Annals of Mathematics **160** (2008), 17–45
https://doi.org/10.4007/annals.2008.160.1.12

Sample Paper for the aomart Class

By American Mathematical Society and Boris Veytsman

Abstract

This is a test file for `aomart` class based on the `testmath.tex` file from the `amsmath` distribution.

It was changed to test the features of the Annals of Mathematics class.

Contents

Keywords: Hamiltonian paths, Typesetting
AMS Classification: Primary: 1AB5, 2FD5; Secondary: FFFF, G25.
The class was commissioned by Annals of Mathematics.

1. Introduction

This paper demonstrates the use of `aomart` class. It is based on `testmath.tex` from $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX distribution. The text is (slightly) reformatted according to the requirements of the `aomart` style. See also [12, 22, 17, 1, 16, 15, 24, 23, 6].

Are these quotations necessary?

It is always a pleasure to cite Knuth [9].

2. Enumeration of Hamiltonian paths in a graph

Let $\mathbf{A} = (a_{ij})$ be the adjacency matrix of graph G. The corresponding Kirchhoff matrix $\mathbf{K} = (k_{ij})$ is obtained from $\mathbf{A}$ by replacing in $-\mathbf{A}$ each diagonal entry by the degree of its corresponding vertex; i.e., the ith diagonal entry is identified with the degree of the ith vertex. It is well known that

$$\det \mathbf{K}(i|i) = \text{ the number of spanning trees of } G, \quad i = 1, \dots, n \tag{1}$$

where $\mathbf{K}(i|i)$ is the ith principal submatrix of $\mathbf{K}$.

```
\det\mathbf{K}(i|i)=\text{ the number of spanning trees of $G$},
```

Let $C_{i(j)}$ be the set of graphs obtained from G by attaching edge $(v_i v_j)$ to each spanning tree of G. Denote by $C_i = \bigcup_j C_{i(j)}$. It is obvious that the collection of Hamiltonian cycles is a subset of C_i. Note that the cardinality of C_i is $k_{ii} \det \mathbf{K}(i|i)$. Let $\widehat{X} = \{\hat{x}_1, \dots, \hat{x}_n\}$.

```
$\wh X=\{\hat x_1,\dots,\hat x_n\}$
```

Define multiplication for the elements of $\widehat{X}$ by

$$\hat{x}_i \hat{x}_j = \hat{x}_j \hat{x}_i, \quad \hat{x}_i^2 = 0, \quad i, j = 1, \dots, n. \tag{2}$$

Let $\hat{k}_{ij} = k_{ij}\hat{x}_j$ and $\hat{k}_{ij} = -\sum_{j\neq i}\hat{k}_{ij}$. Then the number of Hamiltonian cycles H_c is given by the relation [13]

$$\left(\prod_{j=1}^{n}\hat{x}_j\right)H_c = \frac{1}{2}\hat{k}_{ij}\det\widehat{\mathbf{K}}(i|i), \qquad i = 1,\ldots,n. \tag{3}$$

The task here is to express (3) in a form free of any $\hat{x}_i$, $i = 1,\ldots,n$. The result also leads to the resolution of enumeration of Hamiltonian paths in a graph.

It is well known that the enumeration of Hamiltonian cycles and paths in a complete graph K_n and in a complete bipartite graph $K_{n_1n_2}$ can only be found from *first combinatorial principles* [7]. One wonders if there exists a formula which can be used very efficiently to produce K_n and $K_{n_1n_2}$. Recently, using Lagrangian methods, Goulden and Jackson have shown that H_c can be expressed in terms of the determinant and permanent of the adjacency matrix [5]. However, the formula of Goulden and Jackson determines neither K_n nor $K_{n_1n_2}$ effectively. In this paper, using an algebraic method, we parametrize the adjacency matrix. The resulting formula also involves the determinant and permanent, but it can easily be applied to K_n and $K_{n_1n_2}$. In addition, we eliminate the permanent from H_c and show that H_c can be represented by a determinantal function of multivariables, each variable with domain $\{0,1\}$. Furthermore, we show that H_c can be written by number of spanning trees of subgraphs. Finally, we apply the formulas to a complete multigraph $K_{n_1\ldots n_p}$.

The conditions $a_{ij} = a_{ji}$, $i,j = 1,\ldots,n$, are not required in this paper. All formulas can be extended to a digraph simply by multiplying H_c by 2. Some other discussion can be found in [4, 3].

3. Main theorem

Notation. For $p,q \in P$ and $n \in \omega$ we write $(q,n) \le (p,n)$ if $q \le p$ and $A_{q,n} = A_{p,n}$.

```
\begin{notation} For $p,q\in P$ and $n\in\omega$
...
\end{notation}
```

Let $\mathbf{B} = (b_{ij})$ be an $n\times n$ matrix. Let $\mathbf{n} = \{1,\ldots,n\}$. Using the properties of (2), it is readily seen that

Lemma 3.1.

$$\prod_{i\in\mathbf{n}}\left(\sum_{j\in\mathbf{n}} b_{ij}\hat{x}_i\right) = \left(\prod_{i\in\mathbf{n}}\hat{x}_i\right)\operatorname{per}\mathbf{B} \tag{4}$$

where per $\mathbf{B}$ *is the permanent of* $\mathbf{B}$.

Let $\widehat{Y} = \{\hat{y}_1, \ldots, \hat{y}_n\}$. Define multiplication for the elements of $\widehat{Y}$ by

$$\hat{y}_i\hat{y}_j + \hat{y}_j\hat{y}_i = 0, \quad i, j = 1, \ldots, n. \tag{5}$$

Then, it follows that

LEMMA 3.2.

$$\prod_{i\in\mathbf{n}}\Big(\sum_{j\in\mathbf{n}} b_{ij}\hat{y}_j\Big) = \Big(\prod_{i\in\mathbf{n}} \hat{y}_i\Big)\det\mathbf{B}. \tag{6}$$

Note that all basic properties of determinants are direct consequences of Lemma 3.2. Write

$$\sum_{j\in\mathbf{n}} b_{ij}\hat{y}_j = \sum_{j\in\mathbf{n}} b_{ij}^{(\lambda)}\hat{y}_j + (b_{ii} - \lambda_i)\hat{y}_i\hat{y} \tag{7}$$

where

$$b_{ii}^{(\lambda)} = \lambda_i, \quad b_{ij}^{(\lambda)} = b_{ij}, \quad i \neq j. \tag{8}$$

Let $\mathbf{B}^{(\lambda)} = (b_{ij}^{(\lambda)})$. By (6) and (7), it is straightforward to show the following result:

THEOREM 3.3.

$$\det\mathbf{B} = \sum_{l=0}^{n}\sum_{I_l\subseteq n}\prod_{i\in I_l}(b_{ii} - \lambda_i)\det\mathbf{B}^{(\lambda)}(I_l|I_l), \tag{9}$$

where $I_l = \{i_1, \ldots, i_l\}$ and $\mathbf{B}^{(\lambda)}(I_l|I_l)$ is the principal submatrix (obtained from $\mathbf{B}^{(\lambda)}$ by deleting its $i_1, \ldots, i_l$ rows and columns).

Remark 3.1 (convention). Let $\mathbf{M}$ be an $n \times n$ matrix. The convention $\mathbf{M}(\mathbf{n}|\mathbf{n}) = 1$ has been used in (9) and hereafter.

Before proceeding with our discussion, we pause to note that Theorem 3.3 yields immediately a fundamental formula which can be used to compute the coefficients of a characteristic polynomial [14]:

COROLLARY 3.4. *Write* $\det(\mathbf{B} - x\mathbf{I}) = \sum_{l=0}^{n}(-1)^l b_l x^l$. *Then*

$$b_l = \sum_{I_l\subseteq\mathbf{n}} \det\mathbf{B}(I_l|I_l). \tag{10}$$

Let

$$\mathbf{K}(t, t_1, \ldots, t_n) = \begin{pmatrix} D_1t & -a_{12}t_2 & \ldots & -a_{1n}t_n \\ -a_{21}t_1 & D_2t & \ldots & -a_{2n}t_n \\ \ldots & \ldots & \ldots & \ldots \\ -a_{n1}t_1 & -a_{n2}t_2 & \ldots & D_nt \end{pmatrix}, \tag{11}$$

```
\begin{pmatrix} D_1t&-a_{12}t_2&\dots&-a_{1n}t_n\\
-a_{21}t_1&D_2t&\dots&-a_{2n}t_n\\
\hdotsfor[2]{4}\\
-a_{n1}t_1&-a_{n2}t_2&\dots&D_nt\end{pmatrix}
```

where

$$D_i = \sum_{j\in\mathbf{n}} a_{ij}t_j, \quad i = 1, \dots, n. \tag{12}$$

Set

$$D(t_1, \dots, t_n) = \frac{\delta}{\delta t} \det \mathbf{K}(t, t_1, \dots, t_n)|_{t=1}\,.$$

Then

$$D(t_1, \dots, t_n) = \sum_{i\in\mathbf{n}} D_i \det \mathbf{K}(t = 1, t_1, \dots, t_n; i|i), \tag{13}$$

where $\mathbf{K}(t = 1, t_1, \dots, t_n; i|i)$ is the ith principal submatrix of $\mathbf{K}(t = 1, t_1, \dots, t_n)$.

Theorem 3.3 leads to

$$\det \mathbf{K}(t_1, t_1, \dots, t_n) = \sum_{I\in\mathbf{n}} (-1)^{|I|} t^{n-|I|} \prod_{i\in I} t_i \prod_{j\in I} (D_j + \lambda_j t_j) \det \mathbf{A}^{(\lambda t)}(\overline{I}|\overline{I}). \tag{14}$$

Note that

$$\det \mathbf{K}(t = 1, t_1, \dots, t_n) = \sum_{I\in\mathbf{n}} (-1)^{|I|} \prod_{i\in I} t_i \prod_{j\in I} (D_j + \lambda_j t_j) \det \mathbf{A}^{(\lambda)}(\overline{I}|\overline{I}) = 0. \tag{15}$$

Let $t_i = \hat{x}_i, i = 1, \dots, n$. Lemma 3.1 yields

$$\begin{multline}\biggl(\sum_{i\in\mathbf{n}} a_{l_i} x_i\biggr) \det \mathbf{K}(t = 1, x_1, \dots, x_n; l|l) \\ = \biggl(\prod_{i\in\mathbf{n}} \hat{x}_i\biggr) \sum_{I\subseteq\mathbf{n}-\{l\}} (-1)^{|I|} \operatorname{per} \mathbf{A}^{(\lambda)}(I|I) \det \mathbf{A}^{(\lambda)}(\overline{I} \cup \{l\}|\overline{I} \cup \{l\}). \tag{16}\end{multline}$$

```
\begin{multline}
\biggl(\sum_{\,i\in\mathbf{n}}a_{l _i}x_i\biggr)
\det\mathbf{K}(t=1,x_1,\dots,x_n;l |l )\\
=\biggl(\prod_{\,i\in\mathbf{n}}\hat x_i\biggr)
\sum_{I\subseteq\mathbf{n}-\{l \}}
(-1)^{\envert{I}}\per\mathbf{A}^{(\lambda)}(I|I)
\det\mathbf{A}^{(\lambda)}
(\overline I\cup\{l \}|\overline I\cup\{l \}).
\label{sum-ali}
\end{multline}
```

By (3), (6), and (7), we have

PROPOSITION 3.5.

$$H_c = \frac{1}{2n}\sum_{l=0}^{n}(-1)^l D_l, \tag{17}$$

where

$$D_l = \sum_{I_l\subseteq \mathbf{n}} D(t_1,\dots,t_n)2\big|_{t_i=\left\{\begin{smallmatrix}0, & \text{if } i\in I_l\\ 1, & \text{otherwise}\end{smallmatrix}\right., \ i=1,\dots,n}. \tag{18}$$

4. Application

We consider here the applications of Theorems 5.1 and 5.2 to a complete multipartite graph $K_{n_1\dots n_p}$. It can be shown that the number of spanning trees of $K_{n_1\dots n_p}$ may be written

$$T = n^{p-2}\prod_{i=1}^{p}(n-n_i)^{n_i-1} \tag{19}$$

where

$$n = n_1+\dots+n_p. \tag{20}$$

It follows from Theorems 5.1 and 5.2 that

$$\begin{aligned} H_c = {}&\frac{1}{2n}\sum_{l=0}^{n}(-1)^l(n-l)^{p-2}\sum_{l_1+\dots+l_p=l}\prod_{i=1}^{p}\binom{n_i}{l_i}\\ &\cdot[(n-l)-(n_i-l_i)]^{n_i-l_i}\cdot\left[(n-l)^2-\sum_{j=1}^{p}(n_i-l_i)^2\right]. \end{aligned}\tag{21}$$

```
... \binom{n_i}{l _i}\\
```

and

$$\begin{aligned} H_c = {}&\frac{1}{2}\sum_{l=0}^{n-1}(-1)^l(n-l)^{p-2}\sum_{l_1+\dots+l_p=l}\prod_{i=1}^{p}\binom{n_i}{l_i}\\ &\cdot[(n-l)-(n_i-l_i)]^{n_i-l_i}\left(1-\frac{l_p}{n_p}\right)[(n-l)-(n_p-l_p)]. \end{aligned}\tag{22}$$

The enumeration of H_c in a $K_{n_1\cdots n_p}$ graph can also be carried out by Theorem 7.2 or 7.3 together with the algebraic method of (2). Some elegant representations may be obtained. For example, H_c in a $K_{n_1n_2n_3}$ graph may be written

$$\begin{aligned} H_c = {}&\frac{n_1!\,n_2!\,n_3!}{n_1+n_2+n_3}\sum_i\left[\binom{n_1}{i}\binom{n_2}{n_3-n_1+i}\binom{n_3}{n_3-n_2+i}\right.\\ &\left.+\binom{n_1-1}{i}\binom{n_2-1}{n_3-n_1+i}\binom{n_3-1}{n_3-n_2+i}\right]. \end{aligned}\tag{23}$$

5. **Secret key exchanges**

Modern cryptography is fundamentally concerned with the problem of secure private communication. A Secret Key Exchange is a protocol where Alice and Bob, having no secret information in common to start, are able to agree on a common secret key, conversing over a public channel. The notion of a Secret Key Exchange protocol was first introduced in the seminal paper of Diffie and Hellman [2]. [2] presented a concrete implementation of a Secret Key Exchange protocol, dependent on a specific assumption (a variant on the discrete log), specially tailored to yield Secret Key Exchange. Secret Key Exchange is of course trivial if trapdoor permutations exist. However, there is no known implementation based on a weaker general assumption.

The concept of an informationally one-way function was introduced in [8]. We give only an informal definition here:

Definition 5.1 (one way). A polynomial time computable function $f = \{f_k\}$ is informationally one-way if there is no probabilistic polynomial time algorithm which (with probability of the form $1 - k^{-e}$ for some $e > 0$) returns on input $y \in \{0,1\}^k$ a random element of $f^{-1}(y)$.

In the non-uniform setting [8] show that these are not weaker than one-way functions:

THEOREM 5.1 ([8] (non-uniform)). *The existence of informationally one-way functions implies the existence of one-way functions.*

We will stick to the convention introduced above of saying "non-uniform" before the theorem statement when the theorem makes use of non-uniformity. It should be understood that if nothing is said then the result holds for both the uniform and the non-uniform models.

It now follows from Theorem 5.1 that

THEOREM 5.2 (non-uniform). *Weak SKE implies the existence of a one-way function.*

More recently, the polynomial-time, interior point algorithms for linear programming have been extended to the case of convex quadratic programs [19, 21], certain linear complementarity problems [11, 18], and the nonlinear complementarity problem [10]. The connection between these algorithms and the classical Newton method for nonlinear equations is well explained in [11].

6. **Review**

We begin our discussion with the following definition:

Definition 6.1. A function $H\colon \Re^n \to \Re^n$ is said to be *B-differentiable* at the point z if (i) H is Lipschitz continuous in a neighborhood of z, and (ii) there exists a positive homogeneous function $BH(z)\colon \Re^n \to \Re^n$, called the *B-derivative* of H at z, such that

$$\lim_{v\to 0} \frac{H(z+v)-H(z)-BH(z)v}{\|v\|} = 0.$$

The function H is *B-differentiable in set S* if it is B-differentiable at every point in S. The B-derivative $BH(z)$ is said to be *strong* if

$$\lim_{(v,v')\to(0,0)} \frac{H(z+v)-H(z+v')-BH(z)(v-v')}{\|v-v'\|} = 0.$$

LEMMA 6.1. *There exists a smooth function $\psi_0(z)$ defined for $|z|>1-2a$ satisfying the following properties*:

(i) *$\psi_0(z)$ is bounded above and below by positive constants $c_1 \le \psi_0(z) \le c_2$.*
(ii) *If $|z|>1$, then $\psi_0(z)=1$.*
(iii) *For all z in the domain of ψ_0, $\Delta_0 \ln\psi_0 \ge 0$.*
(iv) *If $1-2a<|z|<1-a$, then $\Delta_0\ln\psi_0 \ge c_3 > 0$.*

Proof. We choose $\psi_0(z)$ to be a radial function depending only on $r=|z|$. Let $h(r)\ge 0$ be a suitable smooth function satisfying $h(r)\ge c_3$ for $1-2a<|z|<1-a$, and $h(r)=0$ for $|z|>1-\frac{a}{2}$. The radial Laplacian

$$\Delta_0 \ln\psi_0(r) = \left(\frac{d^2}{dr^2}+\frac{1}{r}\frac{d}{dr}\right)\ln\psi_0(r)$$

has smooth coefficients for $r>1-2a$. Therefore, we may apply the existence and uniqueness theory for ordinary differential equations. Simply let $\ln\psi_0(r)$ be the solution of the differential equation

$$\left(\frac{d^2}{dr^2}+\frac{1}{r}\frac{d}{dr}\right)\ln\psi_0(r) = h(r)$$

with initial conditions given by $\ln\psi_0(1)=0$ and $\ln\psi_0'(1)=0$.

Next, let D_ν be a finite collection of pairwise disjoint disks, all of which are contained in the unit disk centered at the origin in C. We assume that $D_\nu=\{z \mid |z-z_\nu|<\delta\}$. Suppose that $D_\nu(a)$ denotes the smaller concentric disk $D_\nu(a)=\{z \mid |z-z_\nu|\le(1-2a)\delta\}$. We define a smooth weight function $\Phi_0(z)$ for $z\in C-\bigcup_\nu D_\nu(a)$ by setting $\Phi_0(z)=1$ when $z\notin\bigcup_\nu D_\nu$ and $\Phi_0(z)=\psi_0((z-z_\nu)/\delta)$ when z is an element of D_ν. It follows from Lemma 6.1 that Φ_0 satisfies the properties:

(i) $\Phi_0(z)$ is bounded above and below by positive constants $c_1\le\Phi_0(z)\le c_2$.
(ii) $\Delta_0\ln\Phi_0\ge 0$ for all $z\in C-\bigcup_\nu D_\nu(a)$, the domain where the function Φ_0 is defined.

(iii) $\Delta_0 \ln \Phi_0 \geq c_3\delta^{-2}$ when $(1-2a)\delta < |z - z_\nu| < (1-a)\delta$.

Let A_ν denote the annulus $A_\nu = \{(1-2a)\delta < |z - z_\nu| < (1-a)\delta\}$, and set $A = \bigcup_\nu A_\nu$. The properties (2) and (3) of Φ_0 may be summarized as $\Delta_0 \ln \Phi_0 \geq c_3\delta^{-2}\chi_A$, where χ_A is the characteristic function of A. □

Suppose that α is a nonnegative real constant. We apply Proposition 3.5 with $\Phi(z) = \Phi_0(z)e^{\alpha|z|^2}$. If $u \in C_0^\infty(R^2 - \bigcup_\nu D_\nu(a))$, assume that $\mathcal{D}$ is a bounded domain containing the support of u and $A \subset \mathcal{D} \subset R^2 - \bigcup_\nu D_\nu(a)$. A calculation gives

$$\int_{\mathcal{D}} \left|\overline{\partial} u\right|^2 \Phi_0(z)e^{\alpha|z|^2} \geq c_4\alpha \int_{\mathcal{D}} |u|^2 \Phi_0 e^{\alpha|z|^2} + c_5\delta^{-2} \int_A |u|^2 \Phi_0 e^{\alpha|z|^2}.$$

The boundedness, property (1) of Φ_0, then yields

$$\int_{\mathcal{D}} \left|\overline{\partial} u\right|^2 e^{\alpha|z|^2} \geq c_6\alpha \int_{\mathcal{D}} |u|^2 e^{\alpha|z|^2} + c_7\delta^{-2} \int_A |u|^2 e^{\alpha|z|^2}.$$

Let $B(X)$ be the set of blocks of Λ_X and let $b(X) = |B(X)|$. If $\phi \in Q_X$ then ϕ is constant on the blocks of Λ_X.

$$P_X = \{\phi \in M \mid \Lambda_\phi = \Lambda_X\}, \qquad Q_X = \{\phi \in M \mid \Lambda_\phi \geq \Lambda_X\}. \tag{24}$$

If $\Lambda_\phi \geq \Lambda_X$ then $\Lambda_\phi = \Lambda_Y$ for some $Y \geq X$ so that

$$Q_X = \bigcup_{Y \geq X} P_Y.$$

Thus by Möbius inversion

$$|P_Y| = \sum_{X \geq Y} \mu(Y, X) \, |Q_X| \, .$$

Thus there is a bijection from Q_X to $W^{B(X)}$. In particular $|Q_X| = w^{b(X)}$.

Next note that $b(X) = \dim X$. We see this by choosing a basis for X consisting of vectors v^k defined by

$$v_i^k = \begin{cases} 1 & \text{if } i \in \Lambda_k, \\ 0 & \text{otherwise.} \end{cases}$$

```
\[v^{k}_{i}=
\begin{cases} 1 & \text{if $i \in \Lambda_{k}$},\\
0 &\text{otherwise.} \end{cases}
\]
```

Lemma 6.2. *Let $\mathcal{A}$ be an arrangement. Then*

$$\chi(\mathcal{A}, t) = \sum_{\mathcal{B} \subseteq \mathcal{A}} (-1)^{|\mathcal{B}|} t^{\dim T(\mathcal{B})}.$$

In order to compute R'' recall the definition of $S(X,Y)$ from Lemma 3.1. Since $H \in \mathcal{B}$, $\mathcal{A}_H \subseteq \mathcal{B}$. Thus if $T(\mathcal{B}) = Y$ then $\mathcal{B} \in S(H,Y)$. Let $L'' = L(\mathcal{A}'')$. Then

$$\begin{aligned} R'' &= \sum_{H\in\mathcal{B}\subseteq\mathcal{A}} (-1)^{|\mathcal{B}|} t^{\dim T(\mathcal{B})} \\ &= \sum_{Y\in L''} \sum_{\mathcal{B}\in S(H,Y)} (-1)^{|\mathcal{B}|} t^{\dim Y} \\ &= -\sum_{Y\in L''} \sum_{\mathcal{B}\in S(H,Y)} (-1)^{|\mathcal{B}-\mathcal{A}_H|} t^{\dim Y} \\ &= -\sum_{Y\in L''} \mu(H,Y) t^{\dim Y} \\ &= -\chi(\mathcal{A}'',t). \end{aligned} \tag{25}$$

Corollary 6.3. *Let $(\mathcal{A},\mathcal{A}',\mathcal{A}'')$ be a triple of arrangements. Then*

$$\pi(\mathcal{A},t) = \pi(\mathcal{A}',t) + t\pi(\mathcal{A}'',t).$$

Definition 6.2. Let $(\mathcal{A},\mathcal{A}',\mathcal{A}'')$ be a triple with respect to the hyperplane $H \in \mathcal{A}$. Call H a *separator* if $T(\mathcal{A}) \notin L(\mathcal{A}')$.

Corollary 6.4. *Let $(\mathcal{A},\mathcal{A}',\mathcal{A}'')$ be a triple with respect to $H \in \mathcal{A}$.*

(i) *If H is a separator then*

$$\mu(\mathcal{A}) = -\mu(\mathcal{A}'')$$

and hence

$$|\mu(\mathcal{A})| = |\mu(\mathcal{A}'')|.$$

(ii) *If H is not a separator then*

$$\mu(\mathcal{A}) = \mu(\mathcal{A}') - \mu(\mathcal{A}'')$$

and

$$|\mu(\mathcal{A})| = |\mu(\mathcal{A}')| + |\mu(\mathcal{A}'')|.$$

Proof. It follows from Theorem 5.1 that $\pi(\mathcal{A},t)$ has leading term

$$(-1)^{r(\mathcal{A})}\mu(\mathcal{A})t^{r(\mathcal{A})}.$$

The conclusion follows by comparing coefficients of the leading terms on both sides of the equation in Corollary 6.3. If H is a separator then $r(\mathcal{A}') < r(\mathcal{A})$ and there is no contribution from $\pi(\mathcal{A}',t)$. $\square$

The Poincaré polynomial of an arrangement will appear repeatedly in these notes. It will be shown to equal the Poincaré polynomial of the graded algebras which we are going to associate with $\mathcal{A}$. It is also the Poincaré polynomial of the complement $M(\mathcal{A})$ for a complex arrangement. Here we prove

Figure 1. $Q(\mathcal{A}_1) = xyz(x-z)(x+z)(y-z)(y+z)$

Figure 2. $Q(\mathcal{A}_2) = xyz(x+y+z)(x+y-z)(x-y+z)(x-y-z)$

that the Poincaré polynomial is the chamber counting function for a real arrangement. The complement $M(\mathcal{A})$ is a disjoint union of chambers

$$M(\mathcal{A}) = \bigcup_{C \in \mathrm{Cham}(\mathcal{A})} C.$$

The number of chambers is determined by the Poincaré polynomial as follows.

THEOREM 6.5. *Let $\mathcal{A}_{\mathbf{R}}$ be a real arrangement. Then*

$$|\mathrm{Cham}(\mathcal{A}_{\mathbf{R}})| = \pi(\mathcal{A}_{\mathbf{R}}, 1).$$

Proof. We check the properties required in Corollary 6.4: (i) follows from $\pi(\Phi_l, t) = 1$, and (ii) is a consequence of Corollary 3.4. □

THEOREM 6.6. *Let ϕ be a protocol for a random pair (X, Y). If one of $\sigma_\phi(x', y)$ and $\sigma_\phi(x, y')$ is a prefix of the other and $(x, y) \in S_{X,Y}$, then*

$$\langle \sigma_j(x', y) \rangle_{j=1}^{\infty} = \langle \sigma_j(x, y) \rangle_{j=1}^{\infty} = \langle \sigma_j(x, y') \rangle_{j=1}^{\infty}.$$

Proof. We show by induction on i that

$$\langle \sigma_j(x', y)\rangle_{j=1}^{i} = \langle \sigma_j(x, y)\rangle_{j=1}^{i} = \langle \sigma_j(x, y')\rangle_{j=1}^{i}.$$

The induction hypothesis holds vacuously for $i = 0$. Assume it holds for $i - 1$, in particular $[\sigma_j(x', y)]_{j=1}^{i-1} = [\sigma_j(x, y')]_{j=1}^{i-1}$. Then one of $[\sigma_j(x', y)]_{j=i}^{\infty}$ and $[\sigma_j(x, y')]_{j=i}^{\infty}$ is a prefix of the other which implies that one of $\sigma_i(x', y)$ and $\sigma_i(x, y')$ is a prefix of the other. If the ith message is transmitted by $P_{\mathcal{X}}$ then, by the separate-transmissions property and the induction hypothesis, $\sigma_i(x, y) = \sigma_i(x, y')$, hence one of $\sigma_i(x, y)$ and $\sigma_i(x', y)$ is a prefix of the other. By the implicit-termination property, neither $\sigma_i(x, y)$ nor $\sigma_i(x', y)$ can be a proper prefix of the other, hence they must be the same and $\sigma_i(x', y) = \sigma_i(x, y) = \sigma_i(x, y')$. If the ith message is transmitted by $P_{\mathcal{Y}}$ then, symmetrically, $\sigma_i(x, y) = \sigma_i(x', y)$ by the induction hypothesis and the separate-transmissions property, and, then, $\sigma_i(x, y) = \sigma_i(x, y')$ by the implicit-termination property, proving the induction step. □

If ϕ is a protocol for (X, Y), and (x, y), (x', y) are distinct inputs in $S_{X,Y}$, then, by the correct-decision property, $\langle \sigma_j(x, y)\rangle_{j=1}^{\infty} \neq \langle \sigma_j(x', y)\rangle_{j=1}^{\infty}$.

Equation (25) defined $P_{\mathcal{Y}}$'s ambiguity set $S_{X|Y}(y)$ to be the set of possible X values when $Y = y$. The last corollary implies that for all $y \in S_Y$, the multiset[1] of codewords $\{\sigma_\phi(x, y) : x \in S_{X|Y}(y)\}$ is prefix free.

7. One-way complexity

$\hat{C}_1(X|Y)$, the one-way complexity of a random pair (X, Y), is the number of bits $P_{\mathcal{X}}$ must transmit in the worst case when $P_{\mathcal{Y}}$ is not permitted to transmit any feedback messages. Starting with $S_{X,Y}$, the support set of (X, Y), we define $G(X|Y)$, the *characteristic hypergraph* of (X, Y), and show that

$$\hat{C}_1(X|Y) = \lceil \log \chi(G(X|Y)) \rceil .$$

Let (X, Y) be a random pair. For each y in S_Y, the support set of Y, equation (25) defined $S_{X|Y}(y)$ to be the set of possible x values when $Y = y$. The *characteristic hypergraph* $G(X|Y)$ of (X, Y) has S_X as its vertex set and the hyperedge $S_{X|Y}(y)$ for each $y \in S_Y$.

We can now prove a continuity theorem.

THEOREM 7.1. *Let $\Omega \subset \mathbf{R}^n$ be an open set, let $u \in BV(\Omega; \mathbf{R}^m)$, and let*

$$T_x^u = \left\{ y \in \mathbf{R}^m : y = \tilde{u}(x) + \left\langle \frac{Du}{|Du|}(x), z \right\rangle \text{ for some } z \in \mathbf{R}^n \right\} \tag{26}$$

[1]A multiset allows multiplicity of elements. Hence, $\{0, 01, 01\}$ is prefix free as a set, but not as a multiset.

for every $x \in \Omega \backslash S_u$. Let $f\colon \mathbf{R}^m \to \mathbf{R}^k$ be a Lipschitz continuous function such that $f(0) = 0$, and let $v = f(u)\colon \Omega \to \mathbf{R}^k$. Then $v \in BV(\Omega; \mathbf{R}^k)$ and

$$Jv = (f(u^+) - f(u^-)) \otimes \nu_u \cdot \mathcal{H}_{n-1}\Big|_{S_u}. \tag{27}$$

In addition, for $\left|\widetilde{D}u\right|$-almost every $x \in \Omega$ the restriction of the function f to T^u_x is differentiable at $\tilde{u}(x)$ and

$$\widetilde{D}v = \nabla (f|_{T^u_x})(\tilde{u}) \frac{\widetilde{D}u}{\left|\widetilde{D}u\right|} \cdot \left|\widetilde{D}u\right|. \tag{28}$$

Before proving the theorem, we state without proof three elementary remarks which will be useful in the sequel.

Remark 7.1. Let $\omega\colon\ ]0, +\infty[\ \to\ ]0, +\infty[$ be a continuous function such that $\omega(t) \to 0$ as $t \to 0$. Then

$$\lim_{h \to 0^+} g(\omega(h)) = L \Leftrightarrow \lim_{h \to 0^+} g(h) = L$$

for any function $g\colon\ ]0, +\infty[\ \to \mathbf{R}$.

Remark 7.2. Let $g\colon \mathbf{R}^n \to \mathbf{R}$ be a Lipschitz continuous function and assume that

$$L(z) = \lim_{h \to 0^+} \frac{g(hz) - g(0)}{h}$$

exists for every $z \in \mathbf{Q}^n$ and that L is a linear function of z. Then g is differentiable at 0.

Remark 7.3. Let $A\colon \mathbf{R}^n \to \mathbf{R}^m$ be a linear function, and let $f\colon \mathbf{R}^m \to \mathbf{R}$ be a function. Then the restriction of f to the range of A is differentiable at 0 if and only if $f(A)\colon \mathbf{R}^n \to \mathbf{R}$ is differentiable at 0 and

$$\nabla (f|_{\mathrm{Im}(A)})(0)A = \nabla (f(A))(0).$$

Proof. We begin by showing that $v \in BV(\Omega; \mathbf{R}^k)$ and

$$|Dv|(B) \le K\,|Du|(B) \qquad \forall B \in \mathbf{B}(\Omega), \tag{29}$$

where $K > 0$ is the Lipschitz constant of f. By (13) and by the approximation result quoted in §3, it is possible to find a sequence $(u_h) \subset C^1(\Omega; \mathbf{R}^m)$ converging to u in $L^1(\Omega; \mathbf{R}^m)$ and such that

$$\lim_{h \to +\infty} \int_\Omega |\nabla u_h|\, dx = |Du|(\Omega).$$

The functions $v_h = f(u_h)$ are locally Lipschitz continuous in Ω, and the definition of differential implies that $|\nabla v_h| \le K\,|\nabla u_h|$ almost everywhere in Ω. The lower semicontinuity of the total variation and (13) yield

$$
\begin{aligned}
|Dv|(\Omega) &\le \liminf_{h\to+\infty} |Dv_h|(\Omega) = \liminf_{h\to+\infty} \int_\Omega |\nabla v_h| \, dx \\
&\le K \liminf_{h\to+\infty} \int_\Omega |\nabla u_h| \, dx = K\,|Du|(\Omega).
\end{aligned} \tag{30}
$$

Since $f(0)=0$, we have also

$$
\int_\Omega |v| \, dx \le K \int_\Omega |u| \, dx;
$$

therefore $u \in BV(\Omega;\mathbf{R}^k)$. Repeating the same argument for every open set $A \subset \Omega$, we get (29) for every $B \in \mathbf{B}(\Omega)$, because $|Dv|$, $|Du|$ are Radon measures. To prove Lemma 6.1, first we observe that

$$
S_v \subset S_u, \qquad \tilde{v}(x) = f(\tilde{u}(x)) \qquad \forall x \in \Omega \backslash S_u. \tag{31}
$$

In fact, for every $\varepsilon > 0$ we have

$$
\{y \in B_\rho(x) : |v(y) - f(\tilde{u}(x))| > \varepsilon\} \subset \{y \in B_\rho(x) : |u(y) - \tilde{u}(x)| > \varepsilon/K\},
$$

hence

$$
\lim_{\rho\to 0^+} \frac{|\{y \in B_\rho(x) : |v(y) - f(\tilde{u}(x))| > \varepsilon\}|}{\rho^n} = 0
$$

whenever $x \in \Omega\backslash S_u$. By a similar argument, if $x \in S_u$ is a point such that there exists a triplet (u^+, u^-, ν_u) satisfying (14), (15), then

$$
(v^+(x) - v^-(x)) \otimes \nu_v = (f(u^+(x)) - f(u^-(x))) \otimes \nu_u \quad \text{if } x \in S_v
$$

and $f(u^-(x)) = f(u^+(x))$ if $x \in S_u\backslash S_v$. Hence, by (1.8) we get

$$
\begin{aligned}
Jv(B) = \int_{B\cap S_v} (v^+ - v^-) \otimes \nu_v \, d\mathcal{H}_{n-1} &= \int_{B\cap S_v} (f(u^+) - f(u^-)) \otimes \nu_u \, d\mathcal{H}_{n-1} \\
&= \int_{B\cap S_u} (f(u^+) - f(u^-)) \otimes \nu_u \, d\mathcal{H}_{n-1}
\end{aligned}
$$

and Lemma 6.1 is proved. □

To prove (31), it is not restrictive to assume that $k=1$. Moreover, to simplify our notation, from now on we shall assume that $\Omega = \mathbf{R}^n$. The proof of (31) is divided into two steps. In the first step we prove the statement in the one-dimensional case ($n=1$), using Theorem 5.2. In the second step we achieve the general result using Theorem 7.1.

Step 1. Assume that $n=1$. Since S_u is at most countable, (7) yields that $\left|\widetilde{D}v\right|(S_u\backslash S_v) = 0$, so that (19) and (21) imply that $Dv = \widetilde{D}v + Jv$ is the

Radon-Nikodým decomposition of Dv in absolutely continuous and singular part with respect to $\left|\widetilde{D}u\right|$. By Theorem 5.2, we have

$$\frac{\widetilde{D}v}{\left|\widetilde{D}u\right|}(t) = \lim_{s\to t^+} \frac{Dv([t,s[)}{\left|\widetilde{D}u\right|([t,s[)}, \qquad \frac{\widetilde{D}u}{\left|\widetilde{D}u\right|}(t) = \lim_{s\to t^+} \frac{Du([t,s[)}{\left|\widetilde{D}u\right|([t,s[)}$$

$\left|\widetilde{D}u\right|$-almost everywhere in $\mathbf{R}$. It is well known (see, for instance, [20, 2.5.16]) that every one-dimensional function of bounded variation w has a unique left continuous representative, i.e., a function $\hat{w}$ such that $\hat{w} = w$ almost everywhere and $\lim_{s\to t^-} \hat{w}(s) = \hat{w}(t)$ for every $t \in \mathbf{R}$. These conditions imply

$$\hat{u}(t) = Du(]-\infty, t[), \qquad \hat{v}(t) = Dv(]-\infty, t[) \qquad \forall t \in \mathbf{R} \tag{32}$$

and

$$\hat{v}(t) = f(\hat{u}(t)) \qquad \forall t \in \mathbf{R}. \tag{33}$$

Let $t \in \mathbf{R}$ be such that $\left|\widetilde{D}u\right|([t,s[) > 0$ for every $s > t$ and assume that the limits in (22) exist. By (23) and (24) we get

$$\begin{aligned}
\frac{\hat{v}(s) - \hat{v}(t)}{\left|\widetilde{D}u\right|([t,s[)} &= \frac{f(\hat{u}(s)) - f(\hat{u}(t))}{\left|\widetilde{D}u\right|([t,s[)} \\
&= \frac{f(\hat{u}(s)) - f(\hat{u}(t) + \frac{\widetilde{D}u}{\left|\widetilde{D}u\right|}(t)\left|\widetilde{D}u\right|([t,s[))}{\left|\widetilde{D}u\right|([t,s[)} \\
&\quad + \frac{f(\hat{u}(t) + \frac{\widetilde{D}u}{\left|\widetilde{D}u\right|}(t)\left|\widetilde{D}u\right|([t,s[)) - f(\hat{u}(t))}{\left|\widetilde{D}u\right|([t,s[)}
\end{aligned}$$

for every $s > t$. Using the Lipschitz condition on f we find

$$\left|\frac{\hat{v}(s) - \hat{v}(t)}{\left|\widetilde{D}u\right|([t,s[)} - \frac{f(\hat{u}(t) + \frac{\widetilde{D}u}{\left|\widetilde{D}u\right|}(t)\left|\widetilde{D}u\right|([t,s[)) - f(\hat{u}(t))}{\left|\widetilde{D}u\right|([t,s[)}\right| \\
\le K \left|\frac{\hat{u}(s) - \hat{u}(t)}{\left|\widetilde{D}u\right|([t,s[)} - \frac{\widetilde{D}u}{\left|\widetilde{D}u\right|}(t)\right|.$$

By (29), the function $s \to \left|\widetilde{D}u\right|([t,s[)$ is continuous and converges to 0 as $s \downarrow t$. Therefore Remark 7.1 and the previous inequality imply

$$\frac{\widetilde{D}v}{\left|\widetilde{D}u\right|}(t) = \lim_{h\to 0^+} \frac{f(\hat{u}(t) + h\dfrac{\widetilde{D}u}{\left|\widetilde{D}u\right|}(t)) - f(\hat{u}(t))}{h} \qquad \left|\widetilde{D}u\right|\text{-a.e. in } \mathbf{R}.$$

By (22), $\hat{u}(x) = \tilde{u}(x)$ for every $x \in \mathbf{R}\backslash S_u$; moreover, applying the same argument to the functions $u'(t) = u(-t)$, $v'(t) = f(u'(t)) = v(-t)$, we get

$$\frac{\widetilde{D}v}{\left|\widetilde{D}u\right|}(t) = \lim_{h\to 0} \frac{f(\tilde{u}(t) + h\dfrac{\widetilde{D}u}{\left|\widetilde{D}u\right|}(t)) - f(\tilde{u}(t))}{h} \qquad \left|\widetilde{D}u\right|\text{-a.e. in } \mathbf{R}$$

and our statement is proved.

Step 2. Let us consider now the general case $n > 1$. Let $\nu \in \mathbf{R}^n$ be such that $|\nu| = 1$, and let $\pi_\nu = \{y \in \mathbf{R}^n : \langle y, \nu\rangle = 0\}$. In the following, we shall identify $\mathbf{R}^n$ with $\pi_\nu \times \mathbf{R}$, and we shall denote by y the variable ranging in π_ν and by t the variable ranging in $\mathbf{R}$. By the just proven one-dimensional result, and by Theorem 3.3, we get

$$\lim_{h\to 0} \frac{f(\tilde{u}(y+t\nu) + h\dfrac{\widetilde{D}u_y}{\left|\widetilde{D}u_y\right|}(t)) - f(\tilde{u}(y+t\nu))}{h} = \frac{\widetilde{D}v_y}{\left|\widetilde{D}u_y\right|}(t) \qquad \left|\widetilde{D}u_y\right|\text{-a.e. in } \mathbf{R}$$

for $\mathcal{H}_{n-1}$-almost every $y \in \pi_\nu$. We claim that

$$\frac{\langle\widetilde{D}u, \nu\rangle}{\left|\langle\widetilde{D}u, \nu\rangle\right|}(y+t\nu) = \frac{\widetilde{D}u_y}{\left|\widetilde{D}u_y\right|}(t) \qquad \left|\widetilde{D}u_y\right|\text{-a.e. in } \mathbf{R} \tag{34}$$

for $\mathcal{H}_{n-1}$-almost every $y \in \pi_\nu$. In fact, by (16) and (18) we get

$$\int_{\pi_\nu} \frac{\widetilde{D}u_y}{\left|\widetilde{D}u_y\right|} \cdot \left|\widetilde{D}u_y\right| \, d\mathcal{H}_{n-1}(y) = \int_{\pi_\nu} \widetilde{D}u_y \, d\mathcal{H}_{n-1}(y)$$

$$= \langle\widetilde{D}u, \nu\rangle = \frac{\langle\widetilde{D}u, \nu\rangle}{\left|\langle\widetilde{D}u, \nu\rangle\right|} \cdot \left|\langle\widetilde{D}u, \nu\rangle\right| = \int_{\pi_\nu} \frac{\langle\widetilde{D}u, \nu\rangle}{\left|\langle\widetilde{D}u, \nu\rangle\right|}(y + \cdot\nu) \cdot \left|\widetilde{D}u_y\right| \, d\mathcal{H}_{n-1}(y)$$

and (24) follows from (13). By the same argument it is possible to prove that

$$\frac{\langle\widetilde{D}v, \nu\rangle}{\left|\langle\widetilde{D}u, \nu\rangle\right|}(y+t\nu) = \frac{\widetilde{D}v_y}{\left|\widetilde{D}u_y\right|}(t) \qquad \left|\widetilde{D}u_y\right|\text{-a.e. in } \mathbf{R} \tag{35}$$

for $\mathcal{H}_{n-1}$-almost every $y \in \pi_\nu$. By (24) and (25) we get

$$\lim_{h\to 0} \frac{f\left(\tilde u(y+t\nu) + h\dfrac{\langle \widetilde{D}u,\nu\rangle}{\left|\langle \widetilde{D}u,\nu\rangle\right|}(y+t\nu)\right) - f(\tilde u(y+t\nu))}{h} = \frac{\langle \widetilde{D}v,\nu\rangle}{\left|\langle \widetilde{D}u,\nu\rangle\right|}(y+t\nu)$$

for $\mathcal{H}_{n-1}$-almost every $y \in \pi_\nu$, and using again (14), (15) we get

$$\lim_{h\to 0} \frac{f\left(\tilde u(x) + h\dfrac{\langle \widetilde{D}u,\nu\rangle}{\left|\langle \widetilde{D}u,\nu\rangle\right|}(x)\right) - f(\tilde u(x))}{h} = \frac{\langle \widetilde{D}v,\nu\rangle}{\left|\langle \widetilde{D}u,\nu\rangle\right|}(x)$$

$\left|\langle \widetilde{D}u,\nu\rangle\right|$-a.e. in $\mathbf{R}^n$.

Since the function $\left|\langle \widetilde{D}u,\nu\rangle\right| / \left|\widetilde{D}u\right|$ is strictly positive $\left|\langle \widetilde{D}u,\nu\rangle\right|$-almost everywhere, we obtain also

$$\lim_{h\to 0} \frac{f\left(\tilde u(x) + h\dfrac{\left|\langle \widetilde{D}u,\nu\rangle\right|}{\left|\widetilde{D}u\right|}(x)\dfrac{\langle \widetilde{D}u,\nu\rangle}{\left|\langle \widetilde{D}u,\nu\rangle\right|}(x)\right) - f(\tilde u(x))}{h} = \frac{\left|\langle \widetilde{D}u,\nu\rangle\right|}{\left|\widetilde{D}u\right|}(x)\frac{\langle \widetilde{D}v,\nu\rangle}{\left|\langle \widetilde{D}u,\nu\rangle\right|}(x)$$

$\left|\langle \widetilde{D}u,\nu\rangle\right|$-almost everywhere in $\mathbf{R}^n$.

Finally, since

$$\frac{\left|\langle \widetilde{D}u,\nu\rangle\right|}{\left|\widetilde{D}u\right|}\frac{\langle \widetilde{D}u,\nu\rangle}{\left|\langle \widetilde{D}u,\nu\rangle\right|} = \frac{\langle \widetilde{D}u,\nu\rangle}{\left|\widetilde{D}u\right|} = \left\langle \frac{\widetilde{D}u}{\left|\widetilde{D}u\right|},\nu\right\rangle \qquad \left|\widetilde{D}u\right|\text{-a.e. in } \mathbf{R}^n$$

$$\frac{\left|\langle \widetilde{D}u,\nu\rangle\right|}{\left|\widetilde{D}u\right|}\frac{\langle \widetilde{D}v,\nu\rangle}{\left|\langle \widetilde{D}u,\nu\rangle\right|} = \frac{\langle \widetilde{D}v,\nu\rangle}{\left|\widetilde{D}u\right|} = \left\langle \frac{\widetilde{D}v}{\left|\widetilde{D}u\right|},\nu\right\rangle \qquad \left|\widetilde{D}u\right|\text{-a.e. in } \mathbf{R}^n$$

and since both sides of (33) are zero $\left|\widetilde{D}u\right|$-almost everywhere on $\left|\langle \widetilde{D}u,\nu\rangle\right|$-negligible sets, we conclude that

$$\lim_{h\to 0} \frac{f\left(\tilde u(x) + h\left\langle \dfrac{\widetilde{D}u}{\left|\widetilde{D}u\right|}(x),\nu\right\rangle\right) - f(\tilde u(x))}{h} = \left\langle \frac{\widetilde{D}v}{\left|\widetilde{D}u\right|}(x),\nu\right\rangle,$$

$\left|\widetilde{D}u\right|$-a.e. in $\mathbf{R}^n$. Since ν is arbitrary, by Remarks 7.2 and 7.3 the restriction of f to the affine space T^u_x is differentiable at $\tilde u(x)$ for $\left|\widetilde{D}u\right|$-almost every $x \in \mathbf{R}^n$ and (26) holds. □

It follows from (13), (14), and (15) that

$$D(t_1,\ldots,t_n) = \sum_{I\in\mathbf{n}}(-1)^{|I|-1}\,|I|\prod_{i\in I}t_i\prod_{j\in I}(D_j+\lambda_j t_j)\det\mathbf{A}^{(\lambda)}(\bar{I}|\bar{I}). \tag{36}$$

Let $t_i=\hat{x}_i$, $i=1,\ldots,n$. Lemma 1 leads to

$$D(\hat{x}_1,\ldots,\hat{x}_n) = \prod_{i\in\mathbf{n}}\hat{x}_i\sum_{I\in\mathbf{n}}(-1)^{|I|-1}\,|I|\,\mathrm{per}\,\mathbf{A}^{(\lambda)}(I|I)\det\mathbf{A}^{(\lambda)}(\bar{I}|\bar{I}). \tag{37}$$

By (3), (13), and (37), we have the following result:

THEOREM 7.2.

$$H_c = \frac{1}{2n}\sum_{l=1}^{n} l(-1)^{l-1}A_l^{(\lambda)}, \tag{38}$$

where

$$A_l^{(\lambda)} = \sum_{I_l\subseteq\mathbf{n}}\mathrm{per}\,\mathbf{A}^{(\lambda)}(I_l|I_l)\det\mathbf{A}^{(\lambda)}(\bar{I}_l|\bar{I}_l), |I_l|=l. \tag{39}$$

It is worth noting that $A_l^{(\lambda)}$ of (39) is similar to the coefficients b_l of the characteristic polynomial of (10). It is well known in graph theory that the coefficients b_l can be expressed as a sum over certain subgraphs. It is interesting to see whether A_l, $\lambda=0$, structural properties of a graph.

We may call (38) a parametric representation of H_c. In computation, the parameter λ_i plays very important roles. The choice of the parameter usually depends on the properties of the given graph. For a complete graph K_n, let $\lambda_i=1$, $i=1,\ldots,n$. It follows from (39) that

$$A_l^{(1)} = \begin{cases} n!, & \text{if } l=1\\ 0, & \text{otherwise.}\end{cases} \tag{40}$$

By (38)

$$H_c = \frac{1}{2}(n-1)!. \tag{41}$$

For a complete bipartite graph $K_{n_1n_2}$, let $\lambda_i=0$, $i=1,\ldots,n$. By (39),

$$A_l = \begin{cases} -n_1!n_2!\delta_{n_1n_2}, & \text{if } l=2\\ 0, & \text{otherwise .}\end{cases} \tag{42}$$

Theorem 7.2 leads to

$$H_c = \frac{1}{n_1+n_2}n_1!n_2!\delta_{n_1n_2}. \tag{43}$$

Now, we consider an asymmetrical approach. Theorem 3.3 leads to

$$\begin{aligned} \det \mathbf{K}(t=1, t_1, \dots, t_n; l|l) \\ = \sum_{I \subseteq \mathbf{n} - \{l\}} (-1)^{|I|} \prod_{i \in I} t_i \prod_{j \in I} (D_j + \lambda_j t_j) \det \mathbf{A}^{(\lambda)}(\overline{I} \cup \{l\} | \overline{I} \cup \{l\}). \end{aligned} \tag{44}$$

By (3) and (16) we have the following asymmetrical result:

THEOREM 7.3.

$$H_c = \frac{1}{2} \sum_{I \subseteq \mathbf{n} - \{l\}} (-1)^{|I|} \operatorname{per} \mathbf{A}^{(\lambda)}(I|I) \det \mathbf{A}^{(\lambda)}(\overline{I} \cup \{l\} | \overline{I} \cup \{l\}) \tag{45}$$

which reduces to Goulden–Jackson's formula when $\lambda_i = 0, i = 1, \dots, n$ [14].

8. Various font features of the `amsmath` package

8.1. *Bold versions of special symbols.* In the `amsmath` package `\boldsymbol` is used for getting individual bold math symbols and bold Greek letters—everything in math except for letters of the Latin alphabet, where you'd use `\mathbf`. For example,

```
A_\infty + \pi A_0 \sim
\mathbf{A}_{\boldsymbol{\infty}} \boldsymbol{+}
\boldsymbol{\pi} \mathbf{A}_{\boldsymbol{0}}
```

looks like this:

$$A_\infty + \pi A_0 \sim \mathbf{A}_{\boldsymbol{\infty}} \boldsymbol{+} \boldsymbol{\pi} \mathbf{A}_{\boldsymbol{0}}$$

8.2. *"Poor man's bold".* If a bold version of a particular symbol doesn't exist in the available fonts, then `\boldsymbol` can't be used to make that symbol bold. At the present time, this means that `\boldsymbol` can't be used with symbols from the `msam` and `msbm` fonts, among others. In some cases, poor man's bold (`\pmb`) can be used instead of `\boldsymbol`:

$$\frac{\partial x}{\partial y} \pmb{\bigg\vert} \frac{\partial y}{\partial z}$$

```
\[\frac{\partial x}{\partial y}
\pmb{\bigg\vert}
\frac{\partial y}{\partial z}\]
```

So-called "large operator" symbols such as $\sum$ and $\prod$ require an additional command, `\mathop`, to produce proper spacing and limits when `\pmb` is used. For further details see *The TEXbook*.

$$\sum_{\substack{i<B \\ i \text{ odd}}} \prod_\kappa \kappa F(r_i) \qquad \sum_{\substack{i<B \\ i \text{ odd}}} \prod_\kappa \kappa(r_i)$$

```
\[\sum_{\substack{i<B\\\text{$i$ odd}}}
\prod_\kappa \kappa F(r_i)\qquad
\mathop{\pmb{\sum}}_{\substack{i<B\\\text{$i$ odd}}}
\mathop{\pmb{\prod}}_\kappa \kappa(r_i)
\]
```

9. Compound symbols and other features

9.1. *Multiple integral signs.* `\iint`, `\iiint`, and `\iiiint` give multiple integral signs with the spacing between them nicely adjusted, in both text and display style. `\idotsint` gives two integral signs with dots between them.

$$\iint\limits_A f(x,y)\,dx\,dy \qquad \iiint\limits_A f(x,y,z)\,dx\,dy\,dz \tag{46}$$

$$\iiiint\limits_A f(w,x,y,z)\,dw\,dx\,dy\,dz \qquad \idotsint\limits_A f(x_1,\dots,x_k) \tag{47}$$

9.2. *Over and under arrows.* Some extra over and under arrow operations are provided in the `amsmath` package. (Basic LaTeX provides `\overrightarrow` and `\overleftarrow`).

$$\begin{aligned}
\overrightarrow{\psi_\delta(t) E_t h}&=\underrightarrow{\psi_\delta(t) E_t h}\\
\overleftarrow{\psi_\delta(t) E_t h}&=\underleftarrow{\psi_\delta(t) E_t h}\\
\overleftrightarrow{\psi_\delta(t) E_t h}&=\underleftrightarrow{\psi_\delta(t) E_t h}
\end{aligned}$$

```
\begin{align*}
\overrightarrow{\psi_\delta(t) E_t h}&
=\underrightarrow{\psi_\delta(t) E_t h}\\
\overleftarrow{\psi_\delta(t) E_t h}&
=\underleftarrow{\psi_\delta(t) E_t h}\\
\overleftrightarrow{\psi_\delta(t) E_t h}&
=\underleftrightarrow{\psi_\delta(t) E_t h}
\end{align*}
```

These all scale properly in subscript sizes:

$$\int_{\overrightarrow{AB}} ax\,dx$$

```
\[\int_{\overrightarrow{AB}} ax\,dx\]
```

9.3. *Dots.* Normally you need only type `\dots` for ellipsis dots in a math formula. The main exception is when the dots fall at the end of the formula; then you need to specify one of `\dotsc` (series dots, after a comma), `\dotsb` (binary dots, for binary relations or operators), `\dotsm` (multiplication dots), or `\dotsi` (dots after an integral). For example, the input

```
Then we have the series $A_1,A_2,\dotsc$,
the regional sum $A_1+A_2+\dotsb$,
the orthogonal product $A_1A_2\dotsm$,
and the infinite integral
\[\int_{A_1}\int_{A_2}\dotsi\].
```

produces

> Then we have the series $A_1, A_2, \dotsc$, the regional sum $A_1 + A_2 + \dotsb$, the orthogonal product $A_1A_2\dotsm$, and the infinite integral
> $$\int_{A_1}\int_{A_2}\dotsi$$

9.4. *Accents in math.* Double accents:

$$\hat{\hat{H}}\quad\check{\check{C}}\quad\tilde{\tilde{T}}\quad\acute{\acute{A}}\quad\grave{\grave{G}}\quad\dot{\dot{D}}\quad\ddot{\ddot{D}}\quad\breve{\breve{B}}\quad\bar{\bar{B}}\quad\vec{\vec{V}}$$

```
\[\Hat{\Hat{H}}\quad\Check{\Check{C}}\quad
\Tilde{\Tilde{T}}\quad\Acute{\Acute{A}}\quad
\Grave{\Grave{G}}\quad\Dot{\Dot{D}}\quad
\Ddot{\Ddot{D}}\quad\Breve{\Breve{B}}\quad
\Bar{\Bar{B}}\quad\Vec{\Vec{V}}\]
```

This double accent operation is complicated and tends to slow down the processing of a LaTeX file.

9.5. *Dot accents.* `\dddot` and `\ddddot` are available to produce triple and quadruple dot accents in addition to the `\dot` and `\ddot` accents already available in LaTeX:

$$\dddot{Q}\qquad\ddddot{R}$$

```
\[\dddot{Q}\qquad\ddddot{R}\]
```

9.6. *Roots.* In the `amsmath` package `\leftroot` and `\uproot` allow you to adjust the position of the root index of a radical:

```
\sqrt[\leftroot{-2}\uproot{2}\beta]{k}
```

gives good positioning of the β:

$$\sqrt[\leftroot{-2}\uproot{2}\beta]{k}$$

9.7. *Boxed formulas.* The command `\boxed` puts a box around its argument, like `\fbox` except that the contents are in math mode:

```
\boxed{W_t-F\subseteq V(P_i)\subseteq W_t}
```

$$\boxed{W_t-F\subseteq V(P_i)\subseteq W_t}.$$

9.8. *Extensible arrows.* `\xleftarrow` and `\xrightarrow` produce arrows that extend automatically to accommodate unusually wide subscripts or superscripts. The text of the subscript or superscript are given as an optional resp. mandatory argument: Example:

$$0 \xleftarrow[\zeta]{\alpha} F\times\triangle[n-1] \xrightarrow{\partial_0\alpha(b)} E^{\partial_0b}$$

```
\[0 \xleftarrow[\zeta]{\alpha} F\times\triangle[n-1]
  \xrightarrow{\partial_0\alpha(b)} E^{\partial_0b}\]
```

9.9. `\overset`, `\underset`, *and* `\sideset`. Examples:

$$\overset{*}{X}\qquad\underset{*}{X}\qquad\overset{a}{\underset{b}{X}}$$

```
\[\overset{*}{X}\qquad\underset{*}{X}\qquad
\overset{a}{\underset{b}{X}}\]
```

The command `\sideset` is for a rather special purpose: putting symbols at the subscript and superscript corners of a large operator symbol such as $\sum$ or $\prod$, without affecting the placement of limits. Examples:

$$\sideset{_*^*}{_*^*}\prod_k\qquad \sideset{}{'}\sum_{0\le i\le m} E_i\beta x$$

```
\[\sideset{_*^*}{_*^*}\prod_k\qquad
\sideset{}{'}\sum_{0\le i\le m} E_i\beta x
\]
```

9.10. *The* `\text` *command.* The main use of the command `\text` is for words or phrases in a display:

$$\mathbf{y}=\mathbf{y}'\quad\text{if and only if}\quad y'_k=\delta_k y_{\tau(k)}$$

```
\[\mathbf{y}=\mathbf{y}'\quad\text{if and only if}\quad
y'_k=\delta_k y_{\tau(k)}\]
```

9.11. *Operator names.* The more common math functions such as log, sin, and lim have predefined control sequences: `\log`, `\sin`, `\lim`. The `amsmath` package provides `\DeclareMathOperator` and `\DeclareMathOperator*` for producing new function names that will have the same typographical treatment. Examples:

$$\|f\|_\infty=\operatorname{ess\,sup}_{x\in R^n}|f(x)|$$

```
\[\norm{f}_\infty=
\esssup_{x\in R^n}\abs{f(x)}\]
```

$$\operatorname{meas}_1\{u\in R_+^1\colon f^*(u)>\alpha\}=\operatorname{meas}_n\{x\in R^n\colon |f(x)|\geq\alpha\}\quad\forall\alpha>0.$$

```
\[\meas_1\{u\in R_+^1\colon f^*(u)>\alpha\}
=\meas_n\{x\in R^n\colon \abs{f(x)}\geq\alpha\}
\quad \forall\alpha>0.\]
```

`\esssup` and `\meas` would be defined in the document preamble as

```
\DeclareMathOperator*{\esssup}{ess\,sup}
\DeclareMathOperator{\meas}{meas}
```

The following special operator names are predefined in the `amsmath` package: `\varlimsup`, `\varliminf`, `\varinjlim`, and `\varprojlim`. Here's what they look like in use:

$$\varlimsup_{n\rightarrow\infty} \mathcal{Q}(u_n,u_n-u^{\#})\le 0 \tag{48}$$

$$\varliminf_{n\rightarrow\infty} \left\lvert a_{n+1}\right\rvert/\left\lvert a_n\right\rvert=0 \tag{49}$$

$$\varinjlim (m_i^\lambda\cdot)^*\le 0 \tag{50}$$

$$\varprojlim_{p\in S(A)} A_p\le 0 \tag{51}$$

```
\begin{align}
&\varlimsup_{n\rightarrow\infty}
       \mathcal{Q}(u_n,u_n-u^{\#})\le0\\
&\varliminf_{n\rightarrow\infty}
  \left\lvert a_{n+1}\right\rvert/\left\lvert a_n\right\rvert=0\\
&\varinjlim (m_i^\lambda\cdot)^*\le0\\
&\varprojlim_{p\in S(A)}A_p\le0
\end{align}
```

9.12. `\mod` *and its relatives.* The commands `\mod` and `\pod` are variants of `\pmod` preferred by some authors; `\mod` omits the parentheses, whereas `\pod` omits the 'mod' and retains the parentheses. Examples:

$$x\equiv y+1\pmod{m^2} \tag{52}$$

$$x\equiv y+1\mod{m^2} \tag{53}$$

$$x\equiv y+1\pod{m^2} \tag{54}$$

```
\begin{align}
x&\equiv y+1\pmod{m^2}\\
x&\equiv y+1\mod{m^2}\\
x&\equiv y+1\pod{m^2}
\end{align}
```

9.13. *Fractions and related constructions.* The usual notation for binomials is similar to the fraction concept, so it has a similar command `\binom` with two arguments. Example:

$$\begin{split}\sum_{\gamma\in\Gamma_C} I_\gamma&=2^k-\binom{k}{1}2^{k-1}+\binom{k}{2}2^{k-2}\\&\quad+\dots+(-1)^l\binom{k}{l}2^{k-l}+\dots+(-1)^k\\&=(2-1)^k=1\end{split}\tag{55}$$

```
\begin{equation}
\begin{split}
[\sum_{\gamma\in\Gamma_C} I_\gamma&
=2^k-\binom{k}{1}2^{k-1}+\binom{k}{2}2^{k-2}\\
&\quad+\dots+(-1)^l\binom{k}{l}2^{k-l}
+\dots+(-1)^k\\
&=(2-1)^k=1
\end{split}
\end{equation}
```

There are also abbreviations

```
\dfrac        \dbinom
\tfrac        \tbinom
```

for the commonly needed constructions

```
{\displaystyle\frac ... }   {\displaystyle\binom ... }
{\textstyle\frac ... }      {\textstyle\binom ... }
```

The generalized fraction command `\genfrac` provides full access to the six TEX fraction primitives:

$$\text{\over: }\frac{n+1}{2} \qquad \text{\overwithdelims: }\genfrac{\langle}{\rangle}{}{}{n+1}{2}\tag{56}$$

$$\text{\atop: }\genfrac{}{}{0pt}{}{n+1}{2} \qquad \text{\atopwithdelims: }\genfrac{(}{)}{0pt}{}{n+1}{2}\tag{57}$$

$$\text{\above: }\genfrac{}{}{1pt}{}{n+1}{2} \qquad \text{\abovewithdelims: }\genfrac{[}{]}{1pt}{}{n+1}{2}\tag{58}$$

```
\text{\cn{over}: }&\genfrac{}{}{}{}{n+1}{2}&
\text{\cn{overwithdelims}: }&
  \genfrac{\langle}{\rangle}{}{}{n+1}{2}\\
\text{\cn{atop}: }&\genfrac{}{}{0pt}{}{n+1}{2}&
\text{\cn{atopwithdelims}: }&
  \genfrac{(}{)}{0pt}{}{n+1}{2}\\
\text{\cn{above}: }&\genfrac{}{}{1pt}{}{n+1}{2}&
\text{\cn{abovewithdelims}: }&
  \genfrac{[}{]}{1pt}{}{n+1}{2}
```

9.14. *Continued fractions.* The continued fraction

$$\frac{1}{\sqrt{2}+\frac{1}{\sqrt{2}+\frac{1}{\sqrt{2}+\frac{1}{\sqrt{2}+\frac{1}{\sqrt{2}+\cdots}}}}} \tag{59}$$

can be obtained by typing

```
\cfrac{1}{\sqrt{2}+
 \cfrac{1}{\sqrt{2}+
  \cfrac{1}{\sqrt{2}+
   \cfrac{1}{\sqrt{2}+
    \cfrac{1}{\sqrt{2}+\dotsb
}}}}}
```

Left or right placement of any of the numerators is accomplished by using `\cfrac[l]` or `\cfrac[r]` instead of `\cfrac`.

9.15. *Smash.* In `amsmath` there are optional arguments `t` and `b` for the plain TEX command `\smash`, because sometimes it is advantageous to be able to 'smash' only the top or only the bottom of something while retaining the natural depth or height. In the formula $X_j=(1/\sqrt{\smash[b]{\lambda_j}})X_j'$ `\smash[b]` has been used to limit the size of the radical symbol.

```
$X_j=(1/\sqrt{\smash[b]{\lambda_j}})X_j'$
```

Without the use of `\smash[b]` the formula would have appeared thus: $X_j=(1/\sqrt{\lambda_j})X_j'$, with the radical extending to encompass the depth of the subscript j.

9.16. *The 'cases' environment.* 'Cases' constructions like the following can be produced using the `cases` environment.

$$P_{r-j}=\begin{cases} 0& \text{if $r-j$ is odd},\\ r!\,(-1)^{(r-j)/2}& \text{if $r-j$ is even}. \end{cases} \tag{60}$$

```
\begin{equation} P_{r-j}=
  \begin{cases}
    0&  \text{if $r-j$ is odd},\\
    r!\,(-1)^{(r-j)/2}&  \text{if $r-j$ is even}.
  \end{cases}
\end{equation}
```

Notice the use of `\text` and the embedded math.

9.17. *Matrix*. Here are samples of the matrix environments, `\matrix`, `\pmatrix`, `\bmatrix`, `\Bmatrix`, `\vmatrix` and `\Vmatrix`:

$$\begin{matrix} \vartheta & \varrho\\ \varphi & \varpi \end{matrix}\quad \begin{pmatrix} \vartheta & \varrho\\ \varphi & \varpi \end{pmatrix}\quad \begin{bmatrix} \vartheta & \varrho\\ \varphi & \varpi \end{bmatrix}\quad \begin{Bmatrix} \vartheta & \varrho\\ \varphi & \varpi \end{Bmatrix}\quad \begin{vmatrix} \vartheta & \varrho\\ \varphi & \varpi \end{vmatrix}\quad \begin{Vmatrix} \vartheta & \varrho\\ \varphi & \varpi \end{Vmatrix} \tag{61}$$

```
\begin{matrix}
\vartheta& \varrho\\\varphi& \varpi
\end{matrix}\quad
\begin{pmatrix}
\vartheta& \varrho\\\varphi& \varpi
\end{pmatrix}\quad
\begin{bmatrix}
\vartheta& \varrho\\\varphi& \varpi
\end{bmatrix}\quad
\begin{Bmatrix}
\vartheta& \varrho\\\varphi& \varpi
\end{Bmatrix}\quad
\begin{vmatrix}
\vartheta& \varrho\\\varphi& \varpi
\end{vmatrix}\quad
\begin{Vmatrix}
\vartheta& \varrho\\\varphi& \varpi
\end{Vmatrix}
```

To produce a small matrix suitable for use in text, use the `smallmatrix` environment.

```
\begin{math}
  \bigl( \begin{smallmatrix}
      a&b\\ c&d
    \end{smallmatrix} \bigr)
\end{math}
```

To show the effect of the matrix on the surrounding lines of a paragraph, we put it here: $\bigl(\begin{smallmatrix} a&b\\ c&d \end{smallmatrix} \bigr)$ and follow it with enough text to ensure that there will be at least one full line below the matrix.

`\hdotsfor{`*number*`}` produces a row of dots in a matrix spanning the given number of columns:

$$W(\Phi)= \begin{Vmatrix}
\dfrac\varphi{(\varphi_1,\varepsilon_1)}&0&\dots&0\\
\dfrac{\varphi k_{n2}}{(\varphi_2,\varepsilon_1)}&
\dfrac\varphi{(\varphi_2,\varepsilon_2)}&\dots&0\\
\hdotsfor{5}\\
\dfrac{\varphi k_{n1}}{(\varphi_n,\varepsilon_1)}&
\dfrac{\varphi k_{n2}}{(\varphi_n,\varepsilon_2)}&\dots&
\dfrac{\varphi k_{n\,n-1}}{(\varphi_n,\varepsilon_{n-1})}&
\dfrac{\varphi}{(\varphi_n,\varepsilon_n)}
\end{Vmatrix}$$

```
\[W(\Phi)= \begin{Vmatrix}
\dfrac\varphi{(\varphi_1,\varepsilon_1)}&0&\dots&0\\
\dfrac{\varphi k_{n2}}{(\varphi_2,\varepsilon_1)}&
\dfrac\varphi{(\varphi_2,\varepsilon_2)}&\dots&0\\
\hdotsfor{5}\\
\dfrac{\varphi k_{n1}}{(\varphi_n,\varepsilon_1)}&
\dfrac{\varphi k_{n2}}{(\varphi_n,\varepsilon_2)}&\dots&
\dfrac{\varphi k_{n\,n-1}}{(\varphi_n,\varepsilon_{n-1})}&
\dfrac{\varphi}{(\varphi_n,\varepsilon_n)}
\end{Vmatrix}\]
```

The spacing of the dots can be varied through use of a square-bracket option, for example, `\hdotsfor[1.5]{3}`. The number in square brackets will be used as a multiplier; the normal value is 1.

9.18. *The* `\substack` *command.* The `\substack` command can be used to produce a multiline subscript or superscript: for example

```
\sum_{\substack{0\le i\le m\\ 0<j<n}} P(i,j)
```

produces a two-line subscript underneath the sum:

$$\sum_{\substack{0\le i\le m\\ 0<j<n}} P(i,j) \tag{62}$$

A slightly more generalized form is the `subarray` environment which allows you to specify that each line should be left-aligned instead of centered, as here: Maybe "… as below"?

$$\sum_{\begin{subarray}{l} 0\le i\le m\\ 0<j<n \end{subarray}} P(i,j) \tag{63}$$

```
\sum_{\begin{subarray}{l}
        0\le i\le m\\ 0<j<n
      \end{subarray}}
 P(i,j)
```

9.19. *Big-g-g delimiters.* Here are some big delimiters, first in `\normalsize`:

$$\biggl(\mathbf{E}_{y}\int_0^{t_\varepsilon}L_{x,y^x(s)}\varphi(x)\,ds\biggr)$$

```
\[\biggl(\mathbf{E}_{y}
  \int_0^{t_\varepsilon}L_{x,y^x(s)}\varphi(x)\,ds
  \biggr)
\]
```

and now in `\Large` size:

$$\biggl(\mathbf{E}_{y}\int_0^{t_\varepsilon}L_{x,y^x(s)}\varphi(x)\,ds\biggr)$$

```
{\Large
\[\biggl(\mathbf{E}_{y}
  \int_0^{t_\varepsilon}L_{x,y^x(s)}\varphi(x)\,ds
  \biggr)
\]}
```

References

[1] V. I. Arnold, *Mathematical Methods of Classical Mechanics*, second ed., *Graduate Texts in Mathematics* **60**, Springer, New York, 1989.

[2] W. Diffie and E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory* **22** no. 5 (1976), 644–654.

[3] D. H. Fremlin, Cichon's diagram, presented at the Séminaire Initiation à l'Analyse, G. Choquet, M. Rogalski, J. Saint Raymond, at the Université Pierre et Marie Curie, Paris, 23e année., 1983/194.

[4] D. H. Fremlin, *Topological Riesz Spaces and Measure Theory*, Cambridge University Press, 2008.

[5] I. P. Goulden and D. M. Jackson, The enumeration of directed closed Euler trails and directed Hamiltonian circuits by Langrangian methods, *European Journal of Combinatorics* **2** (1981), 131–212.

[6] C. de Groot, D. Würtz, M. Hanf, R. Peikert, T. Koller, and K. H. Hoffmann, Stochastic optimization—efficient algorithms to solve complex problems, in *System Modelling and Optimization*, *Proceedings of the Fifteenth IFIP Conference* (Zürich) (P. Kall, ed.), Springer-Verlag, 1992, pp. 546–555.

[7] F. Harary and E. M. Palmer, *Graphical Enumeration*, Academic Press, 1973.

[8] R. Impagliazzo, L. Levin, and M. Luby, Pseudo-random generation from one-way functions, in *Proc. 21st STOC* (Seattle, WA, USA), ACM, New York, 1989, pp. 12–24.

[9] D. E. Knuth, *The TEXbook*, with illustrations by Duane Bibby, *Computers & Typesetting A*, Addison-Wesley Publishing Company, Reading, MA, 1994.

[10] M. Kojima, S. Mizuno, and A. Yoshise, *A New Continuation Method for Complementarity Problems With Uniform p-Functions*, Tech. Report B-194, Tokyo Inst. of Technology, Dept. of Information Sciences, Tokyo, 1987.

[11] M. Kojima, S. Mizuno, and A. Yoshise, *A Polynomial-Time Algorithm For a Class of Linear Complementarity Problems*, Tech. Report B-193, Tokyo Inst. of Technology, Dept. of Information Sciences, Tokyo, 1987.

[12] H. W. Lenstra, Jr. and F. Oort, Simple abelian varieties having a prescribed formal isogeny type., *J. Pure Appl. Algebra* **4** (1974), 47–53. MR 0279.14009. Zbl 50:7163. https://doi.org/10.1016/0022-4049(74)90029-2.

[13] C. J. Liu and Y. Chow, On operator and formal sum methods for graph enumeration problems, *SIAM Journal of Algorithms and Discrete Methods* **5** (1984), 384–438.

[14] M. Marcus and H. Minc, A survey of matrix theory and matrix inequalities, *Complementary Series in Mathematics* **14** (1964), 21–48.

[15] A. D. Michal, Differential calculus in linear topological spaces, *Proc. nat. Acad. Sci. USA* **24** (1938), 340–342. JFM 64.0366.02.

[16] A. D. Michal, *Matrix and Tensor Calculus*, *GALCIT Aeronautical Series*, John Wiley & Sons, Inc.; Chapman & Hall, Ltd., New York; London, 1948.

[17] A. Minasyan and D. Osin, *Normal Automorphisms of Relatively Hyperbolic Groups*, 2008. arXiv 0809.2408.

[18] S. Mizuno, A. Yoshise, and T. Kikuchi, *Practical Polynomial Time Algorithms for Linear Complementarity Problems*, Tech. Report 13, Tokyo Inst. of Technology, Dept. of Industrial Engineering and Management, Tokyo, April 1988.

[19] R. D. Monteiro and I. Adler, *Interior Path Following Primal-Dual Algorithms*, *Part II*: *Quadratic Programming*, Working paper, Dept. of Industrial Engineering and Operations Research, August 1987.

[20] E. M. Stein, *Singular Integrals and Differentiability Properties of Functions*, Princeton Univ. Press, Princeton, NJ, 1970.

[21] Y. Ye, *Interior Algorithms for Linear*, *Quadratic and Linearly Constrained Convex Programming*, Ph.D. thesis, Stanford Univ., Dept. of Engineering–Economic Systems, Palo Alto, CA, July 1987.

[22] Yu. G. Zarhin, Abelian varieties having a reduction of K3 type, *Duke Math J.* **65** no. 3 (1992), 17 pp. MR 1154181. Zbl 0774.14039.

[23] Yu. G. Zarhin, *Algebra and Cryptography*, Private Communication.

[24] Yu. G. Zarhin, *On Abel Groups*, Private Communication.

(Received: December 24, 2004)
(Revised: April 12, 2006)

AMS, Providence, Rhode Island
E-mail: tech-support@ams.org

George Mason University, Fairfax, Virginia
E-mail: borisv@lk.net
http://borisv.lk.net