On the Complexity of Combinatorial Counting

A series of lectures by
J.A. Makowsky

Advanced Topics in CS, 236 605
Technion, IIT, Haifa
Spring Semester 2001

Lecture 1

- The determinant
- The permanent
- The hamiltonian
- Turing complexity: the class $\sharp\mathbf{P}$
- Generating functions of graph properties
- Graph polynomials

Textbooks

[Pa94] C. Papadimitriou,
Computational Complexity,
Addison-Wesley, 1994
Especially chapter 18

[Bü00] P. Bürgisser, *Completeness and Reduction in Algebraic Complexity Theory*,
Algorithms and Computation in
Mathematics, vol. 7,
Springer, 2000
Especially chapters 1-5

[Bo99] B. Bollobas,
Modern Graph Theory,
Graduate Texts in Mathematics, Springer
1999.

The Determinant, I

Given an $(n \times n)$- matrix $M = (m_{i,j})$
over a field $\mathfrak{k}$ or (or a ring R)
the *determinant* of M,

$$det(M) = \sum_{\pi \in S_n} (-1)^{sign(\pi)} \prod_{i=1}^{n} m_{i,\pi(i)}$$

is a function from $\mathfrak{k}^{n \times n}$ to $\mathfrak{k}$ in n^2 variables.

Here $sign(\pi)$ is the *parity* of the permutation π, i.e. the number m modulo 2 of transpositions τ_i needed to write $\pi = \prod_{i \leq m} \tau_i$.

Exercise:
Show that, given $\pi = (p_1, \ldots, p_n)$ $sign(\pi)$ is well defined and computable in time $O(n)$.

How do we compute $det(M)$?

The Determinant, II

Computing

$$det(M) = \sum_{\pi \in S_n} (-1)^{sign(\pi)} \prod_{i=1}^{n} m_{i,\pi(i)}$$

- There are $n!$ many permutations.
- For $sign(\pi)$ we need $O(n)$ many steps.
- $\prod_{i=1}^{n} m_{i,\pi(i)}$ needs n multiplications.

Alltogether, this gives $(n!)O(n^2)$ many steps in unit cost.

The Determinant, III

Theorem:(Linear Algebra)
Given an $(n \times n)$- matrix $M = (m_{i,j})$ over a ring $\mathfrak{R}$, $det(M)$ can be computed in $O(n^3)$ steps in unit cost in $\mathfrak{R}$.

This is surprising !

Proof uses:

- $det(M)$ is invariant under interchanges of rows or columns.
- $det(M)$ is invariant under replacing a row (column) vector by a linear combination of the other row (column) vectors.
- Can bring M into *triangular form* T_M.
- $det(T_M)$ is computed as the product of the diagonal.

The Permanent, I

Given an $(m \times n)$- matrix $M = (m_{i,j})$ over a field $\mathfrak{k}$ (or a ring $\mathfrak{R}$) of characteristic $\neq 2$ the *permanent* of M,

$$Per(M) = \sum_{\sigma} \prod_{i=1}^{n} m_{i,\pi(i)}$$

is a function from $\mathfrak{k}^{m \times n}$ to $\mathfrak{k}$ in $m \cdot n$ variables and $\sigma : \{1, \ldots, m\} \to \{1, \ldots, n\}$ is a $1-1$ function.

For $m = n$ we have

$$Per(M) =_{def} per(M) = \sum_{\pi \in S_n} \prod_{i=1}^{n} m_{i,\pi(i)}$$

which looks like the determinant, but simpler.

The Permanent, II

$Per(M)$ was first introduced in 1812 by

- J.P.M. Binet
- A.L. Cauchy

Their interest was in *alternating symmetric functions* which includes the determinant.

The Permanent, III

How do we compute $per(M)$?

Question: Can we find matrices E_n with entries $e_{i,j} \in \{-1, 1\}$ such that for all $(n \times n)$ matrices A

$$per(A) = det(E_n \circ A)$$

where $A \circ B$ is the matrix C with $c_{i,j} = a_{i,j} b_{i,j}$.

Answer (Polya 1913) NO

Proof:

- It suffices to show it for $n = 3$? (Why)
- Count the -1's in diagonals of even and of odd permutations.

The Permanent, IV

Theorem (Marcus and Minc, 1961)
There is no $(n \times n)$ matrix M such that for all $(n \times n)$ matrices A

$$per(A) = det(M \cdot A)$$

Question:
Can we "blow up" an $(n \times n)$ matrix A to a $(n' \times n')$ matrix matrix A' such that $per(A) = det(A')$?

Answer: (J. von zur Gathen, 1987) YES
but n' is exponentially bigger than n.

Improved by R. Meshulam 1987

The permanent of $(0,1)$-matrices

Let $G = \langle V, E \rangle$ be a graph and M_G be its (symmetric) adjacency matrix.

Theorem: The number of perfect matchings of G is given by

$$\sum_{E' \subseteq E} \prod_{(i,j) \in E'} 1 = per(M_G)$$

where E' ranges over all perfect matchings of G.

This interpretation of the permanent is due to P. Hall (1935), based on ideas by D. König, (1931).

I. Kaplanski (1941), P. Halmos and H. Vaughan (1950), H. Mann and H.J. Ryser (1953) use the permanent in combinatorics.

The Permanent, V

No efficient algorithm is known for computing the permanent.

Linear algebra does not seem to help.

$per(M)$ is hard to compute.

It is $\sharp\mathbf{P}$-hard in the Turing model of computation.

In Valiant's model of algebraic computation $per(M) \in \mathbf{VNP}_{\mathfrak{k}}$ and it is complete for $\mathbf{VNP}_{\mathfrak{k}}$ via projections.

What is its complexity in the Blum-Shub Smale model?

Counting Problems

Let $M(\bar{x}, \bar{y})$ be a non-deterministic polynomial time Turing machine which takes $\bar{y}$ as input and $\bar{x} \in \{0, 1\}^{\ell(\bar{y})}$ as guess.

We define a function f_M by

$$f_M(\bar{y}) = \mid \{\bar{x} : M(\bar{x}, \bar{y}) = 1\} \mid$$

f_M has values in $\mathbb{N}$.

The class of such functions f_M for non-deterministic polynomial time Turing machines M is denoted by $\sharp\mathbf{P}$.

With f_M we associate the decision problem

$$\bar{y} \in B_M \text{ iff } f_M(\bar{y}) \neq 0$$

This shows that $\mathbf{NP} \subseteq \mathbf{P}^{\sharp\mathbf{P}}$, and hence,
if $\mathbf{P} = \mathbf{P}^{\sharp\mathbf{P}}$, then $\mathbf{NP} = \mathbf{P}$.

The Hamiltonian

Given an $(n \times n)$- matrix $M = (m_{i,j})$ over a field $\mathfrak{k}$, the *hamiltonian* of M is defined by

$$ham(M) = \sum_{\pi \in C_n} \prod_{i=1}^{n} m_{i,\pi(i)}$$

Here C_n is the set of cyclic permutations of n elements.

Note the similarity to the determinant and permanent !

On $(0,1)$ matrices (graphs) $ham(M)$ counts the number of hamiltonian paths.

***

What is the complexity of $ham(M)$

$\sharp\mathbf{P}$-hard problems

We denote the class of discrete functions computable in polynomial time by a deterministic Turing machine by $\mathbf{FP}$.

For a function f (class of functions C) we denote by

$$\mathbf{FP}^f, \text{ resp. } \mathbf{FP}^C$$

the class of functions computable by a deterministic polynomial time Oracle Turing Machine (OTM) which uses f (C) as oracle.

g is **polynomial time Turing reducible to** f if $g \in \mathbf{FP}^f$. We denote this by $g \leq_{Turing} f$,

f is $\sharp\mathbf{P}$**-hard** if $\sharp\mathbf{P} \subseteq \mathbf{FP}^f$.

Examples in $\sharp\mathbf{P}$

$\sharp$-**SAT:** For a set of clauses Σ, the number of satisfying assignments.

$\sharp$-**p.matchings:** For undirected graphs G, the number of perfect matchings.

$\sharp$-**hamiltonian:** For undirected graphs G, the number of hamiltonian cycles (paths).

$\sharp$-**reliability:** For a graph G and a subgraph H and a node $v \notin H$ the number of paths from v to some node in H.

Parsimonious reductions

SAT is the set of satisfiable formulas Σ in CNF (sets of clauses). An instance of SAT is given by Σ together with a satisfying assignment z.

HAM is the set of graphs with a hamiltonian cycle. An instance of HAM is given by $G = \langle V, E \rangle$ together with a hamiltonian cycle $E_0 \subseteq E$.

A **parsimonious reductions** is a polynomial time computable one-one map α between instances of a problem, say SAT, into instances of another problem, say HAM, such that for two instances Σ, z_1 and Σ, z_2 we have
$\alpha(\Sigma, z_1) = (G, E_{0,1})$ and $\alpha(\Sigma, z_2) = (G, E_{0,2})$.

Theorem:(Cook) SAT is $\mathbf{NP}$-complete for parsimonious reductions.

$\sharp\mathbf{P}$-complete problems

Theorem: If $Prob$ is an $\mathbf{NP}$-complete problem with respect to parsimonious reductions, then $\sharp Prob$ is $\sharp\mathbf{P}$-complete.

Corollary: $\sharp SAT$ and $\sharp HAM$ are $\sharp\mathbf{P}$-complete.

$\sharp$-p.matchings and $\sharp$-reliability are not settled by the above theorem, because perfect matchings and connecting paths can be found in polynomial time resp, even in logarithmic space.

Nevertheless, we have

Theorem:(Valiant)
$\sharp$-p.matchings and $\sharp$-reliability are $\sharp\mathbf{P}$-complete.

Complexity of the permanent

Recall:
Let $G = \langle V, E \rangle$ be a graph and M_G be its (symmetric) adjacency matrix.

Theorem: The number of perfect matchings of G is given by

$$\sum_{E' \subseteq E} \prod_{(i,j) \in E'} 1 = per(M_G)$$

where E' ranges over all perfect matchings of G.

Corollary: Computing the permanent of $(0,1)$-matrices is $\sharp\mathbf{P}$-complete.

Complexity of the hamiltonian

Proposition: For $(0,1)$-matrices M the hamiltonian $ham(M)$ is in $\sharp\mathbf{P}$.

Proof: It counts the number of hamiltonian cycles,

Proposition: For $(0,1)$-matrices M the hamiltonian $ham(M)$ is $\sharp\mathbf{P}$-complete.

Proof: HAM is $\mathbf{NP}$-complete for parsimonious reductions.

$$***$$

What about integer-valued matrices ?

What about matrices over $\{0,1,-1\}$?

Counting Spanning Trees

Theorem:(Kirchhoff, 1847) Counting the number of spanning trees of a graph G can be done in polynomial time.

More precisely, for a graph G with adjacency matrix M_G one can compute in polynomial time a matrix M' such that

$$det(M') = \sum_T \prod_{(i,j) \in T} 1$$

where T ranges over the spanning trees of G.

We define the degree matrix $D = (d_{i,j})$ by

$$d_{i,j} = \begin{cases} d_i & \text{the degree of vertex } i \text{ if } i = j \\ -k & \text{where } k \text{ is the number} \\ & \text{of edges connecting} i \text{ and } j \end{cases}$$

and take for M' any matrix obtained from D by deleting one row and one column of the same index.

Counting Eulerian Circuits (BEST Theorem)

Theorem:
(de Bruijn, van Ardenne-Ehrenfest, Smith and Tutte, 1951)

The number of Eulerian circuits $s(G)$ of a rooted directed graph G with $d^-(v) = d^+(v) = d(v)$ for every vertex v is given by

$$s(G) = t_{root}(G) \prod_v (d(v) - 1)!$$

where t_{root} denotes the number of spanning trees of G which are oriented towards the root.

For undirected graphs the number of Eulerian circuits is also computable similarly, but the formula is more complicated.

Generating Functions of Graph Properties

Let $G = \langle V, E, w \rangle$ be an edge weighted graph with weights in a field K.

Let $\mathcal{E}$ be a class of (unweighted) graphs closed under isomorphisms.

We extend w to subsets of E by defining

$$w(E') = \prod_{e \in E'} w(e)$$

The *generating function corresponding to G and $\mathcal{E}$* is defined by

$$GF(G, \mathcal{E}) =_{def} \sum_{\langle V, E' \rangle \in \mathcal{E} \text{ and } E' \subseteq E} w(E')$$

Generating Functions of Graph Properties (contd)

For $\mathcal{E}$ the class of perfect matchings

$$\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \cdots$$

$$\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \cdots$$

we get the **permanent of a matrix** M

$$\sum_{\pi \in S_n} \prod_i m_{i,\pi(i)}$$

For $\mathcal{E}$ the class of cycles

$$\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \cdots \bullet \quad \bullet$$

$$\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \cdots \bullet \quad \bullet$$

we get the **hamiltonian of a matrix** M

$$\sum_{\pi \in Ham_n} \prod_i m_{i,\pi(i)}$$

Generating Functions of Graph Properties (contd)

Strictly speaking $GF(G, \mathcal{E})$ is a function with argument w and value in K.

Furthermore, w is a function

$$w : \{1, \ldots, n\}^2 \to K$$

which can be interpreted as an $(n \times n)$ matrix over K.

If we view $w(i, j) = u_{i,j}$ as indeterminates, $GF(G, \mathcal{E})$ is a multivariate polynomial in

$$K[u_{i,j} : i, j \leq n]$$

Generating Functions of Graph Properties (Variations)

$$GF(G, \mathcal{E}) =_{def} \sum_{\langle V,E'\rangle \in \mathcal{E} \text{ and } E' \subseteq E} w(E')$$

If all the non vanishing weights are 1 we get a **counting** function.

This includes **decision** problems for existence.

$$GF_{MAX}(G, \mathcal{E}) =_{def} MAX_{\langle V,E'\rangle \in \mathcal{E} \text{ and } E' \subseteq E} w(E')$$

gives an **optimization** problem.
Similar for the minimum function MIN.

Graph polynomials, I

Let $<_E$ be a fixed ordering (indexing) of the edges of a graph $\langle V, E\rangle$ and let $\mathcal{G}_{ord}$ x be the class of such edge-ordered graphs.

Let $\mathfrak{R}$ be a ring and $X_{i,j}$ be indeterminates.

The determinant, permanent, hamiltonian are functions

$$\mathcal{F} : \mathcal{G}_{ord} \to \mathfrak{R}[X_{i,j}]$$

from edge-ordered graphs into the polynomial ring over $\mathfrak{R}$.

If we change the order of the edges, we obtain different polynomials.

Graph polynomials, II

A **graph polynomial** is a function

$$\mathcal{F} : \mathcal{G}_{ord} \rightarrow \Re[X_{i,j}]$$

which is **invariant** of the order.
We also speak of *graph invariants*.

$\mathcal{F}$ is a **complete** graph inviariant if

$$\mathcal{F}(G) = \mathcal{F}(G') \text{ iff } G \simeq G'$$

Example:

$$\mathcal{F}_1(G) = \sum \pi \in S_n \prod_{(i,j) \in E} x_{\pi(i),\pi(j)}$$

Is a complete graph invariant.
But not very useful!

Graph polynomials, III

The *generating matching polynomials* $g(G, \lambda)$, the *defect matching polynomials* $m(G, \lambda)$ and the *rook polynomials* $\rho(B, \lambda)$ of a graph G, respectively bipartite graph $B \subset K_{n,n}$, are defined as

$$g(G, \lambda) = \sum_r p(G, r)\lambda^r \qquad \text{(gen-m)}$$

$$m(G, \lambda) = \sum_r (-1)^r p(G, r)\lambda^{n-2r} \qquad \text{(def-m)}$$

$$\rho(B, \lambda) = \sum_r (-1)^r p(B, r)\lambda^{n-r} \qquad \text{(rook)}$$

where $p(G, r)$ denotes the number of (partial) r-matchings of G, and E' ranges over the partial matchings of G, respectively B.

These are polynomials in **one** indeterminate λ in $\mathbb{Z}[\lambda]$.

Graph polynomials, IV

Let $m_r(G)$ be the number of vertex colorings of G with exactly r colors. The **chromatic polynomial** is defined by

$$\chi(G;u) = \sum_{r=1}^{n} \prod_{i=0}^{r-1} (u-i)$$

with $\chi(G;s)$ the number of s-colorings of G for $s \in \mathbb{N}$.

$\chi(G;u)$ is usually studied in $\mathbb{C}[u]$.

The Tutte polynomial $T(G;X,Y)$ is probably the most intriguing graph polynomial. It is a polynomial in $\mathbb{R}[X,Y]$ and has a complicated definition.

Many other graph polynomials are instances of the Tutte polynomial.

Chromatic Polynomial and Tutte polynomial

Let $p_G(m)$ be the number of proper m-vertex-colorings of G. Then

$$p_G(m) = (-1)^{r(G)} \cdot m^{k(G)} \cdot T(G, 1-m, 0)$$

with $k(G)$ the number of connected components of G and
$r(G) = |V| - k(G)$ the *rank of* G.

Tutte Polynomials, preview

The Tutte polynomials have interesting interpretations. Let G be a connected graph.

$T(G,1,1)$: is the number of spanning trees in G.

$T(G,2,1)$: is the number of spanning forests in G.

$T(G,1,2)$: is the number of connected spanning subgraphs in G.

$T(G,2,2)$: is the number of spanning subgraphs in G.

$T(G,2,0)$: is the number of acyclic orientations in a graph G.

Knots

Knots are mappings of S^1 (a closed line) into $\mathbb{R}^3$ (Euclidean space) without selfintersections.

We think of the knot as a closed rope sitting in $\mathbb{R}^3$. We can "move" the rope (topologically).

Two knots are *topologically equivalent* if they can be obtained from each other by "moving the rope".

We can draw a know in $\mathbb{R}^2$ by projection it.

A knot is *tame* if it has projection with a finite number of crossings (undercrossings, overcrossings).

This gives a colored graph.

Can we "understand" knots by analyzing those crossing graphs?

Goal of the course

Develop understanding of

- combinatorial counting functions and graph polynomials

- algebraic aspects of combinatoric

- some knot theory and its polynomials

- complexity of combinatorial counting

We shall (in projects) collect graph polynomials and list systematically their properties.