P. CLARKSON
150 Geometry of low-dimensional manifolds 1, S. DONALDSON & C.B. THOMAS (eds)
151 Geometry of low-dimensional manifolds 2, S. DONALDSON & C.B. THOMAS (eds)
152 Oligomorphic permutation groups, P. CAMERON
153 L-functions and arithmetic, J. COATES & M.J. TAYLOR (eds)
155 Classification theories of polarized varieties, TAKAO FUJITA
156 Twistors in mathematics and physics, T.N. BAILEY & R.J. BASTON (eds)
158 Geometry of Banach spaces, P.F.X. MÜLLER & W. SCHACHERMAYER (eds)
159 Groups St Andrews 1989 volume 1, C.M. CAMPBELL & E.F. ROBERTSON (eds)
160 Groups St Andrews 1989 volume 2, C.M. CAMPBELL & E.F. ROBERTSON (eds)
161 Lectures on block theory, BURKHARD KÜLSHAMMER
162 Harmonic analysis and representation theory, A. FIGA-TALAMANCA & C. NEBBIA
163 Topics in varieties of group representations, S.M. VOVSI
164 Quasi-symmetric designs, M.S. SHRIKANDE & S.S. SANE
166 Surveys in combinatorics, 1991, A.D. KEEDWELL (ed)
168 Representations of algebras, H. TACHIKAWA & S. BRENNER (eds)
169 Boolean function complexity, M.S. PATERSON (ed)
170 Manifolds with singularities and the Adams-Novikov spectral sequence, B. BOTVINNIK
171 Squares, A.R. RAJWADE
172 Algebraic varieties, GEORGE R. KEMPF
173 Discrete groups and geometry, W.J. HARVEY & C. MACLACHLAN (eds)
174 Lectures on mechanics, J.E. MARSDEN
175 Adams memorial symposium on algebraic topology 1, N. RAY & G. WALKER (eds)
176 Adams memorial symposium on algebraic topology 2, N. RAY & G. WALKER (eds)
177 Applications of categories in computer science, M. FOURMAN, P. JOHNSTONE & A. PITTS (eds)
178 Lower K- and L-theory, A. RANICKI
179 Complex projective geometry, G. ELLINGSRUD *et al*
180 Lectures on ergodic theory and Pesin theory on compact manifolds, M. POLLICOTT
181 Geometric group theory I, G.A. NIBLO & M.A. ROLLER (eds)
182 Geometric group theory II, G.A. NIBLO & M.A. ROLLER (eds)
183 Shintani zeta functions, A. YUKIE

184 Arithmetical functions, W. SCHWARZ & J. SPILKER
185 Representations of solvable groups, O. MANZ & T.R. WOLF
186 Complexity: knots, colourings and counting, D.J.A. WELSH
187 Surveys in combinatorics, 1993, K. WALKER (ed)
188 Local analysis for the odd order theorem, H. BENDER & G. GLAUBERMAN
189 Locally presentable and accessible categories, J. ADAMEK & J. ROSICKY
190 Polynomial invariants of finite groups, D.J. BENSON
191 Finite geometry and combinatorics, F. DE CLERCK *et al*
192 Symplectic geometry, D. SALAMON (ed)
194 Independent random variables and rearrangement invariant spaces, M. BRAVERMAN
195 Arithmetic of blowup algebras, WOLMER VASCONCELOS
196 Microlocal analysis for differential operators, A. GRIGIS & J. SJÖSTRAND
197 Two-dimensional homotopy and combinatorial group theory, C. HOG-ANGELONI *et al*
198 The algebraic characterization of geometric 4-manifolds, J.A. HILLMAN
199 Invariant potential theory in the unit ball of $\mathbf{C}^n$, MANFRED STOLL
200 The Grothendieck theory of dessins d'enfant, L. SCHNEPS (ed)
201 Singularities, JEAN-PAUL BRASSELET (ed)
202 The technique of pseudodifferential operators, H.O. CORDES
203 Hochschild cohomology of von Neumann algebras, A. SINCLAIR & R. SMITH
204 Combinatorial and geometric group theory, A.J. DUNCAN, N.D. GILBERT & J. HOWIE (eds)
205 Ergodic theory and its connections with harmonic analysis, K. PETERSEN & I. SALAMA (eds)
207 Groups of Lie type and their geometries, W.M. KANTOR & L. DI MARTINO (eds)
208 Vector bundles in algebraic geometry, N.J. HITCHIN, P. NEWSTEAD & W.M. OXBURY (eds)
209 Arithmetic of diagonal hypersurfaces over finite fields, F.Q. GOUVÊA & N. YUI
210 Hilbert C*-modules, E.C. LANCE
211 Groups 93 Galway / St Andrews I, C.M. CAMPBELL *et al* (eds)
212 Groups 93 Galway / St Andrews II, C.M. CAMPBELL *et al* (eds)
214 Generalised Euler-Jacobi inversion formula and asymptotics beyond all orders, V. KOWALENKO *et al*
215 Number theory 1992–93, S. DAVID (ed)
216 Stochastic partial differential equations, A. ETHERIDGE (ed)
217 Quadratic forms with applications to algebraic geometry and topology, A. PFISTER
218 Surveys in combinatorics, 1995, PETER ROWLINSON (ed)
220 Algebraic set theory, A. JOYAL & I. MOERDIJK
221 Harmonic approximation, S.J. GARDINER
222 Advances in linear logic, J.-Y. GIRARD, Y. LAFONT & L. REGNIER (eds)
223 Analytic semigroups and semilinear initial boundary value problems, KAZUAKI TAIRA
224 Computability, enumerability, unsolvability, S.B. COOPER, T.A. SLAMAN & S.S. WAINER (eds)
225 A mathematical introduction to string theory, S. ALBEVERIO, J. JOST, S. PAYCHA, S. SCARLATTI
226 Novikov conjectures, index theorems and rigidity I, S. FERRY, A. RANICKI & J. ROSENBERG (eds)
227 Novikov conjectures, index theorems and rigidity II, S. FERRY, A. RANICKI & J. ROSENBERG (eds)
228 Ergodic theory of $\mathbf{Z}^d$ actions, M. POLLICOTT & K. SCHMIDT (eds)
229 Ergodicity for infinite dimensional systems, G. DA PRATO & J. ZABCZYK
230 Prolegomena to a middlebrow arithmetic of curves of genus 2, J.W.S. CASSELS & E.V. FLYNN
231 Semigroup theory and its applications, K.H. HOFMANN & M.W. MISLOVE (eds)
232 The descriptive set theory of Polish group actions, H. BECKER & A.S. KECHRIS
233 Finite fields and applications, S. COHEN & H. NIEDERREITER (eds)
234 Introduction to subfactors, V. JONES & V.S. SUNDER
235 Number theory 1993–94, S. DAVID (ed)
236 The James forest, H. FETTER & B. GAMBOA DE BUEN
237 Sieve methods, exponential sums, and their applications in number theory, G.R.H. GREAVES *et al*
238 Representation theory and algebraic geometry, A. MARTSINKOVSKY & G. TODOROV (eds)
239 Clifford algebras and spinors, P. LOUNESTO
240 Stable groups, FRANK O. WAGNER
241 Surveys in combinatorics, 1997, R.A. BAILEY (ed)
242 Geometric Galois actions I, L. SCHNEPS & P. LOCHAK (eds)
243 Geometric Galois actions II, L. SCHNEPS & P. LOCHAK (eds)
244 Model theory of groups and automorphism groups, D. EVANS (ed)
245 Geometry, combinatorial designs and related structures, J.W.P. HIRSCHFELD *et al*
246 p-Automorphisms of finite p-groups, E.I. KHUKHRO
247 Analytic number theory, Y. MOTOHASHI (ed)
248 Tame topology and o-minimal structures, LOU VAN DEN DRIES
249 The atlas of finite groups: ten years on, ROBERT CURTIS & ROBERT WILSON (eds)
250 Characters and blocks of finite groups, G. NAVARRO
251 Gröbner bases and applications, B. BUCHBERGER & F. WINKLER (eds)
252 Geometry and cohomology in group theory, P. KROPHOLLER, G. NIBLO, R. STÖHR (eds)
253 The q-Schur algebra, S. DONKIN
254 Galois representations in arithmetic algebraic geometry, A.J. SCHOLL & R.L. TAYLOR (eds)
255 Symmetries and integrability of difference equations, P.A. CLARKSON & F.W. NIJHOFF (eds)
256 Aspects of Galois theory, HELMUT VÖLKLEIN *et al*
257 An introduction to noncommutative differential geometry and its physical applications 2ed, J. MADORE
258 Sets and proofs, S.B. COOPER & J. TRUSS (eds)
259 Models and computability, S.B. COOPER & J. TRUSS (eds)
260 Groups St Andrews 1997 in Bath, I, C.M. CAMPBELL *et al*
261 Groups St Andrews 1997 in Bath, II, C.M. CAMPBELL *et al*
263 Singularity theory, BILL BRUCE & DAVID MOND (eds)
264 New trends in algebraic geometry, K. HULEK, F. CATANESE, C. PETERS & M. REID (eds)

London Mathematical Society Lecture Note Series. 267

Surveys in Combinatorics, 1999

Edited by

J. D. Lamb
University of Kent at Canterbury

D. A. Preece
University of Kent at Canterbury

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town,
Singapore, Sao Paulo, Delhi, Mexico City

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8Ru, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521653763

© Cambridge University Press 1999

This publication is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without the written
permission of Cambridge University Press.

First published 1999

A catalogue record for this publication is available from the British Library

ISBN 978-0-521-65376-3 Paperback

Cambridge University Press has no responsibility for the persistence or
accuracy of URLs for external or third-party internet websites referred to in
this publication, and does not guarantee that any content on such websites is,
or will remain, accurate or appropriate. Information regarding prices, travel
timetables, and other factual information given in this work is correct at
the time of first printing but Cambridge University Press does not guarantee
the accuracy of such information thereafter.

Contents

Preface

The British Combinatorial Conference, a biennial event, took place at the University of Kent at Canterbury in 1999, with ourselves as the Local Organisers. This volume contains the texts of the Invited Talks from this seventeenth Conference in the series. As at the previous Conferences, the Invited Speakers were distinguished research workers chosen by the British Combinatorial Committee to provide seminal surveys of topics representative of the main areas of present-day combinatorial mathematics. We are delighted with the excellence of the papers that have been produced.

In preparing this volume, we have been greatly assisted by being able to use the LaTeX style-file and other documentation prepared by Professor Rosemary A. Bailey for the Invited Talks for the 1997 Conference [London Mathematical Society Lecture Note Series 241].

The Conference was very grateful for financial support from the London Mathematical Society and from the Institute of Mathematics and Its Applications.

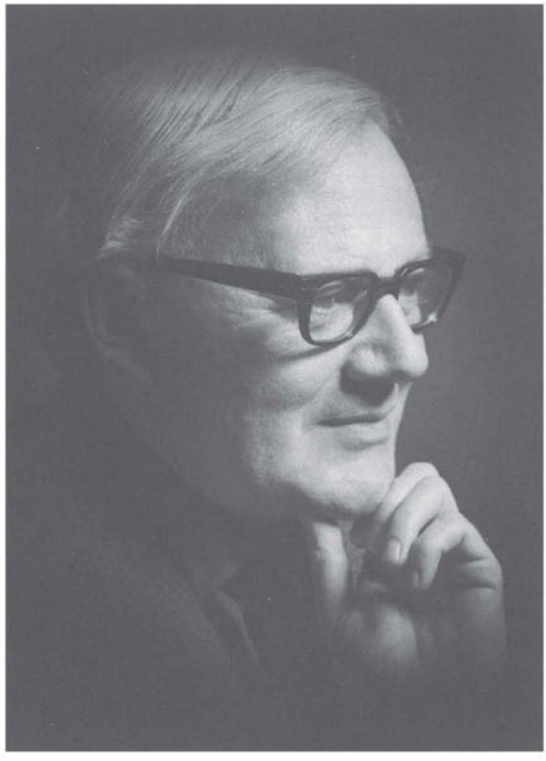
John D. Lamb
Donald A. Preece

University of Kent at Canterbury

J.D.Lamb@ukc.ac.uk
D.A.Preece@ukc.ac.uk

Richard Rado FRS (1906–1989)

The Rado Lecture



Professor W. T. Tutte FRS

The Coming of the Matroids

W. T. Tutte

Summary The author rehearses his role in the development of the theory of matroids. The story starts in 1935 when he became an undergraduate at Trinity College, Cambridge, and started to collaborate with Leonard Brooks, Cedric Smith and Arthur Stone. It continues through his war-time work with codes and ciphers, followed by his return to Trinity in 1945, where his PhD thesis entitled "An Algebraic Theory of Graphs" foreshadowed his matroid papers published in 1958 and 1959. He describes the context in which he obtained the now well-known excluded minor conditions for a binary matroid to be regular and for a regular matroid to be graphic. He subsequently invented the whirl, and lectured on matroids at the 1964 Conference where the theory of matroids was first proclaimed to the world. This paper has two appendices: "Geometrical Terminology" and "Binary and Regular Matroids".

As we all know, matroids made their appearance in the mathematical literature in 1935, in a paper of Hassler Whitney entitled "On the abstract properties of linear dependence" [17].

Whitney looked at a matrix and saw that some sets of columns were independent and some were not. There were even simple rules about this distinction. For example, any subset of an independent set of columns is independent—provided of course that you count the null set as independent. Also, if you had an independent set A you could make it into a bigger one by adding the right member of any independent set that was bigger than A. In a flash of genius, Whitney said "Let us make these statements the axioms of a theoretical structure that is like a matrix and yet more than a matrix!"

I imagine him reflecting: "A spheroid is something like a sphere. A cycloid is something like a cycle. So something like a matrix could be a 'matroid'. So be it!"

Now Whitney, only a few years before, had published some important papers on graph theory—papers making up the nearest thing we had to a textbook on the subject [12–16]. Everyone knows nowadays that a graph has associated matroids, and it seems reasonable that matroid theory should develop out of graph theory. Whitney remarks on the connection between the two subjects in his introduction and carries over some terms from one theory to the other. That is why he calls a circuit a "circuit", though it does not always look like one.

But Whitney left graph theory, and perhaps matroid theory was the path by which he left—though we should note that having sojourned forty years in the wilderness he emerged to part-write a paper on the Four Colour Problem [18].

But let all that be introductory. I suppose you are not anxious for me to make this lecture a recitation from the literature. Better that I should tell

of experiences of my own, of how I myself encountered matroids and other abstractions from graph theory.

1935 was the year when I became an undergraduate at Trinity College, Cambridge. There I joined the Trinity Mathematical Society and formed an informal association with three other members, Leonard Brooks, Cedric Smith and Arthur Stone. The object of this association was the study of out-of-the-way mathematical problems, notably that of dissecting a square into unequal squares.

Since this problem depended on a knowledge of Kirchhoff's Laws for electric currents, it gave us an excellent grounding in graph theory. We therefore began to look at other graph-theoretical problems too.

Our association received different names from time to time. The Important Members, The Four Horsemen, The Gang of Four. Take your pick.

A set of currents in a graph obeying Kirchhoff's Laws we called a "Kirchhoff Chain". Arthur Stone, the topologist, pointed out that this chain was "a cycle modulo the poles" and "an absolute cocycle". Some years later, in a course on combinatorial topology, I found out what he meant.

Smith began to abstract from Four Colour Theory. He started with Tait's variation on that theory, which considers 3-colourings of the edges of a cubic graph G so that all three colours meet at each vertex. In Smith's first abstraction the edges of G became geometrical points associated in threes. Each triad of course corresponded to a vertex of G. He called his abstraction a "3-net".

Now if the edges of G are properly coloured in three colours a, b and c, then those of any two colours a and b form a "Tait cycle", that is, a union of one or more disjoint even circuits that takes in all the vertices. Smith now constructed a second 3-net that he called the "derivative" of the first. Its points were the Tait cycles—and they came in triads, one triad to each Tait colouring. Soon he had a derivative of the derivative, and so on [4].

I have told elsewhere [10] of how others of the Four watched apprehensively this process of abstraction and generalization. Soon Smith's 3-nets had become mere sets of points in a finite vector space, and a Tait colouring was an assignment to those points of non-zero members of the 4-group, the coefficients conforming to the linear relations of the points. It seemed to us other three that our beloved graph theory had vanished into a mist of algebra. "Graph theory" we would explain to our friends "is like the Cheshire cat: the cat has vanished but the grin remains".

Smith's 3-nets as I see them are not matroids but are based on the same principle. Generalize some aspect of graph theory; it shall undergo a change "Into something rich and strange".

I left Cambridge in 1941 with the idea that graph theory could be reduced to abstract algebra, but that it might not be the conventional kind of algebra.

There had been developments since 1935. The Four solved their problem about dissected squares. They wrote a paper about such dissections, eventually published in the Duke Mathematical Journal [1]. They researched on

Hamiltonian circuits. Then a war broke out. I found myself at Bletchley Park, in Buckinghamshire, studying some Continental codes and ciphers. (The work at Bletchley Park was part of the activities of GC & CS, the Government Code and Cipher School.)

I mention this because some of those ciphers posed problems that I thought involved a kind of linear algebra. We would receive an intercepted cipher message that was a long string of letters or teleprinter symbols. That could be called a vector. Call it C for "cipher". In the relevant cases C was formed from two other vectors, P for "plain language" and K for "key". We would have the simple equation

$$C = P + K$$

in some chosen finite arithmetic. The key K would be constructed on some secret machine.

There one had an equation in linear algebra and to start with we, in the Research Section at Bletchley, would know only C. Sometimes mistakes at the European end, such as sending two messages on the same key, would enable us to solve for K and the two P's [2].

In one case of importance, K was a sum of subkeys. Some of these were periodic, advancing one step for each letter. The others were basically periodic but for each new letter they sometimes advanced and sometimes stayed still. These subkeys each involved only two symbols, known to us as "dot" and "cross". The patterns of dot and cross were changed from time to time but the periods of the subkeys were fixed. We called the subkeys "wheels".

Sometimes, knowing C and assuming some statistical properties of P, we were able to disentangle the subkeys of K and determine them all, using a curious mixture of statistics and linear algebra. The problem would be simplified when we knew the cyclic patterns of the wheels and had thereafter only to determine their settings.

The point I want to make is that at Bletchley I was learning an odd new kind of linear algebra; I was still being prepared for the Coming of the Matroids.

I have been warned that this Conference is oriented towards Computer Science. That gives me another reason to mention Bletchley. For there an electronic computer was invented more than half a century ago.

I remember a particular problem of the time and place. We would have a sequence of dots and crosses, at least 2000 long, derived from a cipher message. We would have also a periodic sequence of dots and crosses, of period $31 \times 41 = 1271$, derived from our knowledge of the ciphering machine and its current wheel-patterns. We would want to compare the two in all their 1271 relative settings and pick the setting that gave the best agreement. If there was then a statistically significant agreement we would infer the setting of two wheels and go on to the next stage. Now 1271 comparisons per message were rather too many for the biological computers initially available, so electrical ones were invented and constructed, first with relays and then with thermionic valves (also called vacuum tubes) [2].

A replica of one of the later models can be seen now at Bletchley Park. Over and over again it finds the two sequences of dots and crosses, of periods 31 and 41, whose combination gives the best agreement with a long, long sequence derived from a genuine wartime cipher message.

Late in 1945 I found myself back at Trinity as a Fellow of the College. I now had to work for my PhD degree. What should be the subject of my thesis? Why not that abstractifying of graph theory in a reduction to linear algebra?

Following in the ways of Arthur Stone, I contemplated the additive group of cycles of a graph G, with coefficients in a ring R. Perhaps the coefficients would be integers as with our Kirchhoff chains. Perhaps they would be residues mod 2, as used for Tait cycles. Or perhaps even they would be elements of the four-group of 2-vectors mod 2. Such cycles in cubic graphs, with no zero coefficients, defined the Tait colourings. It seemed that many graph-theoretical entities could be described in terms of these additive cycle-groups.

Each cycle had its "support", the set of graph-edges with non-zero coefficients in it. It seemed good to define an elementary cycle as a non-zero cycle whose support contained that of no other non-zero cycle. That could be abbreviated as a "cycle with minimal (non-null) support". Those elementary cycles corresponded to the circuits of the graph. What a pleasing theorem!

Now I ventured to abstract after the manner of Smith. Forget the graph-structure. Replace it by a finite set S of objects called "cells". Giving a coefficient in R to each cell one got a "chain on S over R". A set of such chains, closed under addition and multiplication by elements of R, was a "chain-group". A cycle-group of a graph was merely a special case of a chain-group.

I went on happily developing a theory of chain-groups and their elementary chains, these latter of course being defined by minimal supports. The method was to select theorems about graphs and try to generalize them to chain-groups. These was not too difficult for theorems expressible in terms of circuits. But theorems about 1-factors imposed problems.

As I look back on this episode I am grieved to recall that I still did not appreciate the work of Whitney. Yet these chain-groups were half-way to matroids and their minimal supports were Whitney's matroid-circuits, his "minimal dependent sets". Perhaps if I had read, marked and learned that paper of Whitney's [17] I would have said "Look, Whitney has done this stuff better already; I will abandon chain-groups and write about other things". That, I think now, would have been a pity.

I understand that Richard Rado was once in a somewhat similar position writing about abstract linear dependence but unaware of the earlier work of Whitney. I get an urge of fellow-feeling with that great man to whom this lecture is dedicated. But my linear dependence was not yet abstract. It was still thoroughly and unadventurously orthodox.

Returning to my own story, I went on to a second stage in chain-group theory. I discussed "binary" chain-groups, those over the ring of residues

mod 2. Binary chain-groups have the interesting property that each chain is uniquely determined by its support. Then I wrote of "regular" chain-groups. These are over the ring of integers. But each elementary chain is restricted to the coefficients 0, 1 and -1, or is an integral multiple of such a chain of the group. An equivalent definition derives a regular chain-group from a totally unimodular matrix, that is, a matrix in which each square submatrix has determinant 1, -1 or 0. The chains correspond to the rows of the matrix and their linear combinations (with integral coefficients). Regular chain-groups were interesting because the cycle-group of a graph, over the integers, was always regular. Last came the "graphic" chain-groups, those that could be represented as integral cycle-groups of graphs.

The later part of my thesis established what would now be called "excluded minor" conditions first for a binary chain-group to be regularizable, that is, to correspond cell to cell and circuit to circuit with a regular chain-group, and then for a regular chain-group to be graphic [5]. All that foreshadowed my own contribution to matroid theory, published some ten years later [6–8].

In the interval I had my thesis accepted and received my PhD degree in 1948. I then became a lecturer at the University of Toronto. By 1958 I was an "Assistant Professor". In the interval I had learned to appreciate matroids. I put the work in my thesis into matroid terminology and generalized from chain-groups to matroids. I found conditions for a given matroid to be "binary", that is, the matroid of a binary chain-group. Then from the thesis-theorems I got the now well-known excluded minor conditions for a binary matroid to be regular and for a regular matroid to be graphic.

I published this work in a 2-part paper entitled "A homotopy theorem for matroids" [6,7]. I do not find that homotopy theorem in the later literature. Perhaps it is mentioned with a warning that it is terribly long and then the author tells of some shorter, slicker proof of the excluded minor conditions. That is the way of Mathematics.

Yet I feel some sadness at the disappearance of the process of homotopy. It began with a geometrical representation of a matroid. The points were the circuits of a matroid, that is, its minimal dependent sets. To any set U of cells could be assigned a "rank", the least number of cells whose removal destroyed all the circuits in U. A union of circuits of rank 2 was a "line" and one of rank 3 was a "plane". And so on. With this terminology you could study matroid theory in a geometrical context provided you bore in mind that two points did not necessarily determine a line, nor three non-collinear points a plane. However two lines in a plane were conventional enough to intersect in a point.

There is a distinction between connected and disconnected lines. A disconnected line has two points only. And these, considered as circuits of the matroid, are disjoint. A connected line has three points. Since the theorem is about binary matroids there cannot be more than three points on a line.

Such combinatorial geometries are still met with. The homotopy paper went on to define a "linear subclass" as a set K of points which with any

two points on a connected line contained also the third. Then attention was directed to those re-entrant paths along the connected lines of the geometry that were "off K", that is, passed through no point of K. To me the most interesting part of the work described in the paper was showing that any such path could be reduced to a null path by a sequence of elementary operations of four kinds.

The first operation replaced

$$XYZYT \quad \text{by} \quad XYT \quad \text{or conversely.}$$

The second replaced

$$XYZTYU \quad \text{by} \quad XYU \quad \text{or conversely,}$$

provided that Y, Z and T were coplanar. The third replaced

$$XYZTUYV \quad \text{by} \quad XYV \quad \text{or conversely,}$$

provided that Y, Z, T and U were coplanar. There were two other points in the plane and these belonged to K.

The fourth operation uses a configuration that can be described briefly as projectively equivalent to a cube with its edges and faces extended to three points at infinity. Any two of these three make up a disconnected line. Four vertices of the cube, no two on the same edge, belong to C. An elementary path of the fourth kind is of the form $AXBYA$ where A and B are "points at infinity" and X and Y are distinct vertices of the cube not in C.

That was the homotopy theorem and I was able to use it to characterize regular matroids. The later result saying when a regular matroid was graphic was guided, in the usual vague graph-to-matroid way, by Kuratowski's Theorem and my favourite proof thereof [8].

One aspect of this work rather upset me. I had valued matroids as generalizations of graphs. All graph theory, I had supposed, would be derivable from matroid theory and so there would be no need to do independent graph theory any more. Yet what was this homotopy theorem, with its plucking of bits of circuit across elementary configurations, but a result in pure graph theory? Was I reducing matroid theory to graph theory in an attempt to do the opposite? Perhaps it was this jolt that diverted me from matroids back to graphs.

Yet I did do some more work on matroids. I can claim to have invented the whirl if not the wheel. And I lectured on matroids at the first formal conference devoted to them [4]. That conference was organised by Jack Edmonds and his colleagues at the National Bureau of Standards in Washington in 1964. To me that was the year of the Coming of the Matroids. Then and there the theory of matroids was proclaimed to the mathematical world. And outside the halls of lecture there arose the repeated cry: "What the hell is a matroid?" In their

text-books Dominic Welsh and James Oxley have attempted to answer that question [3, 11].

Richard Rado took a keen interest in abstract linear dependence, and his name is attached to an important theorem in the theory of transversals and transversal matroids [3, 11]. By the time I met him I was back with graphs and maps, trying to enumerate rooted planar maps of various kinds. My wife and I met Richard and Louise Rado quite often at Waterloo, at Reading and at conferences elsewhere. I enjoyed many stimulating conversations with him. When I spoke of my enumerative work he advised me earnestly to use exponential generating functions. Alas, I still have not found a way of doing that.

References

[1] R. L. Brooks, C. A. B. Smith, A. H. Stone & W. T. Tutte, The dissection of rectangles into squares, *Duke Mathematical Journal*, **7** (1940), 312–340.

[2] F. H. Hinsley and Alan Stripp, editors, *Codebreakers*, Oxford University Press (1993).

[3] J. G. Oxley, *Matroid Theory*, Oxford University Press (1992).

[4] C. A. B. Smith, Map colourings and linear mappings, in *Combinatorial Mathematics and its Applications, Proceedings of a Conference held at the Mathematical Institute, Oxford, from 7–10 July 1969*, (ed. D. J. A. Welsh), Academic Press, London (1969), pp. 259–283.

[5] W. T. Tutte, An Algebraic Theory of Graphs, PhD Thesis, Cambridge, 1948.

[6] W. T. Tutte, A homotopy theorem for matroids, I, *Transactions of the American Mathematical Society*, **88** (1958), 144–160.

[7] W. T. Tutte, A homotopy theorem for matroids, II, *Transactions of the American Mathematical Society*, **88** (1958), 161–174.

[8] W. T. Tutte, Matroids and Graphs, *Transactions of the American Mathematical Society*, **90** (1959), 527–552.

[9] W. T. Tutte, Lectures on Matroids, *Journal of Research of The National Bureau of Standards, Series B, Mathematics and Mathematical Physics*, **69B** (1965), 1–47.

[10] W. T. Tutte, *Graph Theory As I have Known It*, Oxford University Press (1998).

[11] D. J. A. Welsh, *Matroid Theory*, Academic Press, London (1976).

[12] H. Whitney, A theorem on graphs, *Annals of Mathematics 2*, **32** (1931), 378–390.

[13] H. Whitney, The colouring of graphs, *Annals of Mathematics 2*, **33** (1932), 688–718.

[14] H. Whitney, A logical expansion in mathematics, *Bulletin of the American Mathematical Society*, **38** (1932), 572–579.

[15] H. Whitney, 2-isomorphic graphs, *American Journal of Mathematics*, **55** (1933), 245–254.

[16] H. Whitney, Non-separable and planar graphs, *Transactions of the American Mathematical Society*, **34** (1932), 339–362.

[17] H. Whitney, On the abstract properties of linear dependence, *American Journal of Mathematics*, **57** (1935), 509–533.

[18] H. Whitney & W. T. Tutte, Kempe chains and the four colour problem, *Utilitas Mathematica*, **2** (1972), 241–281.

151 Manderston Road
Newmarket
Suffolk CB8 0NS

Appendix I: geometrical terminology

Given a matroid M on a set E, a rank $r(S)$ can be assigned to each subset S of E. In terms of circuits, the rank is the least number of cells of S whose deletion destroys all the circuits of M contained in S. (The "cells" of M are the elements of E.) The rank of E is called also the rank $r(M)$ of M, and similarly $r(S)$ is the rank of $M \times S$, the matroid on S whose circuits are those of M contained in S.

There is another matroid $M \cdot S$ on S. Its circuits are those non-null intersections with S of circuits of M that contain no other such intersections.

The rank-function has the following important properties, where S and T are subsets of E:

$$r(M \times S) + r(M \cdot (E - S)) = r(M), \tag{1}$$

$$r(S \cup T) + r(S \cap T) \geq r(S) + r(T). \tag{2}$$

In [9] it is found convenient to define a "flat" as a union of circuits, the null subset of E being counted as a flat of rank zero. Each $S \subseteq E$ defines a flat $\langle S \rangle$, the union of the circuits contained in S. Noticing some geometrical analogies the author of [9] experimented with a geometrical terminology in which circuits were "points", flats of rank 2 were "lines", those of rank 3 were "planes" and those of rank 4 were "3-spaces". Even the rank $r(S)$ was replaced by the more geometrical "dimension" $d(S) = r(S) - 1$.

The geometrical analogy is not perfect. Two distinct points determine a unique flat, their union as subsets of E, but this flat is not necessarily a line. However, if flat S is properly contained in flat T (as a subset of E) then

$$d(S) < d(T), \tag{3}$$

by (1). Two lines in the same plane intersect in a unique point, and two planes in the same 3-space intersect in a unique line, by (2).

A feature of this geometry was that a distinction had to be made between connected and disconnected flats. A "separator" U of a flat S is a subset of S such that each circuit of M in S is contained either in U or in $S - U$. Thus S and the null subset of E are always separators of S. If S has any other separator it is disconnected; otherwise it is connected.

Elementary matroid theory established some properties of connected and disconnected flats. For example a disconnected line was on exactly two points and a connected one on at least three. Also, a connected d-flat S, that is, a flat of dimension d, on a connected $(d+2)$-flat T was on two distinct connected $(d+1)$-flats contained in T, the union of the two being T.

At this stage the writer's attention was drawn to the graph $G(M)$ of M. The vertices of this graph are the points of M. Two points are adjacent in $G(M)$ if and only if they are on the same connected line of M. Graph-theoretical concepts could now be introduced, such as paths. There were

simple paths (that use no vertex twice), re-entrant paths (which return to their starting points) and the conventional degenerate paths (each confined to a single vertex and counted as re-entrant). There was the pleasing theorem that a flat S is connected if and only if any two distinct points on S can be joined by a simple path in S. Attempts could be made to construct homotopy theorems saying that any re-entrant path could be reduced by suitably defined "elementary operations" to a degenerate path.

Alas, an important possible application made necessary a further complication. In an inductive argument a matroid M_1 on a set E_1 was to be reduced to

$$M = M_1 \cdot (E_1 - \{a\})$$

where $a \in E_1$ and $E_1 - \{a\}$ can be identified with E. The object was to show that if M had a certain property P then so did M_1. But it was found necessary to impose on M a sort of shadow of M_1. This took the form of a subset Q of the set of points of M, the set of all circuits of M that were also circuits of M_1 (without requiring the adjunction of a).

In order to cope with Q without mentioning M_1 a new definition had to be made. A "linear subclass" of M was defined as a set C of points of M such that if two points on a line L belonged to C then so did all the other points of L. Then Q was just one of the linear subclasses of M.

A new homotopy theorem was needed. The matroid M was taken with an arbitrarily chosen linear subclass C and the theorem concerned only those re-entrant paths that were "off C", that is passed through no point of C. Elementary operations were defined within structures of three or fewer dimensions that might include points of C. In the final theorem there were four of these basic structures. They are briefly described in the main text of the Lecture. In [9] the theorem is proved in the geometrical terminology and each main step in the proof is illustrated by a geometrical diagram.

Appendix II: binary and regular matroids

In [9] we considered a binary matroid M on a set E. The distinguishing feature of a binary matroid is that it has exactly three points on each connected line. Any two of these three points must have a non-null intersection as subsets of E, by the connection of the line. A binary matroid becomes "regular" if it can be "co-ordinatized" in the following way. With each circuit S of M we associate a chain $f(S)$ on E with support S and with coefficients restricted to the integers 1, -1 and 0. Now on any connected line L of M there are just three points, S, T and U say. As part of the co-ordinatization we require that their chains $f(S)$, $f(T)$ and $f(U)$ shall be linearly dependent. This means that each of them is a sum or difference of the other two. Note the following implication: the product of its coefficients in $f(S)$ and $f(T)$ has the same value $+1$ or -1 for each cell of $S \cap T$.

If such a co-ordinatization exists its chains $f(S)$ generate a chain-group N on E, and Theorem 5.11 of [9] assures us that its matroid $M(N)$ is identical with M. We can then say that M is regular as well as binary, and that N is a regular chain-group with matroid M.

With regard to the line L of the preceding paragraph and its points S, T and U we write $\mu(S,T)$ for the product of the coefficients in S and T of a cell of the non-null set $S \cap T$.

The main application of the homotopy theorem in [9] is in a proof that a binary matroid is regular if it has no Fano matroid or dual thereof as a minor. In that proof we assume a binary matroid M_1 (on a set E_1) that has neither of these forbidden minors and yet is not regular, and we take M_1 to have the least number of cells consistent with this description. We choose a cell $a \in E_1$ and write

$$M = M_1 \cdot E, \quad \text{where} \quad E = E_1 - \{a\}.$$

We then note that the binary matroid M is regular since it has no forbidden minor and has fewer cells than M_1.

We may assume that the set $\{a\}$ is not a circuit of M_1; if it were, the regularity of M_1 would follow at once from that of M. Some circuits of M will be circuits also of M_1. These constitute a linear subclass C of M. The other circuits of M are made into the remaining circuits of M_1 by the adjunction of a. A line L of M either has all its points of the first kind, that is, in C, or it has one point of the first kind and two of the second.

In [9] the homotopy theorem is used to prove the following result: either the product of the numbers $\mu(S,T)$ around any re-entrant path off C is 1 or one of the four kinds of basic structures occurs in M in such a way as to impose a forbidden minor on M_1. But the latter alternative is ruled out by the definition of M_1.

A co-ordinatization of M can now be extended to M_1. For consider any connected line L in M with one point U in C and two points S and T not in C. By adjunction of a this becomes a line L_a of M_1 with points U, S_a and T_a,

the two last being extensions of S and T. In the co-ordinate-extension each of S_a and T_a receives a number 1 or -1 as the co-ordinate of a. And if we are to prove M_1 regular the product of the two numbers must be $\mu(S,T)$. The theorem noted in the preceding paragraph shows that the coefficients of a can be assigned consistently with this requirement. So, by another application of Theorem 5.11 of [9], M_1 is regular, contrary to assumption.

The Invited Lectures

Polynomials in Finite Geometries

S. Ball

Summary A method of using polynomials to describe objects in finite geometries is outlined and the problems where this method has led to a solution are surveyed. These problems concern nuclei, affine blocking sets, maximal arcs and unitals. In the case of nuclei these methods give lower bounds on the number of nuclei to a set of points in $\mathrm{PG}(n,q)$, usually dependent on some binomial coefficient not vanishing modulo the characteristic of the field. These lower bounds on nuclei lead directly to lower bounds on affine blocking sets with respect to lines. A short description of how linear polynomials can be used to construct maximal arcs in certain translation planes is included. A proof of the non-existence of maximal arcs in $\mathrm{PG}(2,q)$ when q is odd is outlined and some bounds are given as to when a (k,n)-arc can be extended to a maximal arc in $\mathrm{PG}(2,q)$. These methods can also be applied to unitals embedded in $\mathrm{PG}(2,q)$. One implication of this is that when q is the square of a prime a non-classical unital has a limited number of Baer sublines amongst its secants.

1 Introduction

The effectiveness of polynomials as a means of studying problems in finite geometries has become increasingly evident in the 1990's, although the first examples seem to date back to R. Jamison [38] in 1977 and A. E. Brouwer and A. Schrijver [19] in 1978. Indeed in [22] A. A. Bruen and J. C. Fisher described the "Jamison method" as the following: reformulate the problem in terms of points of an affine space and associate suitable polynomials defined over the corresponding finite field; calculate. This is the approach employed in [19] too; in fact the main difference between [38] and [19] is that Jamison viewed the points of an affine space as elements of a finite field. In effect, this has the advantage of reducing the number of variables in the polynomials and allowing one to use simple arguments concerning the degree or the coefficients of a polynomial. Earlier survey papers covering polynomial applications to finite geometries include [11], [12] and [53] and in some ways the present paper is an update of those, although there is much material in those articles that is not covered here.

In general, we are interested in solving problems of the form: Given a set of subspaces (usually points) in a Desarguesian space with restricted intersections with larger subspaces (usually lines), what can we say about the size of the set and can we characterise the extremal cases? Historically this stems from the famous proof of B. Segre [49] that any set of $q+1$ points in the Desarguesian plane of odd order q having at most two points on a line is a conic.

Section 2 considers polynomials whose zeros correspond to subspaces of Desarguesian affine and projective spaces. This leads us to define polynomials,

given an arbitrary set of points $\mathcal{S}$, whose properties reflect the properties of $\mathcal{S}$. These polynomials are fundamental to many of the proofs of the results covered in this paper.

Section 3 updates results concerning nuclei. It is not a complete survey; indeed emphasis is given to those results for which the polynomials in Section 2 have been the most useful. The intriguing conjecture from [16] is included. Following on directly from the bounds in Section 3, lower bounds on the size of affine blocking sets are detailed. I include a general definition for blocking sets in affine and projective spaces in the hope that this will be adopted. Since the early 1990's there have appeared conflicting definitions by various authors, which has led to some confusion. I have not surveyed recent developments in projective blocking sets, there being too much material for the scope of this paper. However a survey from 1997 can be found in [37, Chapter 13]. The recent constructions by G. Lunardon [40] and by P. Polito and O. Polverino [47] concerning linear blocking sets are the most notable developments since then.

Section 5 leaves surveying aside and gives details of how one can view translation planes with polynomials using the construction of André [1] and Bruck and Bose [20], in the hope of proving algebraic results previously only possible in Desarguesian planes. Returning to the surveying, Section 6 contains recent results and constructions concerning maximal arcs, including a sketch of the non-existence proof for Desarguesian planes. A construction of some maximal arcs in translation planes using polynomials is also included.

Finally Section 7 considers unitals embedded in a Desarguesian plane. The classification of such objects appears to be a very hard problem; some characterisations can be obtained from polynomial arguments.

Where possible I have put definitions in their relevant sections in such a way that each section is self-standing. However, the construction in Section 6 is dependent on Section 5 and Section 4 is closely related to Section 3.

2 Definitions and useful polynomials

Let π_n denote a projective space of dimension n and $\mathrm{PG}(n,q)$ the Desarguesian space of order q. Let $\mathcal{A}_n$ denote an affine space of dimension n and $\mathrm{AG}(n,q)$ the Desarguesian space of order q. Throughout, $\theta_n = (q^{n+1}-1)/(q-1)$, the number of points of π_n, and $q = p^h$ for some prime p.

2.1 Affine spaces

The elements of $\mathrm{GF}(q^n)$, where $q = p^h$ for some prime p, can be viewed as the points of $\mathrm{AG}(n,q)$. The points lying on a hyperplane are given by the zeros of equations

$$\mathrm{Tr}_{q^n \to q}(ax) + b = 0,$$

where b is an element of GF(q) and $\mathrm{Tr}_{q^n \to q}(x) = x^{q^{n-1}} + x^{q^{n-2}} + \ldots + x^q + x$ is the trace function from GF(q^n) to GF(q). To see this, note that the polynomial should have degree q^{n-1}. Every hyperplane in AG(n, q) is a translate of a hyperplane through the origin; this translate can be seen as an $(n-1)$-dimensional subspace over GF(q), and the corresponding polynomial is therefore GF(q)-linear and so of the form

$$H(x) := \sum_{j=0}^{n-1} a_j x^{q^j} + b.$$

R. Jamison provided a proof of this [38, Lemma A, p. 259] which he credited to O. Ore, who wrote two expositions on polynomials of the form (1) [44, 45]. These polynomials are called linearized polynomials, see [39, Chapter 3, Section 4]. The polynomial

$$a_{n-1} H^q - a_{n-1}^{q+1}(x^{q^n} - x) - a_{n-2}^q H$$

has degree at most q^{n-2} and since all the points of the hyperplane are zeros it is identically zero. Equating coefficients of x^{q^i} for $0 \leq i \leq n-2$ implies the trace function form above.

A suitable linear combination of k hyperplane polynomials will give an equation of the form

$$\sum_{j=0}^{n-k-1} \alpha_j x^{q^j} + \beta = 0, \tag{1}$$

whose zeros correspond to a subspace of dimension $n-k-1$ that is, the intersection of the corresponding k hyperplanes. In particular, lines are given by the sets of zeros of equations of the form

$$x^q - \alpha x + \beta = 0,$$

and for a line joining a point x and a point y (viewed as elements of GF(q^n)) we have $\alpha = (x-y)^{q-1}$. The non-zero $(q-1)$-th powers are θ_{n-1}-th roots of unity in GF(q^n), so there is a one-to-one correspondence between the θ_{n-1}-th roots of unity in GF(q^n) and the θ_{n-1} directions of lines in AG(n, q).

Given a set of points $\mathcal{S}$, a subset of AG(n, q), viewed as elements of GF(q^n) and not containing the zero element, define the *locator polynomial* (Jamison would call this the *root polynomial* and were $\mathcal{S}$ to be a subspace the *Ore polynomial*) of $\mathcal{S}$ to be

$$S(x) := \prod_{s \in \mathcal{S}} (1 - sx) = \sum_{j=0}^{|\mathcal{S}|} (-1)^j \sigma_j x^j,$$

where σ_j is the j-th symmetric function of the set $\mathcal{S}$. Strictly speaking this is the locator polynomial for the set $\{1/s \mid s \in \mathcal{S}\}$ since these are the zeros

of $S(x)$, but we choose to define it this way simply so that the coefficient of $(-1)^j x^j$ in $S(x)$ is the j-th symmetric function.

Define the *direction polynomial* of a set $\mathcal{S}$ to be

$$F(u,x) := \prod_{s\in\mathcal{S}}(1-(1-sx)^{q-1}u) = \sum_{j=0}^{|\mathcal{S}|}(-1)^j\chi_j(x)u^j,$$

where $\chi_j(x)$ is the j-th symmetric function of the set $\{(1-sx)^{q-1} \mid s\in\mathcal{S}\}$, a polynomial in x of degree at most $k(q-1)$. If $F(u,x_0)$ is viewed as a polynomial in u, its zeros are θ_{n-1}-th roots of unity and moreover

$$(1-s_1x_0)^{q-1} = (1-s_2x_0)^{q-1}$$

if and only if $(1/x_0-s_1)^{q-1} = (1/x_0-s_2)^{q-1}$ if and only if $1/x_0$, s_1 and s_2 are collinear.

2.2 Projective spaces

The $(q-1)$-th powers of the elements of $\mathrm{GF}(q^{n+1})$ can be viewed as the directions of the lines through the origin in $\mathrm{AG}(n+1,q)$ and hence the points of $\mathrm{PG}(n,q)$. The hyperplanes through the origin are given by zeros of equations of the form

$$\mathrm{Tr}_{q^{n+1}\to q}(AX) = 0 = AX\sum_{i=0}^{n}A^{q^i-1}X^{q^i-1},$$

and by writing $x = X^{q-1}$ and $a = A^{q-1}$ the hyperplanes of $\mathrm{PG}(n,q)$ are given by the zeros of equations of the form

$$\sum_{i=0}^{n}a^{(q^i-1)/(q-1)}x^{(q^i-1)/(q-1)} = 0.$$

As in the affine case, taking a suitable linear combination of k hyperplane polynomials, one can obtain an equation of the form

$$\sum_{j=0}^{n-k-1}\alpha_j x^{\theta_j} + \beta = 0$$

whose zeros correspond to the points of a subspace of dimension $n-k-1$, that is the intersection of the corresponding k hyperplanes. In particular, lines are given by the sets of zeros of equations of the form

$$x^{q+1} - \alpha x + \beta = 0,$$

where there exist relations between α and β depending on the dimension, and for a line joining a point x and a point y (viewed as $(q-1)$-th power of $\mathrm{GF}(q^{n+1})$) we have

$$\alpha = (x^{q+1}-y^{q+1})/(x-y).$$