Chapter 41

COMBINATORICS IN PURE MATHEMATICS

László Lovász
Department of Mathematics,
Yale University,
New Haven, CT 06520, USA

László Pyber
Mathematical Research Institute
Hungarian Academy of Sciences
Budapest, Hungary H-1053

Dominic J. A. Welsh
Merton College
Oxford OX1 4JD, United Kingdom

Günter M. Ziegler
Konrad-Zuse-Zentrum für
Informationstechnik Berlin (ZIB)
D-10711 Berlin, Germany

It is a beautiful feature of mathematics that quite often results and methods from one branch can be applied to solve problems in a seemingly distant branch in a successful and often surprising way. In fact, classical fields like analysis or linear algebra belong to the toolbox of every mathematician. In virtually no field would one be surprised to see a generating function or the computation of the eigenvalues of a matrix. This *Handbook* contains several chapters showing how algebra, topology, probability theory etc. can be applied to combinatorial problems in a deep way.

The application of combinatorial methods in other areas is not so common (this may be due to the – relative – youth of the subject). This chapter contains a collection of examples showing the application of a variety of combinatorial ideas to other areas.

In some cases, it is a specific combinatorial theorem that is used. For example, in section 1, theorems from extremal combinatorics are applied in the theory of finite dimensional Banach spaces, to prove embeddability and near-embeddability results. In section 3, the Marriage Theorem is applied to give a very simple constructive proof for the existence of the Haar measure on compact topological groups.

Elsewhere, it is a combinatorial structure whose presence should be recognized to shed light on a seemingly hopelessly complicated situation. Section 4 illustrates the use of graphs and coherent configurations in the study of permutation groups. Finding the combinatorial structure which retains just enough of the group structure is the key point. Section 5 describes a method to analyze a commutative ring (like, for example, the coordinate ring of a Grassmann or Schubert variety) by writing it as an *algebra with straightening law* over a finite poset, and then utilize poset combinatorics to identify algebraic structure of the ring and to prove fundamental algebraic properties of some classical projective varieties. Section 6 shows how the algebraic and topological structure of a *complex hyperplane arrangement* is determined by the intersection lattice of the arrangement (i.e., by a matroid).

And in some cases, problems with a very classical flavour turn out to be so closely related to combinatorial problems that even the direction of the interaction is difficult to tell. In section 2 we see how embeddings of finite metric spaces in classical Banach spaces are related to "hypermetric inequalities", to multicommodity flows, and to lattice-point-free ellipsoids. In section 7 we sketch how a recent topological invariant of knots, the Jones polynomial, can be derived from the Tutte polynomial of an appropriate graph, and how this connection can be used to settle a long-standing conjecture in the theory of knots.

1. Sections of finite dimensional Banach spaces

It is well known that if N_1 and N_2 are two norms on a finite dimensional real linear space $\mathbb{R}^n$ then there exist constants $c_1, c_2 > 0$ such that

$$c_1 N_1(x) \leq N_2(x) \leq c_2 N_1(x)$$

for all vectors x. These constants depend on the norms; but if we allow a linear transformation, then any given norm N_1 can be transformed into one which is more similar to a given other norm N_2. In fact, let $K = K(N_1) = \{x \in \mathbb{R}^n : N_1(x) \leq 1\}$ be the unit ball of the first norm; this is a convex body centrally symmetric with respect to the origin. It can be shown that there exists an ellipsoid E inscribed in K with maximum volume and it is unique; E is called the inscribed Löwner–John ellipsoid of K (cf. Chapters 19 and 30, and also Grötschel, Lovász and Schrijver 1988). Perhaps the most important property of E is that if we blow up E by a factor of $\sqrt{n}$ then the resulting ellipsoid will contain K (for this result, the central symmetry of K is needed; for general convex bodies, $\sqrt{n}$ has to be replaced by n).

If we apply a linear transformation that maps E onto the unit ball, then N_1 will be transformed into a norm N_1' satisfying

$$\frac{1}{\sqrt{n}} \|x\| \leq N_1'(x) \leq \|x\|$$

(here $\|x\|$ denotes the euclidean norm). Applying this argument to the other norm as well we get that N_1 can be transformed by a linear transformation into a norm N_1'' such that

$$N_1''(x) \leq N_2(x) \leq n N_1''(x)$$

for all $x \in \mathbb{R}^n$.

One can achieve a better approximation if one is allowed to restrict the norms to appropriate subspaces; this way one obtains theorems with the flavor of Ramsey's Theorem (see Chapter 25). A classical result of Dvoretzky (1959) asserts that *for every positive integer k and every $\varepsilon > 0$ there exists an $n = n(k, \varepsilon) > 0$ such that for every norm N on $\mathbb{R}^n$ there exists a constant $C > 0$ and a subspace V of $\mathbb{R}^n$ with dimension k such that for every $x \in V$,*

$$C \cdot \|x\| \leq N(x) \leq (1+\varepsilon)C \cdot \|x\|.$$

The following result of Figiel, Lindenstrauss and Milman (1977) illustrates how to obtain finer measures of the approximation of an arbitrary norm by the euclidean norm on a subspace. Let $M_2 = M_2(N)$ denote the square root of the average of $N(x)^2$ over all vectors with unit euclidean length. Then *for every $\varepsilon > 0$ there exists a $\delta > 0$ such that for every norm N on $\mathbb{R}^n$ such that $N(x) \leq \|x\|$ there exists a subspace V with dimension at least $\delta n M_2^2$ such that $N(x) \geq (1-\varepsilon)\|x\|$ for every $x \in V$.*

The proof of such results on the ℓ_2 norm is geometric. Our main topic will be two results with a similar flavour concerning the ℓ_1-norm $\|x\|_1 = \sum_i \|x_i\|$ and the ℓ_∞-norm $\|x\|_\infty = \max_i \|x_i\|$. Both proofs use a number of combinatorial tools.

We introduce some quantities analogous to the quantity $M_2(N)$ defined above. Let N be an arbitrary norm on $\mathbb{R}^n$. Let $M_1 = M_1(N)$ denote the average of $N(x)$ over all ± 1-vectors, and $M_\infty = M_\infty(N)$, the maximum of $N(x)$ over all ± 1 vectors. If we have $N(e_i) = 1$ for all i then $1 \leq M_1(N) \leq n$, with equality in the first inequality iff $N = \|.\|_\infty$ and equality in the second inequality iff $N = \|.\|_1$.

Note that $N(x)$ is a convex function and hence we could take the maximum over the whole cube spanned by $\{-1,1\}^n$ (the unit ball of $\|.\|_\infty$) instead. So we have

$$N(x) \leq M_\infty \|x\|_\infty$$

for all x.

We can also formulate an opposite inequality. Assume that $N(e_i) = 1$ for $i = 1, \ldots, n$. Let $b_i^T x = 1$ be the equation of a supporting hyperplane to K at the point e_i (so b_i is in the polar body). Set $b_i = (b_{i1}, \ldots, b_{in})^T$; then $b_{ii} = 1$. Note that $M_\infty \geq \max_i \sum_j |b_{ij}|$. Let

$$M_0 = \min_i \min_{\substack{x \in \{-1,1\}^n \\ x_i = 1}} b_i^T x = \min_i \left\{ 1 - \sum_{i \neq j} |b_{ij}| \right\}$$

(this may be negative, which will be a trivial case). For any vector $x \in \mathbb{R}^n$, we have

$$N(x) = \max\{b^T x : \ b \in K^*\}.$$

Let i be the index with $|x_i|$ maximum, and assume that, say, $x_i \geq 0$. Then

$$N(x) \geq b_i^T x = \sum_j x_j b_{ij} \geq x_i - \sum_{j \neq i} |x_j| \cdot |b_{ij}| \geq x_i \left(1 - \sum_{j \neq i} |b_{ij}| \right) = M_0 \|x\|_\infty.$$

Our first topic is a theorem of Milman (1982). Let N be a norm in $\mathbb{R}^n$ whose unit ball is a polyhedron (this is so far not a very severe restriction since any norm can be approximated arbitrarily well by a polyhedral norm). Then N can be written as $N(x) = \|Ax\|_\infty$ with an appropriate matrix $A: \mathbb{R}^m \to \mathbb{R}^n$. Now assume that every entry of A is 1 or -1. Then A has at most 2^n distinct rows. Observe that if the number of rows is exactly 2^n then $N(x) = \|x\|_1$.

1.1 Theorem. *If $N(x) = \|Ax\|_\infty$, where A is a ± 1 matrix with m (distinct) rows and n columns, then there exists a linear subspace $V \subseteq \mathbb{R}^n$ with $\dim V \geq \lfloor \log m / \log n \rfloor$ such that the restriction of N to V is isometric to an ℓ_1 norm.*

Proof. Let $k = \lfloor \log m / \log n \rfloor$; we may assume that $k > 1$. Then $m \geq n^k > 1 + n + \binom{n}{2} + \cdots + \binom{n}{k}$, and hence by the Sauer–Shelah theorem (Chapter 24, Theorem 4.9), we can choose k columns of A (say, the first k columns) such that every ± 1-vector arises as the restriction of some row of A to these columns. Let V be the subspace of $\mathbb{R}^n$ consisting of those vectors whose last $n - k$ coordinates are 0. Then for every $v \in V$,

$$N(v) = \|Av\|_\infty = \max_i \left| \sum_{j=1}^k a_{ij} v_j \right| = \sum_{j=1}^k |v_j| = \|v\|_1,$$

since the maximum is attained for the row of A for which $a_{ij} = \operatorname{sign} v_j$. ∎

A corollary of this theorem uses the quantity M_1 to bound the dimension of V:

1.2 Corollary. *If $N(x) = \|Ax\|_\infty$, where A is a ± 1-matrix, then there exists a linear subspace $V \subseteq \mathbb{R}^n$ with $\dim V \geq M_1^2 / (2n \log n)$ such that the restriction of N to V is isometric to an ℓ_1 norm.*

Proof. Assume that A has m distinct rows; trivially, $m \geq n$. We show that $M_1 < \sqrt{2n \log m}$; this then implies that the subspace V in the assertion of theorem 1.1 satisfies $\dim V \geq M_1^2 / (2n \log n)$.

We want to bound, for a random ± 1 vector w, the expectation of $\|Aw\|_\infty$. Let $a_1, \ldots, a_m$ be the rows of A. Then $a_i w$ is the sum of n independent random variables assuming 1 and -1 with equal probability, and hence by Chernoff's inequality (see Chapter 33),

$$\operatorname{Prob}\big(|a_i w| > \sqrt{n \log m}\big) < e^{-2 \log m} = \frac{1}{m^2}.$$

Hence

$$\operatorname{Prob}\big(\max_i |a_i w| > \sqrt{n \log m}\big) < m \cdot e^{-2 \log m} = \frac{1}{m},$$

and so the expectation of $\|Aw\|_\infty$ is at most $(1 - 1/m)\sqrt{n \log m} + n/m < \sqrt{2n \log m}$. (This argument is essentially the same as the probabilistic upper bound on the discrepancy of a hypergraph with n vertices and m edges; cf. Chapter 26). ∎

The next result whose proof uses combinatorial tools is due to Alon and Milman (1983).

1.3 Theorem. *Let N be any norm on $\mathbb{R}^n$ such that $N(e_i) = 1$ for all i.*

(i) *There exists a subspace V spanned by $\lfloor\sqrt{n}\rfloor$ basis vectors e_i such that $M_\infty(N|_V) \leq 8M_1(N)$; in other words we have, for all $x \in V$,*

$$N(x) \leq 8M_1\|x\|_\infty.$$

(ii) *For every $\varepsilon > 0$ there exists a subspace V spanned by $\lfloor\varepsilon n/(8M_\infty)\rfloor$ basis vectors e_i such that $M_0(N|_V) \geq 1 - \varepsilon$, and hence we have for all $x \in V$,*

$$(1-\varepsilon)\|x\|_\infty \leq N(x).$$

Combining (i) with (ii) we obtain that there exists a subspace V spanned by $\lfloor\sqrt{n}/(128M_1)\rfloor$ basis vectors e_i such that for all $x \in V$,

$$\frac{1}{2}\|x\|_\infty \leq N(x) \leq 8M_1\|x\|_\infty.$$

Proof. (i) This part of the proof uses a combinatorial lemma which is analogous to the Sauer–Shelah Theorem. Let $h(n,k)$ denote the smallest integer for which the following holds: whenever $R \subseteq \{-1,1\}^n$ with $|R| > h(n,k)$, then there exists a subset $I \subseteq \{1,\dots,n\}$ with $|I| = k$ such that for every $q \in \{-1,1\}^S$ there exist two vectors $u, w \in R$ such that $u_i = w_i = q_i$ if $i \in I$ and $u_i = -w_i$ if $i \notin I$.

1.4 Lemma.

$$h(n,k) = \begin{cases} \displaystyle\sum_{i=0}^{(n+k-1)/2} \binom{n}{i}, & \text{if } n+k \text{ is odd,} \\ \displaystyle\binom{n-1}{(n+k)/2} + \sum_{i=0}^{(n+k-2)/2} \binom{n}{i}, & \text{if } n+k \text{ is even.} \end{cases}$$

For a proof of this lemma, which uses the “down-shift” technique (cf. Chapter 24), we refer to the original paper.

Now let R denote the set of vectors $w \in \{-1,1\}^n$ such that $N(w) \leq 8M_1$. Let k be the least integer such that $k \geq \sqrt{n}$ and $k \equiv n-1 \pmod 2$. Then

$$M_1 = 2^{-n} \sum_{w\in\{-1,1\}^n} N(w) \leq 2^{-n}(2^n - |R|)(8M_1),$$

whence (if n is large enough)

$$|R| \geq \frac{7}{8}2^n > \sum_{i=0}^{(n+k-1)/2} \binom{n}{i}.$$

Hence by Lemma 1.4, there exists a subset $I \subseteq \{1, \ldots, n\}$ such that $|I| = k$ and for every $q \in \{-1, 1\}^S$ there exist two vectors $u, w \in R$ such that $u_i = w_i = q_i$ if $i \in I$ and $u_i = -w_i$ if $i \notin I$. We claim that the subspace V spanned by $\{e_i : i \in I\}$ satisfies the requirement in (i).

By our discussion of M_∞, it suffices to show that for every $\pm$-vector v spanned by e_i $(i \in I)$ we have $N(q) \leq 8M_1$. To this end, let q be the restriction of v to the coordinates in I and consider the vectors $u, w \in R$ as above. Then $v = (1/2)(u + w)$ and hence

$$N(v) \leq \frac{1}{2}\big(N(u) + N(w)\big) \leq 8M_1.$$

(ii) The proof of this second part also uses a lemma with a combinatorial flavor (Johnson and Schechtman 1981):

1.5 Lemma. *Let A be an $n \times n$ matrix with non-negative entries and with 0's in the diagonal. Assume that each row-sum of A is at most D. Then for every $k \geq 1$, A has a $k \times k$ principal submatrix A' such that each row-sum of A' is at most $8kD/n$.*

This lemma can be cast in graph-theoretic terms: *If G is a directed graph with maximum outdegree D and $k \geq 1$, then G contains an induced subgraph on k nodes with maximum outdegree at most $8kD/n$.* For undirected graphs, this follows from a theorem of Lovász asserting that *if G is an undirected graph with maximum degree D and $t \geq 1$ then the nodes of G can be partitioned into $\lceil (D-1)/t \rceil$ classes such that each class induces a subgraph with maximum degree at most t* (cf. Chapter 4, Theorem 4.2). The directed version follows by deleting the nodes with indegree larger than $2D$ (this means at most half of the nodes), and then applying the undirected version to the remaining graph, disregarding the orientation.

Return to the proof of Theorem 1.3. Let $k = \lfloor \varepsilon n/(8M_\infty) \rfloor$. With the notation introduced at the beginning of the section, consider the matrix $P = (p_{ij})$ defined by

$$p_{ij} = \begin{cases} 0, & \text{if } i = j, \\ |b_{ij}|, & \text{if } i \neq j. \end{cases}$$

Then every row-sum of P is bounded by M_∞:

$$\sum_j p_{ij} \leq \sum_j |b_{ij}| \leq M_\infty.$$

Hence by Lemma 1.4, A has a $k \times k$ principal submatrix in which every row-sum is at most ε. Let, say, the upper left $k \times k$ submatrix of P have this property, and let V be the subspace spanned by $e_1, \ldots, e_k$. Then

$$M_0(N|_V) = \min_{i \leq k} \left(1 - \sum_{\substack{j \leq k \\ j \neq i}} |b_{ij}| \right) \geq 1 - \varepsilon,$$

and hence for every $x \in V$,

$$N(x) \geq (1-\varepsilon)\|x\|_\infty. \qquad \blacksquare$$

We remark that by a rather standard "partitioning" argument one can improve the upper bound in (i) at the cost of decreasing the dimension of the subspace, and prove the following:

1.6 Corollary. *For every norm N on $\mathbb{R}^n$ and every $\varepsilon > 0$ there exists a linear embedding $A:\ \mathbb{R}^k \to \mathbb{R}^n$ where $k = n^{\varepsilon/(4\log M_1)}$ such that for every $x \in \mathbb{R}^k$,*

$$\|x\|_\infty \leq N(Ax) \leq (1+\varepsilon)\|x\|_\infty.$$

2. Embeddings of finite metric spaces and hypermetric inequalities

Let us start by recalling the following classical result of Cayley:

2.1 Theorem. *A symmetric matrix $D = (d_{ij})_{i=1}^{n}{}_{j=1}^{n}$ is the matrix of mutual distances of n (not necessarily distinct) points in $\mathbb{R}^n$ (or in the Hilbert space) if and only if $D \geq 0$, $d_{ii} = 0$ for all i, and the matrix $(a_{ij})_{i,j=1}^{n-1}$ is positive semidefinite, where*

$$a_{ij} = d_{in}^2 + d_{jn}^2 - d_{ij}^2.$$

The proof of this theorem is rather straightforward linear algebra. Another way to state this condition is that the matrix $D^{(2)}$ obtained by squaring each entry of D is *of negative type*, which means that for every vector $x \in \mathbb{R}^n$ with $\sum_i x_i = 0$, we have

$$\sum_i \sum_j d_{ij}^2 x_i x_j \leq 0.$$

We may ask analogous questions about embeddability in other important Banach spaces, such as the L_1 space. The answer to such questions often leads to combinatorial considerations which tie these issues to polyhedral combinatorics, lattice geometry, and flow theory.

So let D be an $n \times n$ matrix and assume that D is the matrix of mutual distances of n points in L_1. There are some obvious conditions that D has to satisfy:

$$d_{ij} = d_{ji}, \tag{2.2}$$

$$d_{ij} \geq 0, \tag{2.3}$$

(2.4) $$d_{ii} = 0,$$

and of course the triangle inequality:

(2.5). $$d_{ij} + d_{jk} \geq d_{ik}.$$

A matrix satisfying these conditions is called a *metric*. (To be precise, it should be called a semimetric, since in the definition of metric it is usually assumed that distinct points have positive distance; but we allow that two rows of the matrix be represented by the same point, and so it is more convenient to allow $d_{ij} = 0$. Also note that (2.2), (2.4) and (2.5) imply (2.3).) All metrics for a fixed n form a convex cone M_n, which we call the *metric cone*. Since M_n is defined by a finite number of linear inequalities, it is a polyhedral cone.

Now consider the fact that D is a metric that is L_1-embeddable, i.e., it can be represented by a measurable space $(\Omega, \mathcal{A}, \mu)$ with finite measure and by integrable functions $f_1, \ldots, f_n : \Omega \to \mathbb{R}$ so that

$$d_{ij} = \int_\Omega |f_i - f_j| \, d\mu.$$

It is not difficult to see that these functions can be chosen 0-1 valued and $(\Omega, \mathcal{A}, \mu)$ can be chosen so that it consists of a finite number of atoms. So if D is L_1-embeddable then there always exists a representation in terms of a finite set Ω, a weighting $\mu : \Omega \to \mathbb{R}_+$, and subsets $A_i \subseteq \Omega$ such that

$$d_{ij} = \mu(A_i \triangle A_j).$$

It is easy to verify from this interpretation that for each fixed n, L_1-embeddable metrics form a convex cone: if D is represented by $(\Omega, \mu, A_1, \ldots, A_n)$ and D' is represented by $(\Omega', \mu', A'_1, \ldots, A'_n)$ (where we may assume that $\Omega \cap \Omega' = \emptyset$), then λD is represented by $(\Omega, \lambda\mu, A_1, \ldots, A_n)$ and $D + D'$ is represented by $(\Omega \cup \Omega', \ \mu \cup \mu', \ A_1 \cup A'_1, \ldots, A_n \cup A'_n)$. This cone is called the *Hamming cone* and is denoted by H_n. (The fact that L_1-embeddable metrics form a convex cone is not entirely obvious: this is not true e.g. for L_2-embeddable metrics.)

It should also be noted that every L_2-embeddable matrix is also L_1-embeddable. In fact, assume that D can be represented by the euclidean distances in a set $\{v_1, \ldots, v_n\} \subset \mathbb{R}^N$. Let Ω be the set of halfspaces in $\mathbb{R}^N$ separating at least one pair $\{v_i, v_j\}$. There exists a translation and rotation invariant measure μ on the halfspaces in $\mathbb{R}^N$, and it is easy to see that $\mu(\Omega)$ is finite. Let A_i denote the set of halfspaces in Ω containing v_i; then $\mu(A_i \triangle A_j)$ is proportional to the euclidean distance of v_i and v_j.

Returning to L_1-embeddability, we want to describe the Hamming cone H_n. The construction showing that it is a cone can be used "backwards" to show that *every Hamming metric is the sum of Hamming metrics on single atoms.* A Hamming metric on a single atom $\Omega = \{a\}$ is quite simple; normalizing by $\mu(a) = 1$, every row must be represented by either $\emptyset$ or $\{a\}$, and so for an appropriate $S \subseteq \{1, \ldots, n\}$, the matrix D looks like

$$d_{ij} = \begin{cases} 1, & \text{if } i \in S \text{ and } j \notin S \text{ or vice versa,} \\ 0, & \text{otherwise.} \end{cases}$$

Such a matrix will be called a cut matrix (or cut metric). Our argument shows that every Hamming metric is a non-negative linear combination of cut metrics. Hence

2.6 Proposition. *The Hamming cone is polyhedral and its extreme rays are spanned by cut metrics.* ∎

In the spirit of polyhedral combinatorics, a next task would be to describe the facets of H_n. Unfortunately, no complete description is available; membership in H_n is NP-hard to decide (Karzanov 1985). The Hamming cone can be viewed as the *cut cone* of the complete graph, and general results on the cut polyhedron yield many facets. Nevertheless, much of the development of the two topics has been independent; see Barahona and Mahjoub (1986), Deza and Laurent (1992a,b,c).

An important class of inequalities with geometric flavour is that D is of negative type, i.e., for every $x \in \mathbb{R}^n$ we have

$$\sum_i x_i = 0 \quad \Longrightarrow \quad \sum_i \sum_j d_{ij} x_i x_j \leq 0. \tag{2.7}$$

(for L_2-embeddable metrics, we had the squared distances in a similar inequality). To see that (2.7) holds for every Hamming metric, it suffices to consider the extreme rays of H_n, i.e., the cut metrics; and for such a metric, we have

$$\sum_i \sum_j d_{ij} x_i x_j = 2 \sum_{i \in S} \sum_{j \notin S} x_i x_j = 2\big(\sum_{i \in S} x_i\big)\big(\sum_{j \notin S} x_j\big) = -2\big(\sum_{i \in S} x_i\big)^2 \leq 0.$$

Another way to state this inequality is the following. Let $i_1, \ldots, i_k, j_1, \ldots, j_k$ be (not necessarily distinct) indices from $\{1, \ldots, n\}$. Then

$$\sum_{1 \leq p < r \leq k} d(i_p, i_r) + \sum_{1 \leq p < r \leq k} d(j_p, j_r) \leq \sum_{\substack{1 \leq p \leq k \\ 1 \leq r \leq k}} d(i_p, j_r) \tag{2.8}$$

(distances between the same kind of points sum up to not more than distances between different kinds of points). To derive (2.8) from (2.7), let x_i be the number of times i occurs among the indices j_r, less the number of times i occurs among the indices i_p; then $\sum_i x_i = 0$ and (2.7) implies (2.8). Conversely, (2.8) implies (2.7) directly for integral vectors x, from which the rational case follows by homogeneity and the general case follows by continuity.

There is a way to sharpen this inequality, which leads to perhaps the most important class of inequalities valid for H_n (Deza 1960, Kelly 1970). Let $i_1, \ldots, i_k, j_1, \ldots, j_{k+1}$ be (not necessarily distinct) indices from $\{1, \ldots, n\}$. Then

$$\sum_{1 \leq p < r \leq k} d(i_p, i_r) + \sum_{1 \leq p < r \leq k+1} d(j_p, j_r) \leq \sum_{\substack{1 \leq p \leq k \\ 1 \leq r \leq k+1}} d(i_p, j_r) \tag{2.9}$$

is valid for every Hamming metric. The triangle inequality is just the special case $k = 1$. This is why these inequalities are called *hypermetric inequalities.*

We can give a linear algebraic formulation of these inequalities analogous to (2.7):

$$\sum_i x_i = 1,\ x_i \text{ integer} \quad \Longrightarrow \quad \sum_i \sum_j d_{ij} x_i x_j \le 0 \tag{2.10}$$

(the condition that the x_i are integral cannot be dropped; else, the inequality would hold for every vector x, and so D would be negative semidefinite, which is impossible for $D \neq 0$ as trace$(D) = 0$). From this formulation, the inequality can be proved for cut metrics (and hence for all Hamming metrics) similarly to the proof of (2.8) above.

The hypermetric inequalities hold, in particular, for the euclidean metric (this is not quite obvious to see directly), and have interesting applications in discrete geometry (see e.g. Kelly 1975).

The convex cone defined by the inequalities (2.7) (or (2.8)) is called the *negative type cone*, while that defined by the inequalities (2.9) (or (2.10)) is called the *hypermetric cone*. The negative type cone is non-polyhedral for $n \ge 3$; but Deza, Grishukhin and Laurent (1991) prove the following:

2.11 Theorem. *The hypermetric cone is polyhedral for every $n \ge 2$.*

This fact is non-trivial, since seemingly there are infinitely many defining inequalities. To analyze the structure of hypermetric inequalities, let us substitute $x_n = 1 - \sum_{i=1}^{n-1} x_i$ in (2.10), then we get that for every $x \in \mathbb{Z}^{n-1}$,

$$\sum_{i,j \le n-1} (d_{in} + d_{jn} - d_{ij}) x_i x_j - 2 \sum_{i \le n-1} d_{in} x_i \ge 0. \tag{2.12}$$

It follows easily that the matrix $A = (d_{in} + d_{jn} - d_{ij})_{i=1}^{n-1}{}_{j=1}^{n-1}$ is positive semidefinite (in fact, this is equivalent to (2.7)). Let E denote the solution set of

$$\sum_{i,j \le n-1} (d_{in} + d_{jn} - d_{ij}) x_i x_j - 2 \sum_{i \le n-1} d_{in} x_i \le 0.$$

Property (2.12) implies that E contains no lattice points in its interior. On the other hand, it follows by substitution that the zero vector and the unit vectors are on the boundary of E. If A is positive definite, then E is an ellipsoid; in general, it is a direct product of a linear subspace with an ellipsoid, which we call a *generalized ellipsoid*. So every hypermetric corresponds to a lattice-point-free generalized ellipsoid in $\mathbb{R}^{n-1}$, having 0 and the unit vectors on its boundary. Conversely, every such generalized ellipsoid yields a hypermetric (uniquely up to a scalar factor). Such a generalized ellipsoid corresponds to an extreme ray of the hypermetric cone if and only if the system of hypermetric equalities satisfied by d admit d as a unique solution (up to a scaling).

Deza, Grishukhin and Laurent use this description of the extreme rays, together with a theorem of Voronoi on the finiteness of affine types of Delaunay polytopes of a lattice of a given dimension, to show that the number of extreme rays of the hypermetric cones is finite, i.e., this cone is polyhedral.

An interesting connection between the metric cone and multicommodity flows was pointed out by Avis and Deza (1991). We formulate the multicommodity flow problem as follows (cf. Chapter 2). Consider the complete graph K_n on nodes $\{1, \ldots, n\}$. For each unordered pair i, j of nodes, we are given a capacity $c_{ij} \geq 0$, and a demand $d_{ij} \geq 0$. So (c_{ij}) and (d_{ij}) are symmetric matrices, and we assume that $c_{ii} = d_{ii} = 0$ for each node i. We want to find a flow f_{ij} from i to j of value d_{ij} for every $1 \leq i < j \leq n$ such that

$$\sum_{i,j} |f_{ij}(uv)| \leq c_{uv}$$

for every pair u, v. We say that the pair (C, D) is *feasible* if such a system of flows exists. (If we want to work on a graph different from the complete graph, we can set $c_{uv} = 0$ for the non-adjacent pairs. Similarly, we set $d_{ij} = 0$ if we do not want a flow from i to j.) Now this is a system of linear inequalities and a characterization of feasibility can be obtained from the Farkas lemma. However, this condition is not very transparent; Iri (1970) and Onaga and Kakusho (1971) managed to replace it by the following elegant criterion (Chapter 2, Theorem 8.1): *a capacity–demand pair (C, D) is feasible if and only if $C - D$ is contained in the polar of the metric cone.*

A special necessary condition for feasibility, also formulated in Chapter 2, is the *cut condition:* for every partition $\{S, V \setminus S\}$, we must have

$$\sum_{i \in S, j \in V \setminus S} d_{ij} \leq \sum_{i \in S, j \in V \setminus S} c_{ij}.$$

It is easy to see that this is equivalent to saying that $C - D$ gives a non-negative inner product with every cut metric. Since cut metrics are just the extreme rays of the Hamming cone H_n, this means that $C - D$ is contained in the polar of the Hamming cone. (Note that $H_n \subseteq M_n$ and hence $H_n^* \supseteq M_n^*$.)

Various results on multicommodity flows discussed in Chapter 2 are worth re-phrasing in terms of these cones (see in particular Theorem 8.9). The Max-Flow-Min-Cut Theorem says that if a symmetric matrix A has 0's in its diagonal and has only one pair of negative entries, then $A \in H_n^*$ implies $A \in M_n^*$. Hu's theorem on 2-commodity flows implies that this holds also when A has two pairs of negative entries. Papernov's work can be viewed as a characterization of all patterns of negative entries of a matrix in $H_n^* \setminus M_n^*$. Other results on multicommodity flows exclude certain supports for a matrix in $H_n^* \setminus M_n^*$; e.g. Seymour's Theorem 8.9(g) in Chapter 2 implies that such a support cannot be the adjacency matrix of a planar graph.

3. Matchings and the Haar measure

A fundamental notion in measure theory is the Haar measure on locally compact topological groups. We shall show that matching theory can be applied to give a simple and constructive proof of the existence of the Haar measure in the compact case (Harper and Rota 1971). We in fact prove the existence of invariant integration; this result, proved by von Neumann, is equivalent to the existence of the Haar measure. We refer to Halmos (1950) for measure-theoretic background. For further applications of matching theory to measure theory, see also Lovász and Plummer (1986).

Let G be a compact topological group (i.e., a group G endowed with a compact topology such that the group operations of multiplication and inverse are continuous). Let $C(G)$ denote the space of real valued continuous functions defined on G. An *invariant integration* is a functional defined on $C(G)$, having the following properties:

(1) $L(\alpha f + \beta g) = \alpha L(f) + \beta L(g)$ (linearity);

(2) if $f \geq 0$ then $L(f) \geq 0$ (positivity);

(3) if $\mathbf{1}$ denotes the identically 1 function then $L(\mathbf{1}) = 1$ (normalization);

(4) if $s, t \in G$ and $f \in C(G)$, and g is defined by $g(x) = f(sxt)$ then $L(g) = L(f)$ (double translation invariance).

3.1 Theorem. *Every compact topological group admits an invariant integration.*

For the proof, we need some notation. If A is a finite set and $f:\ A \to \mathbb{R}$ then we set

$$\overline{f}(A) = \frac{1}{|A|} \sum_{a \in A} f(a).$$

If $\mathcal{H} = (V, E)$ is a (finite or infinite) hypergraph and $f:\ V \to \mathbb{R}$ then we set

$$\delta(f, \mathcal{H}) = \sup\{|f(x) - f(y)| :\ x, y \in U \text{ for some } U \in \mathcal{H}\}.$$

The combinatorial lemma we use is the following.

3.2 Lemma. *Let $\mathcal{H}$ be a hypergraph and let A, B be two minimum cardinality blocking sets of $\mathcal{H}$. Assume that A (and B) are finite. Then*

$$|\overline{f}(A) - \overline{f}(B)| \leq \delta(f, \mathcal{H}).$$

Proof. Consider the bipartite graph whose color classes are A and B, where $a \in A$ is connected to $b \in B$ iff there exists an edge $U \in \mathcal{H}$ containing both a and b. We claim that this bipartite graph has a perfect matching. We verify the conditions in the Marriage Theorem (see Chapter 3, Corollary 2.5). It is clear that $|A| = |B|$. Let $T \subseteq A$ and let $N(T)$ denote the set of neighbors of T in B.

We show that the set $A' = A \cup N(T) \setminus T$ is also a blocking set for $\mathcal{H}$. In fact, every edge U of $\mathcal{H}$ meets A as well as B, since A and B are blocking. Let $a \in U \cap A$ and $b \in U \cap B$. If $a \notin T$ then we are done. If $a \in T$ then $b \in N(T)$ and so again A' meets U.

So A' is a blocking set and hence $|A'| \geq |A|$, which implies that $|N(T)| \geq |T|$. Thus the Marriage Theorem applies and G has a perfect matching, say $\{a_1b_1, \ldots, a_nb_n\}$. Then

$$\begin{aligned}|\overline{f}(A) - \overline{f}(B)| = \left|\frac{1}{n}\sum_{i=1}^{n}\big(f(a_i) - f(b_i)\big)\right| &\leq \frac{1}{n}\sum_{i=1}^{n}|f(a_i) - f(b_i)| \\ &\leq \frac{1}{n} n\delta(f, \mathcal{H}) = \delta(f, \mathcal{H}).\end{aligned}$$ ∎

Proof of Theorem 3.1. Let U be a non-empty open subset of G. We denote by $\mathcal{H}_U$ the hypergraph with underlying set G, whose edges are the *translates* of U, i.e., the sets $sUt = \{sut : u \in U\}$ $(s, t \in G)$. A blocking set of $\mathcal{H}_U$ is called a *U-net.* It follows from the compactness of the group G that there exists a finite U-net. Let $f \in C(G)$; we want to define the value $L(f)$.

Claim. *Let U and V be non-empty open subsets of G. Let A be a minimum cardinality U-net and B, a minimum cardinality V-net. Then*

$$|\overline{f}(A) - \overline{f}(B)| \le \delta(f, \mathcal{H}_U) + \delta(f, \mathcal{H}_V).$$

To prove this claim, observe that Ab is also a minimum U-net for any $b \in B$, and hence by Lemma 3.2,

$$|\overline{f}(A) - \overline{f}(Ab)| \le \delta(f, \mathcal{H}_U).$$

Hence

$$|\overline{f}(A) - \overline{f}(AB)| = \left|\overline{f}(A) - \frac{1}{|B|}\sum_{b\in B}\overline{f}(Ab)\right| \le \frac{1}{|B|}\sum_{b\in B}|\overline{f}(A) - \overline{f}(Ab)| \le \delta(f, \mathcal{H}_U).$$

Similarly,

$$|\overline{f}(B) - \overline{f}(AB)| \le \delta(f, \mathcal{H}_V),$$

and hence $|\overline{f}(A) - \overline{f}(B)| \le \delta(f, \mathcal{H}_U) + \delta(f, \mathcal{H}_V)$.

Now we construct the integration. Let $f \in C(G)$. Let U_n be a sequence of open sets such that $\delta(f, \mathcal{H}_{U_n}) \longrightarrow 0$ (such a sequence exists by the continuity of f and the compactness of G). Choose, for each n, a U_n-net A_n with minimum cardinality. Then by the Claim, the sequence $\{\overline{f}(A_n)\}$ satisfies the Cauchy convergence criterion and hence it has a limit $L(f)$. The Claim also implies that this limit is independent of the choice of the sets U_n and A_n.

We verify conditions (1)–(4). For (1), note that we can choose a sequence V_n such that simultaneously

$$\delta(\alpha f + \beta g, \mathcal{H}_{V_n}) \to 0, \qquad \delta(f, \mathcal{H}_{V_n}) \to 0, \qquad \delta(g, \mathcal{H}_{V_n}) \to 0.$$

Let A_n be a minimum V_n-net. Then

$$\begin{aligned} L(\alpha f + \beta g) &= \lim_{n\to\infty} \big(\alpha\overline{f}(A_n) + \beta\overline{g}(A_n)\big) \\ &= \alpha \lim_{n\to\infty} \overline{f}(A_n) + \beta \lim_{n\to\infty} \overline{g}(A_n) = \alpha L(f) + \beta L(g). \end{aligned}$$

Conditions (2) and (3) are trivial; also, (4) is clear since the whole construction is invariant under translations. ∎

4. The minimal degree of primitive permutation groups

The *minimal degree* of a permutation group G is the smallest number of points moved by any non-identity element of G. This parameter has been subject to considerable study since the 19th century (see Wielandt (1964) for references).

The minimal degree of the symmetric group is 2 and that of the alternating group is 3. In contrast, there are only finitely many primitive permutation groups with minimal degree μ for $\mu > 3$, and none for $\mu = 9, 25$ or 49. These results were proved by Jordan in 1871 and 1874 (see Jordan 1961). He showed (essentially) that if G is a primitive permutation group of degree n not containing A_n, then

$$\mu \geq (1 + o(1))\sqrt{\frac{8n}{\log n}}.$$

Much more is true for doubly transitive groups. Bochert (1889) proved that if G is a doubly transitive permutation group of degree n not containing A_n, then

$$\mu \geq \frac{n}{4} - 1.$$

The question remains, can Jordan's bound be improved for *uniprimitive* (primitive but not doubly transitive) permutation groups. Consider the line graph $L(K_{v,v})$ of the complete bipartite graph. The automorphism group of this graph is primitive of degree $n = v^2$, and has minimal degree $2v = 2\sqrt{n}$ (consider the automorphism of $L(K_{v,v})$ induced by the transposition of two non-adjacent nodes of $K_{v,v}$).

This example shows that the following result of Babai (1981) is best possible up to the constant.

4.1 Theorem. *If G is a uniprimitive group of degree n then*

$$\mu(G) \geq \frac{1}{2}\sqrt{n-1}.$$

Below we prove the somewhat weaker inequality $\mu(G) \geq \sqrt{(n-1)/6}$. A slight refinement of the proof would yield $\mu(G) \geq (1 + o(1))\sqrt{2n/3}$.

Babai proved the theorem by reducing the group-theoretical problem to a combinatorial question on coherent configurations. We shall give this reduction and then a rather simple proof of the result on coherent configurations, incorporating some ideas of Zemlyachenko (see Zemlyachenko, Kornienko and Tyshkevich 1985).

We need some notions from the theory of coherent configurations (see also Chapter 15). A *coherent configuration* $\Xi = (\Omega; R_1, \ldots, R_r)$ is a finite set Ω of vertices and a family $R_1, \ldots, R_r$ of non-empty binary relations on Ω such that

(i) $\{R_1, \ldots, R_r\}$ forms a partition of $\Omega \times \Omega$;

(ii) The diagonal $\Delta = \{(\omega, \omega) : \omega \in \Omega\}$ is the union of some of the R_i;

(iii) R_i^{-1} (the inverse of R_i) is one of the R_j.

(iv) There is collection of r^3 integers p_{ij}^k such that for every $\alpha, \beta \in R_k$, one has

$$|\{\gamma : (\alpha, \gamma) \in R_i, \ (\gamma, \beta) \in R_j\}| = p_{ij}^k$$

(independently of the particular choice of α and β).

For $(\alpha, \beta) \in R_i$ we set $i = c(\alpha, \beta)$ and call (α, β) an "edge of color i". We call r the *rank* of Ξ. The digraphs (Ω, R_i) are the *classes* of Ξ. A coherent configuration is *homogeneous* if $R_1 = \Delta$. It is *primitive* if it is homogeneous and each of the classes (Ω, R_i) $(i \geq 2)$ is connected as a digraph (here we do not have to worry which definition of connectedness to choose, since for the classes of a homogeneous coherent configuration connectivity and strong connectivity are equivalent). A primitive coherent configuration is *uniprimitive* if its rank is at least 3.

The classical examples of coherent configurations arise from permutation groups. If G is a permutation group acting on Ω, we let $R_1, \ldots, R_k$ be the orbits of the induced action on $\Omega \times \Omega$, to get a coherent configuration $\Xi(G)$ associated with the permutation group G.

Choosing the indices appropriately, $\Xi(G)$ is homogeneous iff G is transitive. Connected components of any non-diagonal class correspond to blocks of imprimitivity of G; hence it is easy to see that G is primitive [uniprimitive] iff the associated coherent configuration is primitive [uniprimitive].

The key result of Babai is the following. We say that a vertex ω *distinguishes* vertices α and β if $c(\alpha, \omega) \neq c(\beta, \omega)$.

4.2 Theorem. *Let Ξ be a uniprimitive coherent configuration. Then each pair of vertices α, β is distinguished by at least $\sqrt{(n-1)/6}$ vertices.*

To see that this result implies Theorem 4.1, assume that $\Xi = \Xi(G)$ and let $g \in G$ be a permutation moving only a set M of $\mu(G)$ elements. Let $\alpha \in M$ and $\beta = \alpha^g$. Then for $\omega \notin M$ we have $c(\alpha, \omega) = c(\beta, \omega)$, as g maps (α, ω) onto (β, ω). So α and β are distinguished by at most μ elements. So Theorem 4.2 implies that $\mu \geq \sqrt{(n-1)/6}$.

The main idea in proving Theorem 4.1 was to find the right combinatorial relaxation of the group-theoretic notion of minimum degree. As we shall see, the rest of the proof (i.e., the proof of Theorem 4.2) uses only elementary combinatorics.

To prove Theorem 4.2, we need some notation and a series of simple lemmas. For $\omega \in \Omega$, consider the number of edges of color i leaving ω. As Ξ is homogeneous, this number does not depend on ω, and we denote it by d_i. We write $i^{-1} = j$ if $R_i^{-1} = R_j$. In this case $d_i = d_j$. We denote by X_i the digraph (Ω, R_i) and by X_i', the undirected graph $(\Omega, R_i \cup R_i^{-1})$. Let $\mathrm{diam}(i)$ denote the diameter of X_i'.

For two vertices α, β, let $D(\alpha, \beta)$ denote the set of vertices distinguishing α and β. Note that the cardinality of $D(\alpha, \beta)$ depends only on the color of the pair (α, β) (by the definition of coherent configurations); we set $f(i) = |D(\alpha, \beta)|$ if $i = c(\alpha, \beta)$. Clearly $f(i) = f(i^{-1})$. We want to prove that $f(i) \geq \sqrt{(n-1)/6}$.

4.3 Lemma. *Let t denote the distance of vertices α and β in the (undirected) graph X'_i. Then $f(i) \geq |D(\alpha, \beta)|/t$.*

Proof. Let $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_t = \beta$ be a path of length t in X'_i. Clearly $D(\alpha, \beta) \subseteq \cup_{s=1}^{t} D(\alpha_{i-1}, \alpha_i)$. Using $f(i) = f(i^{-1})$ we obtain $|D(\alpha, \beta)| \leq t \cdot f(i)$. ∎

This observation leads to the following important inequality:

4.4 Lemma. *If* $\operatorname{diam}(i) \geq 3$ *then* $f(i) \geq 2d_i/3$.

Proof. Let α and β be vertices at distance 3 in X'_i. The sets of neighbors (in X'_i) of α and β are disjoint, therefore these sets are contained in $D(\alpha, \beta)$. This yields $|D(\alpha, \beta)| \geq 2d_i$. So Lemma 4.3 implies that $f(i) \geq 2d_i/3$. ∎

This lemma settles the case when X'_i has diameter at least 3 and d_i is "large". For the case when d_i is "small" we need another simple observation. Let $\Gamma_i(\alpha)$ denote the set vertices β with $c(\alpha, \beta) = i$.

4.5 Lemma. *If there is an edge with color h from $\Gamma_i(\alpha)$ to $\Gamma_j(\alpha)$ then there are at least* $\max\{d_i, d_j\}$ *such edges.*

Proof. The assumption says that for some vertices β and γ we have $c(\alpha, \beta) = i$, $c(\alpha, \gamma) = j$ and $c(\beta, \gamma) = h$. By the definition of coherent configurations, this implies that for every $\beta \in \Gamma_i(\alpha)$ there exists at least one vertex γ such that $c(\alpha, \gamma) = j$ and $c(\beta, \gamma) = h$. Hence there are at least d_i edges of color h from $\Gamma_i(\alpha)$ to $\Gamma_j(\alpha)$. Applying the argument to h^{-1}, the assertion follows. ∎

4.6 Lemma. *Any vertex distinguishes the endpoints of at least $n - 1$ edges of each color.*

Proof. Consider a vertex ω and a color h, and define a graph W on vertex set $\{1, \ldots, r\}$ by joining i to j if there is an edge of color h from $\Gamma_i(\omega)$ to $\Gamma_j(\omega)$. This graph is connected since X_h is connected. Let T be a spanning tree of W. Orient the edges of T away from 1. By Lemma 4.5, every edge ij of T represents at least d_j edges of color h distinguished by ω. Hence the total number of edges of color h distinguished by ω is at least

$$\sum_{ij \in T} d_j = \sum_{j=2}^{r} d_j = n - 1.$$ ∎

Counting the triples (α, β, ω) with $c(\alpha, \beta) = i$ and $\omega \in D(\alpha, \beta)$ in two ways, and using Lemma 4.6 we obtain

$$n d_i f(i) \geq n(n - 1),$$

which yields one of our key inequalities:

4.7 Lemma. $f(i) \geq (n - 1)/d_i$. ∎

Combining with Lemma 4.4, we obtain:

4.8 Lemma. *If* $\operatorname{diam}(i) \geq 3$ *then* $f(i) \geq \sqrt{2(n - 1)/3}$. ∎

What remains is to find a good lower bound on $f(i)$ in the case when $\operatorname{diam}(i) = 2$.

4.9 Lemma. *There exists a pair distinguished by at least* $\sqrt{2(n-1)/3}$ *vertices.*

Proof. Suppose that $d_2 \leq d_3 \leq \ldots$. If $\mathrm{diam}(2) \geq 3$ we are done by Lemma 4.8. If $\mathrm{diam}(2) = 2$ then obviously $1 + d_2 + (d_2 - 1)d_2 \geq n$ hence $d_2 \geq \sqrt{n-1}$. Further, trivially $d_2 \leq (n-1)/2$.

Any given vertex distinguishes at least $2d_2(n-1-d_2) \geq 2(n-1)(\sqrt{n-1}-1)$ ordered pairs. Hence there must be an ordered pair distinguished by at least $2(\sqrt{n-1}-1)$ vertices, i.e., $f_{\max} \geq 2(\sqrt{n-1}-1) > \sqrt{2(n-1)/3}$. ∎

Proof of Theorem 4.2. Choose a pair α, β of vertices with $|D(\alpha,\beta)| \geq \sqrt{2(n-1)/3}$. Let $i \geq 2$. If $\mathrm{diam}(i) > 2$ then we have $f(i) \geq \sqrt{2(n-1)/3}$ by lemma 4.8. If $\mathrm{diam}(i) = 2$ then we have

$$f(i) \geq \frac{1}{2}|D(\alpha,\beta)| \geq \sqrt{\frac{n-1}{6}}$$

by Lemma 4.3. ∎

Invoking the classification theorem of finite simple groups, Liebeck (1984) obtained a classification of all primitive permutation groups with $\mu \leq n/(9\log n)$. From this, Theorem 4.1 can be read off. Still, it is good to have a short solution for a classical problem, which helps us understand why the result holds.

The situation is similar for a related classical problem. Using Theorem 4.2 and a simple probabilistic argument, Babai (1981) proved that every uniprimitive permutation group of degree n has a base of size $b \leq 4\sqrt{n}\log n$. (A base is a subset Φ of Ω such that the only group element fixing every vertex in Φ is the identity.) This immediately gives an upper bound $n^b \leq \exp(4\sqrt{n}\log^2 n)$ on the order of uniprimitive permutation groups, another remarkable result.

This bound has been supplemented (Babai 1982) by an even stronger upper bound of $\exp(\exp(1.08\sqrt{\log n}))$ on the order of doubly transitive permutation groups not containing A_n. Recently Pyber (1990) found a simple combinatorial proof of the bound $n^{c(\log n)^2}$ using Babai's ideas. Once more the classification theorem of finite simple groups gives a stronger bound of $n^{(1+o(1))\log n}$, but perhaps less insight.

5. Algebras with Straightening Law

In this section, we give a brief glimpse into applications of combinatorial techniques to some questions of algebraic geometry and commutative algebra.

Graded commutative rings (that is, quotients $A = \mathbf{k}[x_1,\ldots,x_m]/(f_1,\ldots,f_m)$, where the f_i are homogeneous polynomials) are a central object of study for commutative algebra. A main motivation for this comes from algebraic geometry, which studies *projective varieties* (that is, solution sets of systems $f_1 = 0,\ldots,f_m = 0$ of homogeneous polynomial equations). The geometry of such a variety is encoded in its *coordinate ring* $A = \mathbf{k}[x_1,\ldots,x_m]/I$, where I is the ideal of all polynomial functions that vanish on the variety, and A can be interpreted as the ring of functions on the variety (see for example Shafarevich (1977), Kunz (1985)).

For the study of projective varieties and their coordinate rings, algebraic geometry has a variety of tools available: algebraic, homological, analytic, etc. Combinatorics comes into play in the case of “classical” varieties, such as Grassmann and flag manifolds, determinantal and Schubert varieties, and many more. These varieties and their rings have additional structure: for example, the varieties are very symmetric, and they satify nice smoothness, completeness and regularity conditions. The coordinate rings can be given by generators and relations in a very explicit way, and so it is not too surprising if combinatorial techniques can be applied.

Cohen-Macaulay Rings. Let A be a graded commuatative ring, that is, the quotient of a polynomial ring modulo a homogeneous ideal,

$$A = \mathbf{k}[x_1, \dots, x_m]/I.$$

In particular A has a direct sum decomposition $A = \bigoplus_{k\geq 0} A_k$, where A_k is the finite-dimensional $\mathbf{k}$-vector space of residue classes of homogeneous polynomials of degree k in A.

In this exposition we will, as an example, consider the Cohen-Macaulay property of A, which expresses a quite subtle regularity property of the associated variety. The usual definition is in homological algebra terms: A is *Cohen-Macaulay* if and only if its *depth* is equal to its *dimension*. Here the dimension $d = \dim(A)$ is the maximal number of algebraically independent elements $\{\theta_1, \dots, \theta_d\}$ in A, and the depth is the maximal length $p = depth(A)$ of a *regular sequence:* a sequence $(\theta_1, \dots, \theta_p)$ such that θ_i is not a zero-divisor in $A/\langle\theta_1, \dots, \theta_{i-1}\rangle$ for $1 \leq i \leq p$. This in particular means that $p \leq d$: the depth never exceeds the dimension.

There are many reformulations of the Cohen-Macaulay condition, the most explicit perhaps being the following. A is Cohen-Macaulay if and only if it has a *Hironaka decomposition*: for some set $\{\theta_1, \dots, \theta_d\}$ of algebraically independent, homogeneous elements of A there exist homogeneous elements $\eta_1, \dots, \eta_t$ such that A has a direct sum decomposition

$$A = \bigoplus_{i=1}^{t} \eta_i \mathbf{k}[\theta_1, \dots, \theta_d].$$

This means that A is a free $\mathbf{k}[\theta_1, \dots, \theta_d]$-module, and the set of *separators* $\{\eta_1, \dots, \eta_t\}$ forms a module basis for A. The maximal regular sequence $(\theta_1, \dots, \theta_d)$ is called a *system of parameters* in this case. (It turns out that if A is Cohen-Macaulay, then *any* sequence $(\theta_1, \dots, \theta_d)$ with $\dim_{\mathbf{k}} A/\langle\theta_1, \dots, \theta_d\rangle < \infty$ can be used as a system of parameters of a Hironaka decomposition.)

To show that the coordinate rings of classical varieties are Cohen-Macaulay, this offers two alternative approaches. One can compute their dimensions and depths – or one can try to construct explicit Hironaka decompositions. The second approach is more far-reaching: a Hironaka decomposition of A carries a lot of extra structure, such that for example the Hilbert function of the ring can be read off. For this we denote the *Hilbert function* of A by

$$\mathrm{H}(A, k) := \dim_{\mathbf{k}} A_k,$$

and its *Poincaré series* (or *Hilbert series*) by

$$\mathrm{Poin}(A,t) := \sum_{k\geq 0} \mathrm{H}(A,k)t^k,$$

So the Poincaré series of A is the ordinary generating function (see Chapter 21) of the Hilbert function.

A basic result (that can for example be derived from the existence of a finite free resolution of A) now states that the Poincaré series is a rational function of the form

$$\mathrm{Poin}(A,t) = \frac{P_A(t)}{(1-t)^d},$$

where $P_A(t)$ is a polynomial in t with integer coefficients, $P_A(0) = 1$ and $P_A(1) \neq 0$, such that the order of the pole of $\mathrm{Poin}(A,t)$ at $t = 1$ is $d = \dim(A)$.

¿From this in turn we get the basic properties of the Hilbert function: for large k, $\mathrm{H}(A,k)$ is a polynomial in k of degree $d-1$, with rational coefficients.

Now, if A is Cohen-Macaulay with $A = \bigoplus_{i=1}^{s} \eta_i \mathbf{k}[\theta_1,\ldots,\theta_d]$, then it is easy to read off the Poincaré series

$$\mathrm{Poin}(A,t) = \frac{\sum_{i=1}^{s} t^{\deg \eta_i}}{(1-t)^d}.$$

Note that the numerator polynomial $P_A(t)$ has non-negative coefficients in this Cohen-Macaulay case – this is not true in general. We can also compute the Hilbert function

$$\mathrm{H}(A,k) = \sum_{i=1}^{s} \binom{k - \deg \eta_i + d - 1}{d-1},$$

[with the convention that the summands are zero if $k < \deg \eta_i$], which is a polynomial in k for $k \geq \max(\deg \eta_i)$.

Let us mention that more general decompositions allow us to treat quite general classes of rings in a similar way, as is described in Bacławski and Garsia (1981). Computational aspects of this framework are treated in Sturmfels and White (1991).

The Straightening Law. A common structural feature of many of the important coordinate rings of "classical varieties" (and all those listed above) is that they have the structure of an "algebra with straightening law" over a finite poset – such that the combinatorics of the poset allows to construct decompositions of the algebra A. A reasonable level of generality is given by the following definition. It describes what is called an *ordinal Hodge algebra* by De Concini, Eisenbud and Procesi (1982), and an *algebra with strongly lexicographic straightening law based on a poset* by Bacławski (1981). See, for example, De Concini and Lakshmibai (1981) for a more general set-up.

5.1 Definition. *Let A be a $\mathbf{k}$-algebra and $P = \{x_1,\ldots,x_m\}$ a finite poset. Then A is an algebra with straightening law over P if A has a presentation of the form $A = \mathbf{k}[x_1,\ldots,x_m]/I$ (identifying the elements of P with generators of A) such that*

(1) *the products of variables* $x_{i_1}x_{i_2}\dots x_{i_k}$ *that correspond to multichains* $x_{i_1} \le \dots \le x_{i_k}$ *of* P*, called* standard monomials*, form a* $\mathbf{k}$*-basis of* A*, and*

(2) *the* non-standard monomials *can be* straightened*: if for two incomparable elements* x_i *and* x_j *of* P *the monomial* $x_i x_j$ *is written as a linear combination of standard monomials, then every standard monomial in the expansion contains a variable that is smaller than* x_i *and a variable that is smaller than* x_j*.*

For every poset $P = \{x_1, \dots, x_m\}$ we get a canonical algebra with straighening law, called the *Stanley-Reisner ring of* P, as

$$\mathbf{k}[P] := \mathbf{k}[x_1, \dots, x_m]/I_P,$$

where I_P is the ideal generated by the non-standard monomials $x_i x_j$, corresponding to incomparable pairs in P. In this ring the non-standard monomials are all zero, so that the straightening law is trivial.

If A is an algebra with straightening law over P, then A and $\mathbf{k}[P]$ are isomorphic as $\mathbf{k}$-vector spaces. However, $\mathbf{k}[P]$ is endowed with a rather trivial multiplication: the product of two standard monomials is either again standard or it is zero (depending on whether the corresponding union of two multichains is again a multichain or not).

Thus the whole algebra structure of $\mathbf{k}[P]$ is determined by the combinatorial data of P. This is the case which allows a complete combinatorial analysis. The main result now reduces the general case of an algebra with straightening law to the corresponding Stanley-Reisner ring.

5.2 Theorem. [Bacławski and Garsia (1981); De Concini, Eisenbud and Procesi (1982)] *Let* A *be an algebra with straightening law over* P*, and* $\mathbf{k}[P]$ *the corresponding Stanley-Reisner ring. Then every Hironaka decomposition* $A = \bigoplus_{i=1}^{t} \eta_i \mathbf{k}[\theta_1, \dots, \theta_d]$ *of* $\mathbf{k}[P]$ *induces a Hironaka decomposition of* A *via the canonical vector space isomorphism* $A \cong \mathbf{k}[P]$*. In particular, if the Stanley-Reisner ring* $\mathbf{k}[P]$ *is Cohen-Macaulay, then* A *is also Cohen-Macaulay.*

Thus in order to prove that an algebra A with straightening law over a poset P is Cohen-Macaulay, it suffices to establish that the "combinatorial" algebra $\mathbf{k}[P]$ is Cohen-Macaulay. If parameters θ_i and separators η_j for $\mathbf{k}[P]$ have been constructed, then *the same* parameters and separators also yield a Hironaka decomposition of A.

The work by De Concini, Eisenbud and Procesi contains a careful algebraic analysis of the transition from A to $\mathbf{k}[P]$. It shows in particular that in fact both algebras have the same dimension, whereas only $depth(A) \ge depth(\mathbf{k}[P])$ holds in general.

Cohen-Macaulay Posets. At this stage of the argument, combinatorial methods take over to decide whether $\mathbf{k}[P]$ is Cohen-Macaulay, and possibly to construct decompositions.

5.3 Definition. *P is a Cohen-Macaulay poset* (*with respect to* $\mathbf{k}$) *if* $\mathbf{k}[P]$ *is a Cohen-Macaulay algebra.*

Cohen-Macaulay posets were introduced independently by Bacławski and Stanley, around 1975. Subsequent intensive research has produced a wealth of powerful results, criteria and techniques. For surveys, we refer to Björner, Garsia and Stanley (1982) and to the “Topological Methods” Chapter 34, where Cohen-Macaulay posets are treated in some detail (emphasizing the topological approach). Historical details and all the facts needed in the following are also discussed there. We will here review three aspects.

First, there are very strong conditions on the combinatorics of a poset to allow for the Cohen-Macaulay property. In fact, P has to be *ranked* (of *rank* $r(P) = r = \dim \mathbf{k}[P]$): this means that every maximal chain $x_1 < x_2 < \ldots < x_r$ in P has the same length $r-1$. Given such a maximal chain, we will write $r(x_i) = i$ for $1 \le i \le r$. This defines the *rank* $r(x)$ uniquely for every $x \in P$. A *rank selection* of P is a subposet $P_S := \{x \in P : r(x) \in S\}$ for some $S \subseteq [r]$. Also, denote by $\hat{P}$ the poset obtained by adding a new maximal element $\hat{1}$ and a new minimal element $\hat{0}$ to P.

5.4 Proposition. *If P is a Cohen-Macaulay poset, then so is every rank selection of every interval of $\hat{P}$.*

Now a strong numerical test has to be satisfied by P (and all its rank selections of intervals). For this, say that the *Möbius function* (see Chapter 21) *alternates on* P if for any $x, y \in \hat{P}$ one gets $\mu_{\hat{P}}(x,y) \cdot (-1)^{r(y)-r(x)} \ge 0$.

5.5 Proposition. *If P is Cohen-Macaulay, then the Möbius function alternates on P.*

Secondly, there is a complete characterization of Cohen-Macaulay posets in terms of the topology of the simplicial complex $\Delta(P)$ of chains in P, given in (10.8) of the “Topological Methods” Chapter 34. In particular, Cohen-Macaulayness is a topological invariant of $|\Delta(P)|$.

And finally, the techniques of *shellability* and *lexicographical shellability* allow to explicitly prove Cohen-Macaulayness and to construct Hironaka decompositions for all major classes of Cohen-Macaulay posets. We will use the following formulation of shellability.

5.6 Definition. *A poset P is shellable if it is ranked and its set $\mathcal{M}$ of maximal chains admits a linear ordering $\mathcal{M} = (C_1, C_2, \ldots, C_t)$ such that every chain C_i contains a unique minimal subset F_i that is not contained in any previous chain C_j $(j < i)$.*

The definition immediately implies that for the first chain C_1 one gets $F_1 = \emptyset$, whereas every chain C_i with $i > 1$ satisfies $F_i \neq \emptyset$ and contains at most one “new” vertex. It is not quite trivial to see that the Möbius function alternates on $\hat{P}$. However, the following result implies this.

5.7 Theorem. [Hochster (1972); Stanley (1975); Garsia (1980); Kind and Kleinschmidt (1979)] *If P is shellable, then it is Cohen-Macaulay with respect to every field* $\mathbf{k}$. *In this case we can derive parameters $\theta_i := \sum_{r(x)=i} x$ for $1 \le i \le r$ and separators $\eta_j := \prod_{x \in F_j} x$ for $1 \le j \le t$ from a shelling of P as above.*

This yields, for any shellable poset P, an explicit Hironaka decomposition of $\mathbf{k}[P]$ and thus – with Theorem 5.2 – of any algebra with straightening law over P.

For shellability techniques we again refer to Chapter 34 and the references given there. It turns out that very general classes of posets can be shown to be shellable, see (11.10) in Chapter 34. A very powerful result that covers the posets arising from many classical varieties was achieved by Björner and Wachs.

5.8 Theorem. [Björner and Wachs (1982)] *The Bruhat order of any finite quotient of a Coxeter group by a parabolic subgroup is (lexicographically) shellable.*

Example: Grassmann Varieties. We will illustrate this approach by the most "classical" case of the coordinate rings of Grassmann varieties.

For this let $\mathbf{k}$ be a field of characteristic zero, and consider the p-th exterior product of $\mathbf{k}^n$, denoted $\Lambda_p\mathbf{k}^n$. It is a $\mathbf{k}$-vector space of dimension $\binom{n}{p}$, with an explicit basis given by $\{\mathbf{e}_{i_1} \wedge \ldots \wedge \mathbf{e}_{i_p} : 1 \le i_1 < \ldots < i_p \le n\}$. The corresponding coordinate functions for $\Lambda_p\mathbf{k}^n$ are denoted by $[i_1 \ldots i_p]$. Thus a general (antisymmetric) tensor in $\Lambda_p\mathbf{k}^n$ has the form $\omega = \sum_{1\le i_1<\ldots<i_p\le n} [i_1 \ldots i_p]\ \mathbf{e}_{i_1} \wedge \ldots \wedge \mathbf{e}_{i_p}$.

An *extensor* is a non-zero, decomposable tensor in $\Lambda_p\mathbf{k}^n$, that is, a tensor of the form $\omega = \mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_p$ for p linearly independent vectors $\mathbf{v}_i \in \mathbf{k}^n$. Two p-tuples $(\mathbf{v}_1, \ldots, \mathbf{v}_p)$ and $(\mathbf{v}'_1, \ldots, \mathbf{v}'_p)$ determine up to a scalar the same extensor (that is, $\mathbf{v}_1\wedge\ldots\wedge\mathbf{v}_p = c\cdot\mathbf{v}'_1\wedge\ldots\wedge\mathbf{v}'_p$ for some $c \ne 0$) if and only if they span the same p-dimensional subspace of $\mathbf{k}^n$.

In coordinates, for $\mathbf{v}_i = \sum_{j=1}^n v_{ij}\mathbf{e}_j$, one gets

$$\mathbf{v}_1\wedge\ldots\wedge\mathbf{v}_p = \sum_{1\le i_1<\ldots<i_p\le n} [i_1 \ldots i_p]\mathbf{e}_{i_1}\wedge\ldots\wedge\mathbf{e}_{i_p}, \text{ where } [i_1 \ldots i_p] = \begin{vmatrix} v_{1i_1} & v_{1i_2} & \cdots & v_{1i_p} \\ v_{2i_1} & v_{2i_2} & \cdots & v_{2i_p} \\ \vdots & \vdots & \ddots & \vdots \\ v_{pi_1} & v_{pi_2} & \cdots & v_{pi_p} \end{vmatrix}.$$

The vector of $\binom{n}{p}$ coordinates $([i_1 \ldots i_p] : 1 \le i_1 < \ldots < i_p \le n)$ is called a vector of *Plücker coordinates* for $V := \mathrm{span}(\mathbf{v}_1, \ldots, \mathbf{v}_p)$.

Passing to the projective space of $\Lambda_p\mathbf{k}^n$, we find that the set

$$G_{p,n} := \big\{[\mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_p] \in P(\Lambda_p\mathbf{k}^n)\big\}$$

is in natural bijection to the set of p-subspaces of $\mathbf{k}^n$. As the image of a homogeneous polynomial map (which sends the matrix (v_{ij}) to the vector $([i_1 \ldots i_p])$ of all its maximal minors) this $G_{p,n}$ is an irreducible projective variety, called the *Grassmann variety* of p-subspaces in $\mathbf{k}^n$. This variety turns out to have dimension $p(n-p)$, in an ambient space of dimension $\binom{n}{p} - 1$. Note that $G_{1,n} = P(\mathbf{k}^n)$ is projective space.

The coordinate ring of the projective variety $G_{p,n}$ is

$$A(G_{p,n}) = \mathbf{k}\big[[i_1 \ldots i_p] : 1 \le i_1 < \ldots < i_p \le n\big]/I_{p,n},$$

where $I_{p,n}$ is the ideal of relations between the $(p \times p)$-minors of a generic $(p \times n)$-matrix, that is, between the variables $[i_1 \ldots i_p]$ if they are given by $[i_1 \ldots i_p] := \begin{vmatrix} v_{1i_1} & \cdots & v_{1i_p} \\ \vdots & \ddots & \vdots \\ v_{pi_1} & \cdots & v_{pi_p} \end{vmatrix}$.

Monomials of degree t in $A(G_{p,n})$ are customarily denoted by $(t\times p)$-arrays whose rows denote the names of the variables. So $[i_1 \ldots i_p] \cdot [j_1 \ldots j_p]$ will be denoted as $\begin{bmatrix} i_1 \cdots i_p \\ j_1 \cdots j_p \end{bmatrix}$, etc.

The basic theorem now is that the ideal $I_{p,n}$ is generated by the *straightening syzygies*:

$$\begin{bmatrix} i_1 \dots i_p \\ j_1 \dots j_p \end{bmatrix} = -\sum_{\sigma} \operatorname{sign}(\sigma) \begin{bmatrix} i_1 \dots i_{l-1}\sigma(i_l) \ \dots \sigma(i_p) \\ \sigma(j_1) \dots \ \sigma(j_l) j_{l+1} \dots j_p \end{bmatrix}, \qquad (*)$$

where l is an arbitrary fixed position ($1 \le l \le p$), and the sum is over all shuffles σ of $(j_1 \dots j_l | i_l \dots i_p)$ except for the identity, that is, over all permutations $\sigma \neq \mathrm{id}$ of the (multi)set $\{j_1, \dots, j_l, i_l, \dots, i_p\}$ that satisfy $\sigma(j_1) < \dots < \sigma(j_l)$ and $\sigma(i_l) < \dots < \sigma(i_p)$. Here we define $[i_{\sigma(1)} \dots i_{\sigma(p)}] := \operatorname{sign}(\sigma)[i_1 \dots i_p]$ for p-tuples that are not increasing, and $[i_1 \dots i_p] = 0$ whenever two entries i_l are equal.

[In fact, the ideals $I_{p,n}$ are already generated by the *Grassmann-Plücker relations* that are obtained from $(*)$ in the special case $l = 1$. However, these are not sufficient for straightening – see Sturmfels and White (1989).]

We want to conclude that $A(G_{p,n})$ is an algebra with straightening law. For this we define a partial order on the set of variables, by putting $[i_1 \dots i_p] \le [j_1 \dots j_p]$ whenever $i_1 \le j_1, \dots, i_p \le j_p$. This makes

$$\Lambda_{p,n} := \big(\{[i_1 \dots i_p] : 1 \le i_1 < \dots < i_p \le n\}, \le\big)$$

into a partial order – in fact, $\Lambda_{p,n}$ turns out to be a distributive lattice. In particular, $\Lambda_{p,n}$ is ranked: its rank function is given by $r([i_1 \dots i_p]) = 1 + (i_1 - 1) + \dots + (i_p - p)$, and $\Lambda_{p,n}$ has length $r([n-p+1, \dots, n]) = 1 + p(n-p)$.

Furthermore, $\Lambda_{p,n}$ is shellable: shellings for distributive lattices are easily obtained by a lexicographic technique; also – and this is the argument that generalizes for other classical varieties – $\Lambda_{p,n}$ is the quotient of (the Bruhat order of) the Coxeter group $\mathcal{S}_n$ by its maximal parabolic subgroup $\mathcal{S}_p \times \mathcal{S}_{n-p}$ and hence shellable as a special case of the Björner-Wachs Theorem 5.8.

Now reconsider the tableau corresponding to a monomial in $A(G_{p,n})$. The rows of such tableaux are variable names and thus strictly increasing, and a tableau is *standard* (that is, corresponds to a standard monomial) exactly if the columns are all non-decreasing (if read from top to bottom).

With the facts we have collected now, it is not hard to verify that $A(G_{p,n})$ is an algebra with straightening law over $\Lambda_{p,n}$: in fact the Grassmann-Plücker relations $(*)$, iterated, show that the standard monomials span $A(G_{p,n})$, and they also provide the straightening law for $A(G_{p,n})$: for this consider any monomial of degree 2 that is not standard, that is, a tableau $\begin{bmatrix} i_1 \dots i_p \\ j_1 \dots j_p \end{bmatrix}$ for which $i_l > j_l$ for some l. In this situation one has $j_1 < \dots < j_l < i_l < \dots < i_p$, and the formula $(*)$ expresses the tableau as a linear combination of tableaux whose top rows are all smaller than $[i_1 \dots i_p]$. Iterating this procedure, we get an expression of $\begin{bmatrix} i_1 \dots i_p \\ j_1 \dots j_p \end{bmatrix}$ as a linear combination of standard tableaux whose top rows are smaller than $[i_1 \dots i_p]$. (This shows that the standard monomials span $A(G_{p,n})$.) But we could have applied the same procedure to $\begin{bmatrix} j_1 \dots j_p \\ i_1 \dots i_p \end{bmatrix}$ as well, to get the *same* expression again (because the standard monomials form a basis!). Thus the top rows of all the standard tableaux in the expansion of $\begin{bmatrix} i_1 \dots i_p \\ j_1 \dots j_p \end{bmatrix}$ are also smaller than $[j_1 \dots j_p]$, which shows property (2) of an algebra with straightening law.

Thus $G_{p,n}$ is a Cohen-Macaulay variety, much of whose structure is (in a subtle way) controlled by the poset $\Lambda_{p,n}$.

For an explicit example, consider the Grassmann variety $G_{3,5}$. Its coordinate ring is

$$A(G_{3,5}) = \mathbf{k}\big[[123],[124],[125],[134],[135],[145],[234],[235],[245],[345]\big]/I_{3,5},$$

where the ideal $I_{3,5}$ is generated by Grassmann-Plücker relations like

$$\begin{bmatrix} 145 \\ 234 \end{bmatrix} - \begin{bmatrix} 134 \\ 245 \end{bmatrix} + \begin{bmatrix} 124 \\ 345 \end{bmatrix} = 0.$$

Now $A(G_{3,5})$ is an algebra with straightening law over the poset $\Lambda_{3,5}$:

$$\begin{array}{ccccc}
 & [345] & & & \\
 & | & & & \\
 & [245] & & & \\
[145] & & [235] & & \\
 & [135] & & [234] & \\
[125] & & [134] & & \\
 & [124] & & & \\
 & | & & & \\
 & [123] & & &
\end{array}$$

It is easy to get a (lexicographic) shelling: take

$$\begin{aligned}
C_1 &= ([123] < [124] < [125] < [135] < [145] < [245] < [345]) \\
C_2 &= ([123] < [124] < [125] < [135] < [235] < [245] < [345]) \\
C_3 &= ([123] < [124] < [134] < [135] < [145] < [245] < [345]) \\
C_4 &= ([123] < [124] < [134] < [135] < [235] < [245] < [345]) \\
C_5 &= ([123] < [124] < [134] < [234] < [235] < [245] < [345])
\end{aligned}$$

This yields parameters $\eta_1 = 1$, $\eta_2 = [235]$, $\eta_3 = [134]$, $\eta_4 = [134][235]$, $\eta_5 = [234]$, and separators $\theta_1 = [123]$, $\theta_2 = [124]$, $\theta_3 = [125] + [134]$, $\theta_4 = [135] + [234]$, $\theta_5 = [145] + [235]$, $\theta_6 = [245]$ and $\theta_7 = [345]$, which describes a Hironaka decomposition of the Cohen-Macaulay algebra $A(G_{3,5})$, with $d = 7$ and $t = 5$:

$$\begin{aligned} A(G_{3,5}) = \quad & \mathbf{k}\big[[123],[124],[125]+[134],[135]+[234],[145]+[235],[245],[345]\big] \\ & \oplus[235]\mathbf{k}\big[[123],[124],[125]+[134],[135]+[234],[145]+[235],[245],[345]\big] \\ & \oplus[134]\mathbf{k}\big[[123],[124],[125]+[134],[135]+[234],[145]+[235],[245],[345]\big] \\ & \oplus[134][235]\mathbf{k}\big[[123],[124],[125]+[134],[135]+[234],[145]+[235],[245],[345]\big] \\ & \oplus[234]\mathbf{k}\big[[123],[124],[125]+[134],[135]+[234],[145]+[235],[245],[345]\big] \end{aligned}$$

From this we can read off the Poincaré series as

$$\operatorname{Poin}(A(G_{3,5}),t) = \frac{1+3t+t^2}{(1-t)^7},$$

and the Hilbert function as

$$\mathrm{H}(A(G_{3,5}),k) = \binom{k+6}{6} + 3\binom{k+5}{6} + \binom{k+4}{6}.$$

6. Complex Hyperplane Arrangements

Combinatorial properties of arrangements of hyperplanes in real linear space have been studied in geometry for quite a while. Several properties of such arrangements are described in Chapter 17. A more recent development is the application of combinatorial techniques to the theory of complex hyperplane arrangements.

In the course of investigation it has turned out that deep structural properties of arrangements are controlled by its matroid, and combinatorial methods allow to not only compute important invariants (such as the cohomology algebra of the complement, and the homotopy type of the link) but also identify correctly extreme cases with special structure (supersolvable and 3-generic arrangements).

In the following sketch we focus on the links and connections between **combinatorial** data (hyperplane arrangements as represented matroids), **algebraic structure** (hyperplane arrangements as singular varieties) and **topological aspects** (complements of arrangements as complex manifolds).

We refer to the lecture notes by Orlik (1989) and the book by Orlik and Terao (1992) on arrangements for further details, expositions and extensive bibliographies.

For this section we restrict our attention to the following scenario (although greater generality is possible and natural for many aspects).

6.1 Definition. *A* hyperplane arrangement *is a finite set $X = \{H_1, \ldots, H_m\}$ of hyperplanes (vector subspaces of codimension 1) in a complex vector space $V = \mathbb{C}^n$, with $\bigcap_{i=1}^m H_i = \{0\}$.*

This definition describes *complex* arrangements (it is also interesting to study arrangements over other fields, the case of arrangements in real vector spaces being the best studied one). The arrangements considered here are *linear*, because all hyperplanes are required to contain the origin, and they are *essential*: the last condition requires that the *dimension* $n = \dim(V)$ coincides with the *rank* $r = \mathrm{codim}_V(\bigcap_{i=1}^m H_i) = n - \dim(H_1 \cap \ldots \cap H_m)$ of the arrangement X. These last two conditions (linear and essential) are not very restrictive – usually questions are easily reduced to this case. There are, in fact, standard constructions that transform from *affine* or *projective* arrangements to linear ones, and every arrangement has a canonical essential arrangement associated with it.

Choosing coordinates $x_1, \ldots, x_n \in V^*$ for V, we write $S := \mathbb{C}[x_1, \ldots, x_n]$ for the ring of polynomial functions on V. For every hyperplane $H \in X$ we can then choose a linear form $\ell_H \in V^*$ whose kernel is H, which may also be seen as a linear function $\ell_H \in S$ that defines $H = \{x \in V : \ell_H(x) = 0\}$.

The product $Q := \prod_{H \in X} \ell_H \in S$ is thus interpreted as a *defining equation* for the arrangement X: it defines the hypersurface obtained by the union of the hyperplanes in X. Note that both Q and the ℓ_H are unique up to a non-zero complex factor.

We will in the following sketch structures associated with hyperplane arrangements by various branches of mathematics. The common questions will be:

– *How much of the structure of a hyperplane arrangement is encoded in and determined by its combinatorics?*
– *Do the combinatorial data allow simple construction or computation of the relevant information?*
– *Do the combinatorial invariants identify interesting special cases with additional structure?*

In the light of these questions, the following three sections will first consider the combinatorics associated with an arrangement, then the topological properties and finally algebraic structures.

The Matroid of an Arrangement. The *combinatorial structure* associated with a hyperplane arrangement is that of a *matroid* (cf. Chapter 9). [This contrasts the case of real arrangements, where much more information is encoded in the associated *oriented matroid* (cf. Chapter 9,§15 and Björner, Las Vergnas, Sturmfels, White and Ziegler (1993)).]

6.2 Definition. *The* matroid $M = M_X$ *of the arrangement* X *is given by linear independence on the set* $\{\ell_H : H \in X\}$ *of vectors in* V^**. A property of arrangements is* combinatorial *if it is determined by the matroid of the arrangements alone.* M *is a matroid of rank* $r(M) = n$ *on a ground set of* $m = |X|$ *elements, which we identify with* X*. Important invariants for the following are its* lattice of flats*, which is isomorphic to the intersection lattice*

$$L = \{\bigcap Y : Y \subseteq X\}$$

(ordered by reverse inclusion), its characteristic polynomial

$$\chi(t) = \sum_{x \in L} \mu(\hat{0}, x) t^{n-r(x)} = \sum_{i=0}^{r} w_i (-1)^i t^{n-i},$$

and the broken circuit complex $BC(M) \subseteq 2^{\{1,2,\ldots,m\}}$*, a simplicial complex with exactly* w_i *faces of cardinality* i*, which implies* $w_i > 0$ *for* $0 \leq i \leq n$*.*

We will now introduce three classes of hyperplane arrangements that are distinguished by combinatorial conditions, but also by algebraic and topological ones, as we will soon see.

— A hyperplane arrangement is *supersolvable* if its matroid is supersolvable (in the sense of Stanley (1972), that is, if its intersection lattice contains a maximal chain of modular elements).

  A key fact is the factorization $\chi(t) = \prod_{i=1}^{n}(t - e_i)$ for positive integers e_i in this case. This can be explained by a factorization of the broken circuit complex which characterizes supersolvability, according to Björner and Ziegler (1991).

  Supersolvable arrangements form a very interesting class of highly structured arrangements. For example, if G is a graph on $\{1, \ldots, n\}$, then the arrangement of hyperplanes $x_i = x_j$ (for $ij \in E(G)$) is supersolvable if and only if the graph is chordal.

— An arrangement is *generic* if arbitrary small perturbations do not change the combinatorial structure. This is equivalent to the property that the matroid M is *uniform*, such that $M \cong U_{n,m}$.

  A weaker condition is that no hyperplane of the arrangement contains the intersection of two other hyperplanes. Equivalently, we require that M contains no 3-circuits, which defines 3-*generic* arrangements.

  The 3-generic arrangements are a large class of arrangements with very little (combinatorial) structure.

— A third class of "special" (although not combinatorially defined) complex arrangements arises by complexifying simplicial real arrangements (that is, by field extension for arrangements that subdivide $\mathbb{R}^n$ into simplicial cones). Such arrangements arise, for example, from the action of finite Coxeter groups (groups generated by reflections), when one considers the arrangement of all hyperplanes of reflections in the group.

  Complexified real arrangements can be treated in terms of the combinatorial data given by the real hyperplane arrangement. This is the reason why they are much better understood than general complex ones.

Topology of the Complement. Consider the hyperplane arrangement X as a complex hypersurface (of real codimension 2!) in V. Then $T := V \backslash X$, called the *complement* of the arrangement, is a connected open complex manifold with interesting cohomology and homotopy properties. Closely related to this one studies the *link* $D := X \cap S^{2n-1}$, the intersection of the arrangement with the unit sphere in $\mathbb{C}^n$.

Note that for the real analogue (a linear arrangement in $\mathbb{R}^n$), this complement is a union of disjoint open convex cones, and so its topological structure is entirely determined by the number of its components, which is described by Zaslavsky's theorem (see Chapter 17). The link has the homotopy type of a wedge of $(n-2)$-spheres. In contrast to this, no complete description of (say, the homotopy type of) the space T is known for the complex case. However, one can describe the homotopy type of the link in this case, see below.

In the following, we will present a complete combinatorial construction of the cohomology algebra of T, and some interesting partial results for the homotopy structure.

The construction for the cohomology algebra can be sketched as follows. Let E be a free $\mathbb{Z}$-module with basis $\{e_1, \ldots, e_m\}$ in bijection with X. Let ΛE be the exterior algebra over E, with basis $\{e_K : K \subseteq [n]\}$. Denote by I the ideal of ΛE which is generated by all the elements of the form $\partial(e_C)$, where C is a circuit of M. Here the boundary map ∂ is defined by linear extension of

$$\partial(e_K) \quad = \quad \sum_{j=1}^{p} (-1)^{j-1} e_{K-\{i_j\}}, \qquad \text{for} \quad K = \{i_1, i_2, \ldots, i_p\}_<.$$

Now define the *Orlik-Solomon algebra* of X as $A(M) := \Lambda E/I$. This algebra is combinatorial, since it is constructed from matroid data only. It provides a model for the cohomology algebra of T which is combinatorial in the sense of Definition 6.2.

6.3 Theorem. [Orlik and Solomon (1980)] *Let X be a complex arrangement, M its matroid and T its complement. Then the cohomology algebra of T (with integer coefficients) is isomorphic as a graded $\mathbb{Z}$-algebra to the Orlik-Solomon algebra $A(M)$:*

$$H^*(T, \mathbb{Z}) \quad \cong \quad A(M).$$

This fundamental theorem allows a complete analysis of the cohomology of T with well-developed combinatorial tools. So one finds that the broken circuit complex of M induces a basis of $A(L)$ and hence of the cohomology algebra $H^*(T, \mathbb{Z})$. This follows from Björner (1982) and Orlik and Solomon (1980) and was rediscovered by Jambu and Terao (1989). In particular this proves that the Betti numbers of T are given by

$$\beta^i(T) \quad = \quad \operatorname{rank} H^i(T, \mathbb{Z}) \quad = \quad w_i,$$

such that the Poincaré polynomial of $H^*(T, \mathbb{Z})$ is $t^n \chi(-\frac{1}{t})$ (Orlik and Solomon 1980). It can also be used for an elementary proof of Theorem 6.3, see Björner and Ziegler (1992).

With observations of this type there is a complete analysis of the cohomology algebra of T with matroid theory tools. Similarly, the following result shows that the homotopy type of the link D is combinatorial.

6.4 Theorem. [Björner and Ziegler (1992), Ziegler and Živaljević (1993)] *The link $D = X \cap S^{2n-1}$ of every complex arrangement has the homotopy type of a wedge of spheres, put together from w_i spheres of dimension $2n-2-i$, for $i > 0$:*

$$D \quad \simeq \quad \bigvee_{A \in BC(M) \setminus \emptyset} S^{2n-2-|A|}.$$

Here for $d = 2$ the wedge is formed to produce a disjoint union of circles. Otherwise, the link is connected and the homotopy type of the wedge does not depend on the choice of wedge points.

The approach of Björner and Ziegler (1992) produces explicit spheres S_A in the link D that induce the homotopy equivalence. The "diagram method" of Ziegler and Živaljević (1993) works in a much more general situation. It produces homotopy formulas for links of arrangements of arbitrary real subspaces, and the above is just a special application of their method.

Using Alexander duality (see Spanier (1966)), one gets from Theorem 6.4 the *linear structure* of the cohomology algebra of T. However, the *multiplicative structure* described by Theorem 6.3 cannot be derived from the homotopy type of the link: it encodes subtle details about the complex structure of the arrangement, see Ziegler (1993).

Also, via Spanier-Whitehead duality one gets from Theorem 6.4 that the complement T has the stable homotopy type of a wedge of spheres (i.e., after a sufficient number of suspensions it is homotopy equivalent to a wedge of spheres). However, a complete description of the homotopy type of T seems to be out of reach. In fact, the following basic problems are open, see Falk and Randell (1985), Salvetti (1987).

- Is the homotopy type of a complex arrangement combinatorial? That is, do arrangements with isomorphic matroids always have homotopy equivalent complements?
- In particular, is the fundamental group $\pi_1(T)$ combinatorial? That is, can one give a presentation of $\pi_1(T)$ from the knowledge of M alone?

Without a positive solution to this problem, more data than just the matroid are necessary to construct the homotopy type of an arrangement. For example, in the case of complexified real arangements, one can construct T *up to homeomorphism* using the additional data given by the oriented matroid of the real arrangement. This was shown by Björner and Ziegler (1992), extending an earlier similar result of Salvetti (1987) for the homotopy type.

In the general complex case, several non-trivial results have been given, and there is very active research going on. See, for example, Arvola (1992) and Falk (1993) for recent progress. Much of the attention centers on the first homotopy group $\pi_1(T)$, together with the question under which conditions T is a $K(\pi,1)$ space, that is, the higher homotopy groups $\pi_i(T)$ $(i>1)$ vanish.

Crucial parameters are given by the *lower central series* of $\pi_1(T)$, defined by $c_k := \text{rank}(G_k/G_{k+1})$, where $G_1 = \pi_1(T)$, and $G_{k+1} = [G_k, G_1]$ is the subgroup of G_1 generated by the commutators $ghg^{-1}h^{-1}$ for elements $g \in G_k$ and $h \in G_1$.

6.5 Theorem. *Let T be the complement of a complex arrangement X.*

(1) (Hattori 1975) *If X is generic and $|X| > n \geq 2$, then T is not a $K(\pi,1)$ space: in this case $\pi_i(T) = 0$ for $1 < i < n$, and $\pi_n(T)$ is free abelian on an infinite number of generators.*

(2) (Deligne 1972) *If X is a complexified simplicial arrangement, then T is a $K(\pi,1)$ space.*

(3) (Terao 1986, Falk and Randell 1985) *If X is supersolvable, then T is a $K(\pi,1)$ space, and its lower central series is given by $\prod_{j=1}^{\infty}(1-t^j)^{c_j} = \prod_{k=1}^{n}(1-e_k t) = t^n \chi(\frac{1}{t})$.*

The combinatorics underlying Deligne's Theorem 6.5(2) was clarified recently by Paris (1991a,b), see also Cordovil (1991) and Salvetti (1993).

It is safe to say that the homotopy groups of T are in general extremely complicated objects. We just mention that the formula in part (3) of this theorem fails even for very nice complexified simplicial arrangements.

The homotopy structure of T is, nevertheless, a very promising field of research, and combinatorial approaches and methods should be helpful to attack some basic open problems, the most striking ones being the following "$K(\pi, 1)$-problems" (of which the last one is is a special case of Problem 6.4):

– Does Hattori's result Theorem 6.5(1) generalize to 3-generic arrangements? Or can T be a $K(\pi, 1)$ for some 3-generic arrangement?
– Describe neccessary and sufficient conditions for T to be a $K(\pi, 1)$.
– Does the matroid alone determine whether the complement of a complex arrangement is a $K(\pi, 1)$?

The Module of Logarithmic Vector Fields. An *algebraic* structure of interest here is the S-module of algebraic vector fields that are tangent to the hyperplanes. Saito's (1980) investigations in singularity theory first suggested to study these modules of *logarithmic vector fields* and, dually, of *logarithmic differential forms* at a hypersurface singularity. Specialization to the case of hyperplane arrangements lead Terao (1980) to his fascinating theory of *free* hyperplane arrangements.

The following module captures a lot of structure of the arrangement. Its control by combinatorial data is quite strong, but not straightforward.

6.6 Definition. *Let X be a complex arrangement defined by $Q = \prod_{H \in X} \ell_H \in S$. The* S-module of logarithmic vector fields *at X is the set of derivations*

$$\mathrm{Der}(X) = \left\{ \theta = \sum_{i=1}^n p_i \frac{\partial}{\partial x_i} : Q | \theta(Q) \right\}$$

with the obvious S-module structure.

There is also a very simple, geometric description: $\mathrm{Der}(X)$ *is isomorphic to the module of all polynomial maps* $\mathbf{p} : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ *that map every hyperplane of X into itself.*

For this, $\mathbf{p}$ is considered as an n-tuple $\mathbf{p} = (p_1, \dots, p_n) \in S^n$ of n-variable polynomials; the corresponding element in $\mathrm{Der}(X)$ is $\theta_{\mathbf{p}} = \sum_{i=1}^n p_i \frac{\partial}{\partial x_i}$. To see that the set of such maps $\mathbf{p}$ is an S-module, one has to show that S-linear combinations have the same form.

The following "basis criterion" of Saito (1980) identifies the case when $\mathrm{Der}(X)$ is a free module (that is, has a basis).

6.7 Lemma. *The logarithmic vector fields $\theta_1, \dots, \theta_n \in \mathrm{Der}(X)$ with $\theta_i = \sum_{j=1}^n p_{ij} \frac{\partial}{\partial x_j}$ form a basis of* $\mathrm{Der}(X)$ *if and only if* $\det(p_{ij}) = cQ$ *for a non-zero constant $c \in C$.*

This situation arises in many important examples and provides an algebraic criterion for "strong combinatorial structure" in an arrangement.

6.8 Definition. [Terao (1980)] *The arrangement X is* **free** *if* $\mathrm{Der}(X)$ *is a free S-module.*

$\mathrm{Der}(X)$ is an S-module of rank n (every maximal S-linearly independent subset has cardinality S), such that the basis criterion above characterizes (bases of) free arrangements.

At this point we observe that it pays off to also study the dual module $\Omega^1(X) = \mathrm{Hom}_S(\mathrm{Der}(X), S)$ of *logarithmic 1-forms at X*, because it has additional structure. $\Omega^1(X)$ is the S-module of differential 1-forms $\omega = \frac{1}{Q}\sum_{i=1}^n q^i \mathrm{d}x_i$ with $q^i \in S$, such that $\mathrm{d}\omega$, like ω, has at most a first order pole at every hyperplane $H \in X$. This is equivalent to requiring that the restrictions $(Q\omega)|_H$ vanish. The differential forms $\frac{\mathrm{d}\ell_H}{\ell_H}$ for $H \in X$ are some obvious elements of $\Omega^1(X)$.

There is a non-degenerate pairing between $\mathrm{Der}(X)$ and $\Omega^1(X)$. In particular $\Omega^1(X)$ is free if and only if $\mathrm{Der}(X)$ is free, which offers a second approach to free arrangements.

Both $\mathrm{Der}(X)$ and $\Omega^1(X)$ have the natural structure of a graded module, where $\theta \in \mathrm{Der}(X)$ is homogeneous of degree e if $\theta = \sum_{i=1}^n p_i \frac{\partial}{\partial x_i}$, where all the p_i are either 0 or homogeneous of degree e. Similarly, a logarithmic differential form $\omega = \frac{1}{Q}\sum_{i=1}^n q^i \mathrm{d}x_i$ has degree $e - m$ if all the polynomials q^i are either zero or homogeneous of degree e: here $m = |X|$ is the degree of Q.

So for every $H \in X$, $\frac{\mathrm{d}\ell_H}{\ell_H}$ is a form of degree -1, whereas $\frac{1}{\ell_1}(\frac{\mathrm{d}\ell_2}{\ell_2} - \frac{\mathrm{d}\ell_3}{\ell_3})$ is a form of degree -2 in $\Omega^1(X)$ if and only if the linear forms ℓ_1, ℓ_2, and ℓ_3 are dependent, so the corresponding hyperplanes satisfy $H_1 \supseteq (H_2 \cap H_3)$, that is, they form a 3-circuit in M_X.

Now if $\mathrm{Der}(X)$ is free, then it has a basis $\{\theta_1, \ldots, \theta_n\}$ consisting of homogeneous vector fields $\theta_i = \sum_{j=1}^n p_{ij} \frac{\partial}{\partial x_j}$ of respective degrees e_i. Similarly, $\Omega^1(X)$ then has a homogeneous basis $\{\omega_1, \ldots, \omega_n\}$ with degrees $\deg(\omega_j) = -e_j$, which is explicitly given as $\omega_j = \sum_{i=1}^n q^{ij} \mathrm{d}x_i$, where the matrices (q^{ij}) and (p_{ij}) are inverses of each other.

Terao's (1982) remarkable "Factorization Theorem" now implies that the degrees of these homogeneous basis elements – if X is free – can be computed combinatorially.

6.9 Theorem. [Terao (1981)] *If X is a free arrangement, then the characteristic polynomial of M_X factors as*

$$\chi(t) = \prod_{i=1}^n (t - e_i),$$

where the e_i are the degrees of the vector fields in a homogeneous basis of $\mathrm{Der}(X)$.

This result in particular allows to disprove freeness for large classes of examples. It also suggests classes of arrangements that "ought to be free" – because they meet the strong combinatorial criterion that $\chi(t)$ factors over $\mathbb{Z}$.

The original proof of this result was very difficult. New ideas by Solomon and Terao (1987) leading to Rose and Terao's (1990) concept of a "Möbius sum with Hilbert coefficients" put this into a simpler and broader framework.

Theorem 6.9 is part of a bulk of evidence for the following conjecture that has motivated a lot of research on free arrangements.

6.10 "Terao's Conjecture". *Freeness is a combinatorial property.*

Extensive work has gone into this conjecture, without final success, yet. Special cases can be settled: for example, arrangements with a graphic matroid are free if and only if they are supersolvable (Stanley, see Edelman and Reiner (1992)), and Terao's conjecture is true if the matroid is binary (Ziegler 1990). Edelman & Reiner (1992) characterized freeness for a larger class of arrangements (described in terms of graphs), which includes both free and nonfree arrangements. Their analysis also provides classes of counterexamples to "Orlik's conjecture": it is *not* true that the restriction of a free arrangement to one of its hyperplanes always a free arrangement, see Edelman and Reiner (1991).

Furthermore, ten years of research have clarified the structure of the Saito-Terao modules quite a bit, and in this course the importance and the scope of the underlying combinatorial structure has become more apparent – see also Ziegler (1990) and Yuzvinsky (1993). It has also led to algebraic characterizations for the two combinatorial classes of arrangements discussed above.

6.11 Theorem. [Stanley (1984); Jambu and Terao (1984); Ziegler (1989)] *Let X be a complex arrangement.*

(1) *X is supersolvable if and only if it is free with a basis $\{\theta_1, \ldots, \theta_n\}$ of* $\mathrm{Der}(X)$ *that (in suitable coordinates) has an upper-triangular coefficient matrix: $\theta_i = \sum_{j=i}^{n} p_{ij} \frac{\partial}{\partial x_j}$ for $1 \leq i \leq n$.*

(2) *X is 3-generic if and only if the module $\Omega^1(X)$ does not contain forms of degree -2, that is, if it is generated by $\{\frac{\mathrm{d}\ell_H}{\ell_H} : H \in X\}$.*

Thus a 3-generic arrangement (and, in particular, a generic arrangement in dimension $n \geq 3$) can never be free unless $n = m$.

The role of the complexified simplicial arrangements is less clear in this context. Terao (1980) has shown, analyzing the $n = 3$ case, that many, but not all such arrangements are free. This leads to the following open question, which also links freeness to the topological properties that we have studied before.

– Is T a $K(\pi, 1)$ space for every free arrangement X? (This was conjectured by Saito. The converse was disproved by Terao (1980), via his Theorem 6.9 and Deligne's Theorem 6.5(2)).

A lot of work will still have to be done, elaborating on the interpretation and relevance of combinatorial data for the complex structure of hypersurface singularities. Combinatorial, discrete data control much of the algebraic and topological properties. To understand how this works, also in much more general settings than the model of this section, should lead to a deeper understanding of the connections between singularity theory, local topology, reflection groups, and a zoo of other topics that we have not even touched upon here.

7. Knots and the Tutte polynomial

In this section we present a recent development in knot theory, which has turned out to be very closely related to classical combinatorial constructions like the Tutte polynomial of a graph. We will not have the opportunity to discuss another exciting development: the recent approach of Vassiliev (1990), which gives a systematic method to produce knot invariants, and reduces in a completely different way to combinatorial problems, see also Birman and Lin (1993). We refer to Burde and Zieschang (1985) for a broad development

The trefoil knot The Borromean Rings: a 3-component link

Figure 7.1

of the "classical" knot theory. More extensive surveys of the recent progress are Kauffman (1988), Lickorish (1988) and Birman (1993).

A *link* L with $c(L)$ *components* consists of $c(L)$ disjoint simple smooth closed curves in $\mathbb{R}^3$. A *knot* is a link with one component. The natural way to represent a link L is by means of a *link diagram*, which is obtained from L by projecting it onto a plane in such a way that a plane in such a way that the projection of each component is smooth and at most two curves intersect at any point. At each crossing point of the link diagram the curve which goes over the other is specified as shown in Figure 7.1.

Two links are *equivalent* if one can be deformed continously to the other in three dimensional space. A knot is *trivial* if it is equivalent to the knot without a crossing, the *unknot* "O". A link is trivial if it is equivalent to a disjoint union of trivial, unlinked knots, that is, to a link with out a crossing. The *union* "$\cup$" operation used for this places two link diagrams into the plane such that they do not touch.

Clearly a link diagram represents a unique link up to equivalence, but many diagrams can represent the same link. Modifying a link diagram locally as represented in Figure 7.2 does not change the link represented; these local changes are known as the *Reidemeister moves* of type I, II and III. The classic theorem of combinatorial knot theory is:

7.1 Theorem. *Two link diagrams represent equivalent links if and only if one can be obtained from the other by a finite sequence of Reidemeister moves.*

Figure 7.2

Reidemeister's classic theorem is an existence theorem: it does not provide an algorithm of any "time bounded" complexity for testing whether or not two links are equivalent, see for example the remark in Burde and Zieschang (1985).

As a result, any invariant f of a link which is both easily calculated and has the property that L_1 and L_2 are equivalent only when $f(L_1) = f(L_2)$ is clearly of great significance in the theory of knots.

Here we shall present an easily derived "partial invariant" namely the Jones polynomial, discovered by V.F.R. Jones (1985). In order to do this we introduce first the closely related bracket polynomial introduced by L. Kauffman (1987).

The Bracket Polynomial. For any link diagram L define a Laurent polynomial $\langle L \rangle$ in one variable A, which obeys the following three rules:

(i) $\langle O \rangle = 1$,

(ii) $\langle L \cup O \rangle = -(A^2 + A^{-2})\langle L \rangle$,

(iii) $\Big\langle \quad \Big\rangle = A\Big\langle \quad \Big\rangle + A^{-1}\Big\langle \quad \Big\rangle.$

Notes:

I. A *Laurent polynomial* in z is a polynomial featuring positive powers of z and z^{-1}.

II. The rule (iii) is applied locally, that is, at each crossing of the link diagram.

III. Rules (i) to (iii) recursively define the bracket $\langle L \rangle$ for every link L: (i) starts the recursion with the unknot, (iii) expresses $\langle L \rangle$ in terms of brackets of links with less crossings, and (ii) deletes components without crossings, for example for trivial links.

The fundamental properties of $\langle \, . \, \rangle$ are summed up in:

7.2 Theorem. *For any link L the bracket polynomial* $\langle L \rangle$ *is independent of the order in which rules* (i) *to* (iii) *are applied to the crossings and furthermore is invariant under the Reidemeister moves* II *and* III.

It is important to note that:

7.3 Proposition. *The bracket polynomial is not invariant under Reidemeister move I.*

Proof: Apply move I to get

$$\Big\langle \quad \Big\rangle = A\Big\langle \quad \Big\rangle + A^{-1}\Big\langle \quad \Big\rangle = -A(A^2 + A^{-2})\Big\langle \quad \Big\rangle + A^{-1}\Big\langle \quad \Big\rangle = -A^3\Big\langle \quad \Big\rangle. \qquad \blacksquare$$

Oriented links and the Jones polynomial. Suppose now that the link L is *oriented*, by which we mean that each of its components is assigned an arrow representing a direction of motion along the given component. Once the orientation has been given we may assign a *sign* to each crossing of the link diagram by the rule displayed in Figure 7.3.

$+ve$ crossing $\qquad$ $-ve$ crossing

Figure 7.3

A crossing is *positive* if the over arc at the crossing is on the left as one approaches the crossing in the direction of the two indirected arcs.

Figure 7.4: An oriented link with writhe $\omega(L) = 1$

The *writhe* of an oriented link L is the sum of the signs at the crossings of L and is denoted by $\omega(L)$ (see Figure 7.4). The writhe is *not* an invariant of a link since it changes by ± 1 under the type I Reidemeister move. However it turns out that if we combine the writhe with the bracket polynomial of Kauffman we get a link invariant.

7.4 Theorem. *For an oriented link L, the function*

$$V_L(t) = f_L(t^{-1/4})$$

where

$$f_L(A) = (-A^3)^{\omega(L)} \langle L \rangle$$

is an invariant of the link.

$V_L(t)$ is called the *Jones polynomial* of the oriented link L.

From Knots to Signed Graphs. Now given any unoriented link L there is a natural way in which to associate with it a *signed graph* $G(L)$, constructed as follows.

Two-colour the faces of the link diagram of L with colours black and white in such a way that adjacent faces have different colours. (This is possible since L, regarded as a graph, is planar and regular of degree 4, hence eulerian. Thus its dual graph is bipartite.) By convention let the unbounded face be white. Let $G(L)$ have vertices corresponding to the black faces and join two vertices of $G(L)$ when the corresponding faces are the opposite faces of a crossing. The sign of the crossing is defined by the convention illustrated in Figure 7.5.

$+ve$ $-ve$

Figure 7.5

This is that a crossing is *positive* when viewed along the edge joining the two black faces over the edge is on the left; otherwise it is *negative*.

In general the graph $G(L)$ will have both positive and negative edges but there is an important class of knots (links), called *alternating links*, for which $G(L)$ has edges of only one sign.

A link diagram L is *alternating* if the crossings alternate under-over-under-over… as the link is traversed. It is very easy to verify: A link is *alternating* if it has some link diagram that is alternating.

7.5 Lemma. *A link L diagram is alternating iff the edges of the associated signed graph $G(L)$ are all positive or all negative.*

Alternating links; the Jones, Bracket and Tutte Polynomial. In general the bracket polynomial and Jones polynomial of a link will not be completely specified by the graph $G(L)$, they will also depend on the signs associated with the edges of $G(L)$. However in the important case where L is an alternating link diagram, we saw above that all edges of $G(L)$ have the same sign and hence essentially the undirected graph $G(L)$ determines L.

Now consider the fundamental bracket equation or skein diagram (as it is called in knot theory).

$$\left\langle \qquad \right\rangle = A \left\langle \qquad \right\rangle + A^{-1} \left\langle \qquad \right\rangle.$$

In terms of the associated graph $G(L)$, this can be translated to

$$\left\langle \begin{matrix} \cdot\, u \\ \cdot v \end{matrix} \right\rangle = A \left\langle \begin{matrix} \cdot\, u \\ \cdot v \end{matrix} \right\rangle + A^{-1} \left\langle \quad \cdot\, uv \right\rangle,$$

which is exactly the contract/delete formulation used in the definition of the Tutte polynomial of a graph and matroid (see Chapter 9).

It is not surprising therefore that we have the following fundamental relationship.

7.6 Theorem *If L is an oriented alternating link and G denotes its associated unsigned "black face" graph then the Jones polynomial $V_L(t)$ is given by*

$$V_L(t) = (t^{-1/4})^{3\omega(L)-2} T(G; -t, -t^{-1})$$

where $T(G; x, y)$ is the Tutte polynomial of G.

In other words, the Jones polynomial of an alternating link is given by the evaluation of the Tutte polynomial of its associated black face graph along the hyperbola $xy = 1$, up to an easily derived factor.

A Proof of a Conjecture by Tait. As an example of the use of these knot polynomials we show a very simple proof of a longstanding conjecture by Tait (1898).

Consider first the knot K of Figure 7.6. The crossing joining AB is called an *isthmus* because in the associated link diagram the edge AB will be an isthmus in the usual graph theoretic sense. A link diagram is *reduced* if it has no crossing which is an isthmus.

Figure 7.6

It is easy to see that the knot represented by Figure 7.6 is equivalent to the alternating knot K' obtained by "twisting one component and removing the isthmus crossing AB".

The key fact we shall need is the following, obtained by considering the representation of $\langle K \rangle$ in terms of the Tutte polynomial of $G(K)$:

7.7 Theorem *Let L be a reduced alternating diagram, then in the bracket polynomial $\langle K \rangle$*

$$\text{max degree}\langle K \rangle = V + 2(W - 1)$$

$$\text{min degree}\langle K \rangle = -V - 2(B - 1)$$

where V is the number of regions and W and B are the number of white (respectively black) regions in the shaded graph $G(L)$.

We now state and prove Tait's conjecture.

7.8 Theorem [Murasugi (1987), Thistlethwaite (1987)]. *The number of crossings in a reduced alternating projection of a link L is a topological invariant of L.*

Expressed more informally, this means that if we have a link diagram which is alternating and contains no isthmuses and has n crossings then we know that there is no other reduced alternating link diagram representing the same knot and having a different number of crossings.

Proof. Let span(L) denote the difference between the maximum and minimum degrees of A in the bracket polynomial $\langle L\rangle$. By Theorem 7.7 (with the notation introduced there) we have

$$\text{max degree}\langle K\rangle = V + 2(W-1)$$
$$\text{min degree}\langle K\rangle = -V - 2(B-1).$$

Thus span$(L) = 2V + 2(W + B - 2)$ and since $W + B = V + 2$ (Euler's formula for planar graphs) we have span$(L) = 4V$. But $f(L) = a^{-\omega(L)}\langle L\rangle$ is a topological invariant of links, thus span(L) is also, hence V, the number of crossings in an alternating presentation, is also a topological invariant. ∎

References

N. Alon and V. D. Milman (1983), Embedding of ℓ^k_∞ in finite dimensional Banach spaces, *Israel J. Math.* **45**, 265–280.

W. A. Arvola (1992), The fundamental group of the complement of an arrangement of complex hyperplanes, *Topology* **31**, 757-765.

D. Avis and M. Deza (1991), The cut cone, L^1-embeddability, complexity and multicommodity flows, *Networks* **21**, 595–617.

L. Babai (1981), On the order of uniprimitive permutation groups, *Ann. Math.* **113**, 553–568.

L. Babai (1982), On the order of doubly transitive permutation groups, *Invent. Math.* **68**, 473–484.

K. Bacławski (1981), Rings with lexicographic straightening law, *Advances in Math.* **39**, 185–213.

K. Bacławski, and A. M. Garsia (1981), Combinatorial decompositions of rings, *Advances in Math.* **39**, 155–184.

F. Barahona and A.R.Mahjoub (1986), On the cut polytope, *Math. Programming* **36**, 157–173.

J. S. Birman (1993), New points of view in knot theory theory, *Bull. Amer. Math. Soc.* **28**, 253–287.

J. S. Birman and X.-S. Lin (1993), Knot polynomials and Vassiliev's invariants, *Invent. Math.* **111**, 225–270.

A. Björner, A. M. Garsia, and R. P. Stanley (1982), An introduction to Cohen-Macaulay partially ordered sets, in: *Ordered Sets* (I. Rival, ed.), D. Reidel, 583–615.

A. Björner, M. Las Vergnas, B. Sturmfels, N. White and G. M. Ziegler (1993), Oriented Matroids, Encyclopedia of Mathematics, Vol. 46, Cambridge University Press, Cambridge.

A. Björner and M. Wachs (1982), Bruhat order of Coxeter groups and shellability, *Advances in Math.* **43**, 87–100.

A. Björner and G. M. Ziegler (1991), Broken circuit complexes: factorizations and generalizations, *Journal of Comb. Theory*, Ser. B **51**, 96-126.

A. Björner and G. M. Ziegler (1992), Combinatorial stratification of complex arrangements, *Journal Amer. Math. Soc.* **5**, 105-149.

A. Bochert (1889), Über die Zahl der verschiedenen Werthe, die eine Funktion gegebener Buchstaben durch Vertauschung derselben erlangen kann, *Math. Annalen* **33**, 584–590.

G. Burde and H. Zieschang (1985), *Knots*, de Gruyter, Amsterdam.

R. Cordovil (1991), On the homotopy of the Salvetti complexes determined by simplicial arrangements, preprint, 1991.

C. De Concini, D. Eisenbud and C. Procesi (1982), Hodge algebras, *Astérisque* **91**.

C. De Concini and V. Lakshmibai (1981), Arithmetic Cohen-Macaulayness and arithmetic normality for Schubert varieties, *Amer. J. of Math.* **103**, 835–850.

C. De Concini and C. Procesi (1981), Hodge algebras. A survey, in: *Proc. Int. Conference "Young tableaux and Schur functors in algebra and geometry"*, Torun, Poland 1980, *Astérisque* **87-88**, 79–83.

P. Deligne (1972), Les immeubles des groupes de tresses généralisés, *Invent. Math.* **17**, 273–302.

M. Deza [M.E.Tylkin] (1960), On the Hamming geometry of unit cubes, *Doklady Akad. Nauk SSSR* **134** 1037–1040.

M. Deza and M. Laurent (1992a), Facets for the cut cone I, *Mathematical Programming* **56**, 121–160.

M. Deza and M. Laurent (1992b), Facets for the cut cone II: clique-web facets, *Mathematical Programming* **56**, 161–188.

M. Deza and M. Laurent (1992c), New results on facets of cut cone, *Journal of Combinatorics, Information and System Sciences* **17**, 19–38.

M. Deza, V. P. Grishukhin and M. Laurent (1991), The hypermetric cone is polyhedral, preprint; *Combinatorica*, to appear.

A. Dvoretzky (1959), A theorem on convex bodies and applications to Banach spaces, *Proc. Natl. Acad. Sci. USA* **45**, 223–226.

P. H. Edelman and V. Reiner (1991), A counterexample to Orlik's conjecture, preprint, 1991; *Proceedings Amer. Math. Soc.*, to appear.

P. H. Edelman and V. Reiner (1992), Free hyperplane arrrangements between A_{n-1} and B_n, preprint 1992, 18 pages.

D. Eisenbud (1980), Introduction to algebras with straightening laws, in: *Ring Theory and Algebra*, Proc. 3rd Oklahoma Conference (B.R. McDonald, ed.), Marcel Dekker, New York.

M. J. Falk (1993), Homotopy types of line arrangements, *Inventiones Math.* **111**, 139–150.

M. J. Falk and R. Randell (1985), The lower central series of a fiber-type arrangement, *Invent. Math.* **82**, 77–88.

T. Figiel, J. Lindenstrauss and V. Milman (1977), The dimension of almost spherical sections of convex bodies, *Acta Math.* **139**, 53–94.

A. M. Garsia (1980), Combinatorial methods in the Theory of Cohen-Macaulay rings, *Advances in Math.* **38**, 229–266.

M. Grötschel, L. Lovász and A. Schrijver (1988), *Geometric Algorithms and Combinatorial Optimization*, Algorithms and Combinatorics **2**, Springer-Verlag, Berlin Heidelberg.

P. Halmos (1950), *Measure Theory*, Van Nostrand, Princeton, NJ.

A. Hattori (1975), Topology of $\mathbb{C}^n$ minus a finite number of hyperplanes in general position, *J. Fac. Sci. Univ. Tokio* **22**, 205–219.

M. Hochster (1972), Rings of invariants of tori, Cohen-Macauay rings generated by monomials, and polytopes, *Annals of Math.* **(2) 96**, 318–337.

M. Iri (1970), On an extension of the max-flow-min-cut theorem to multicommodity flows, *J. Oper. Res. Japan* **13** 129–135.

M. Jambu and H. Terao (1984), Free arrangements of hyperplanes and supersolvable lattices, *Advances in Math.* **52** 248–258.

M. Jambu and H. Terao (1989), Arrangements of hyperplanes and broken-circuits, in: *Singularities*, Proceedings of the International Conference on Singularities, Iowa City 1986, *Contemporary Math.* **90**, 147–162.

V. B. Johnson and G. Schechtman (1981), On subspaces of L_1 with maximal distance to euclidean space, in: *Proc. Res. Workshop on Banach Space Theory* (ed. Bor Luh Lin), Univ. of Iowa, 83–96.

V. F. R. Jones (1985), A polynomial invariant for knots via von Neumann algebras, *Bull. Amer. Math. Soc.* **12**, 103–111.

C. Jordan (1961), *Oeuvres I*, (ed. J. Dieudonné), Gauthier-Villars, Paris, 408, 453.

A. V. Karzanov (1985), Metrics and undirected cuts, *Math. Prog.* **32**, 183–198.

L. H. Kauffman (1987), State models and the Jones polynomial, *Topology* **26**, 395–407.

L. H. Kauffman (1988), New invariants in the theory of knots, *American Math. Monthly* **95**, 195–242.

J. B. Kelly (1970), Matric inequalities and symmetric differences, in: *Inequalities II*, Academic Press, New York, 193–212.

J. B. Kelly (1975), Hypermetric spaces, in: *Lecture Notes in Math.* **490**, Springer-Verlag, 17–31.

B. Kind and P. Kleinschmidt (1979), Schälbare Cohen-Macaulay-Komplexe und ihre Parametrisierung, *Math. Zeitschrift* **167**, 173–179.

E. Kunz (1985), Introduction to Commutative Algebra and Algebraic Geometry, Birkhäuser, Boston.

W. B. R. Lickorish (1988), Polynomials for links, *Bull. London Math. Society* **20**, 558–588.

M. V. Liebeck (1984), On minimal degrees and base sizes of primitive permutation groups, *Arch. Math.* **43**, 11–15.

L. Lovász and M. D. Plummer (1986), *Matching Theory*, Akadémiai Kiadó - North Holland, Budapest - Amsterdam.

V. Milman (1982), Some remarks about embedding of ℓ_1^k in finite dimensional spaces, *Israel J. Math.* **43**, 129–138.

K. Murasugi (1987), Jones polynomials and classical conjectures in knot theory, *Topology* **26**, 187–194.

K. Onaga and O. Kakusho (1971), On feasibility conditions of multicommodity flows in networks, *IEEE Trans. Circuit Theory* **18**, 425–429.

P. Orlik (1989), *Introduction to Arrangements*, CBMS Regional Conference Series in Math. **72**, Amer. Math. Soc., Providence, RI.

P. Orlik and L. Solomon (1980), Combinatorics and topology of complements of hyperplanes, *Invent. Math.* **56**, 167–189.

P. Orlik and H. Terao (1992), *Arrangements of Hyperplanes,* Grundlehren der math. Wissenschaften, Vol. 300, Springer-Verlag, Berlin Heidelberg.

L. Paris (1991a), Universal cover of Salvetti's complex and topology of simplicial arrangements of hyperplanes, preprint; *Trans. Am. Math. Soc.*, to appear.

L. Paris (1991b), The Deligne complex of a real arrangement of hyperplanes, preprint.

L. Pyber (1990), On the orders of doubly transitive permutation groups: elementary estimates,

L. L. Rose and H. Terao (1990), Hilbert polynomials and geometric lattices, *Advances in Math.* **84**, 209-225.

G.-C. Rota and L. H. Harper (1971), Matching theory, an introduction, in: *Advances in Probability Theory and Related Topics* (ed. P. Ney) Vol. I, Marcel Dekker, New York 1971, 169–215.

K. Saito (1980), Theory of logarithmic differential forms and logarithmic vector fields, *J. Fac. Science, University of Tokyo, Sci. IA* **27**, 265–291.

M. Salvetti (1987), Topology of the complement of real hyperplanes in $\mathbb{C}^N$, *Invent. Math.* **88**, 603–618.

M. Salvetti (1993), On the homotopy theory of the complexes associated to metrical-hemisphere complexes, *Discrete Math.* **113**, 155–177.

I. R. Shafarevich (1977), *Basic Algebraic Geometry*, Springer-Verlag, New York.

L. Solomon and H. Terao (1987), A formula for the characteristic polynomial of an arrangement, *Advances in Math.* **64**, 305–325.

E. H. Spanier (1966), *Algebraic Topology*, McGraw-Hill and Springer-Verlag.

R. P. Stanley (1972), Supersolvable lattices, *Algebra Universalis* **2**, 197–217.

R. P. Stanley (1975), Cohen-Macaulay rings and constructible polytopes, *Bull. Amer. Math. Soc.* **81**, 133–135.

R. P. Stanley (1984), T-free arrangements of hyperplanes, in: *Progress in Graph Theory* (eds. J.A. Bondy and U.S.R. Murty), Academic Press, 539.

R. P. Stanley (1986), *Enumerative Combinatorics, Vol. I*, Wadsworth & Brooks/Cole, Monterey 1986.

B. Sturmfels and N. White (1989), Gröbner bases and invariant theory, *Advances in Math.* **76**, 245–259.

B. Sturmfels and N. White (1991), Computing combinatorial decompositions of rings, *Combinatorica* **11** (1991), 275–293.

P. G. Tait (1898), On knots I, II, III, in: *Scientific Papers* Vol. I, Cambridge University Press, London, 273–347.

H. Terao (1980), Arrangements of hyperplanes and their freeness I, *J. Fac. Science, University of Tokyo, Sci. IA* **27**(2), 293–312.

H. Terao (1981), Generalized exponents of a free arrangement of hyperplanes and Shephard-Todd-Brieskorn formula, *Invent. Math.* **63**, 159–179.

H. Terao (1986), Modular elements of lattices and topological fibration, *Advances in Math.* **62**, 135–154.

M. B. Thistlethwaite (1987), A spanning tree expansion of the Jones polynomial, *Topology* **26**, 297–309.

V. A. Vassiliev (1990), Cohomology of knot spaces, in: *Theory of Singularities and it Applications* (ed. V. I. Arnol'd), *Advances in Soviet Mathematics* **1**, Amer. Math. Soc., 23-69.

H. Wielandt (1964), *Finite permutation groups*, Academic Press, New York.

S. Yuzvinsky (1993), The first two obstructions to the freeness of arrangements, *Trans. Amer. Math. Soc.* **335**, 231-244.

V. N. Zemlyachenko, N. M. Vornienko and R. I. Tyshkevich (1985), Graph isomorphism problems, *J. Soviet Math.* **29**, 1426–1481.

G. M. Ziegler (1989), Combinatorial construction of logarithmic differential forms, *Advances in Math.* **76**, 116–154.

G. M. Ziegler (1990), Matroid representations and free arrangements, *Trans. Amer. Math. Soc.* **320**, 525–541.

G. M. Ziegler (1993), On the difference between real and complex arrangements, *Math. Zeitschrift* **212**, 1–11.

G. M. Ziegler and R. T. Živaljević (1993), Homotopy types of arrangements via diagrams of spaces, *Math. Annalen* **295**, 527–574.