

Author: Christos H. Papadimitriou

Title: On the Symbolic Evaluation of Determinants

Creator: HDML

**BULLETIN OF THE GREEK MATHEMATICAL SOCIETY**  
**Vol. 21(1980)**

**ON THE SYMBOLIC EVALUATION OF DETERMINANTS**

**By**  
**Christos H. Papadimitriou**

---

**Abstract**

We show that the problem of computing an individual term of the determinant of a matrix with entries multivariate polynomials is  $\mathcal{P}$ -complete, and, therefore, it is possible that it cannot be solved in polynomial time even in the unlikely event that  $\mathcal{P} = \mathcal{N}^{\mathcal{P}}$ . Our proof also suggests a new probabilistic algorithm for Hamilton's problem.

## 1. Introduction.

Symbolic manipulation is the area of computational mathematics which deals with the formal manipulation of multivariate rational functions (e.g., factorization of polynomials, partial fraction decomposition, etc.); symbolic integration of functions; automated solution of algebraic and differential equations (in closed form); automatic manipulation and conversion of special functions; automatic expansion in Taylor series, etc. It is emphasized that the results sought are symbolic, not numerical. For example, the output of the symbolic integration of the function

$$x^2 \cdot \sin(x)$$

---

is the function

$$2x \cdot \sin(x) + (2 - x^2) \cdot \cos(x)$$

Among the most ambitious and rigorous projects in symbolic manipulation is the program MACSYMA [7]. For an overview of the outstanding successes and future challenges in this field see [8]. In that paper it was pointed out that one of the most prominent unsolved problems in the area is the task of computing efficiently the determinant of a matrix whose entries are polynomials in many variables.

The determinant of an  $n \times n$  numerical matrix can be computed in  $O(n^3)$  steps by Gaussian elimination [2]. The same method can be used when the entries are univariate polynomials. However, when the number of variables is large - e.g., comparable to  $n$  - then this method cannot be applied efficiently, because the intermediate results can be enormous.

Recently Zippel [13] discovered an efficient probabilistic algorithm for computing such determinants. To understand his idea, suppose that we simply wish to determine

whether a multivariate determinant is identically 0 or not. A strikingly simple idea is the following: We substitute "random" integer values for the variables. Now the matrix is numerical, and we can compute the determinant by Gaussian elimination. If the result is not 0, then we have our answer: the determinant is not identically 0. If, however, the result is 0, the determinant may or may not be identically 0. It is intuitively clear, however, that if we repeat this experiment and the result always comes out 0, then most probably the determinant is identically 0. Zippel proved rigorously that if the "random" values are integers in the interval  $[-vdn/\epsilon, vdn/\epsilon]$  - where  $v$  is the number of variables,  $d$  bounds from above the degree of any variable and  $\epsilon > 0$  -

---

then the probability of error in one experiment is below  $\epsilon$ . Zippel's method can be extended to compute the determinant (again, with negligible probability of error) in a number of steps that grows as a polynomial in  $n, v$  and  $t$ , where  $n$  and  $v$  are as above and  $t$  is the number of terms (i.e., monomials) in the determinant.

This excellent result, however, leaves open another interesting question. Suppose that we have a matrix with multivariate polynomial coefficients, and we wish to compute, not the whole determinant, but a single term of it - for example, the coefficient of  $x^3y^7z^2wt^4$  in the determinant. Can we do this efficiently? In this paper we show that it is very unlikely that an efficient algorithm for doing this exists, even in the relatively simple case in which the entries of the matrices are 0, 1 or individual indeterminates such as  $x, y$ , and  $z$ .

We prove this result based on the theory of computational complexity (see [5], [6], [1], [3], [10], [11]). For a long time researchers had identified certain common comput-

ational tasks which appeared to require an exponential - in the size of the input - amount of time. Such problems originated from a number of areas of mathematics, such as number theory, logic, operations research and combinatorics. Examples of such problems are

(a) the problem of finding out whether a Boolean formula is satisfiable, i.e., can be made true by some truth assignment.

(b) the traveling salesman problem, i.e., finding the shortest way of visiting a set of  $n$  cities, where the distance between any two cities is given [10].

(c) the problem of solving Diophantine quadratic equations with two unknowns.

---

(d) Hamilton's problem [10]. In this problem we are given a directed graph  $G = (V, E)$  - a finite set  $V$  of nodes and a set of edges  $E \subseteq V \times V$  - and two distinguished vertices  $s, t \in V$ . We are asked whether there is a path in  $G$  from  $s$  to  $t$  that visits each node of  $V$  exactly once.

(e) over 300 other problems (see [3],[10]).

Recent advances in computational complexity showed that these problems are all equivalent in the sense that if one of them has a polynomial-time algorithm for its solution, then all of them have. Such problems are called **NP**-complete - see Section 2 and the references for the precise definition - and are widely believed to be all computationally intractable.

In this paper we point out an interesting connection between the theory of **NP**-completeness and symbolic evaluation. In particular, we show that the problem of computing a specific coefficient of a multivariate determinant is at least as hard as that of counting the number of Hamilton paths in a graph. Since Hamilton's problem simp-

ly asks whether such a path exists, the counting version is even harder than this  $\mathcal{NF}$ -complete problem! Valiant uses the term  $\mathcal{F}$ -complete (which stands for "number" or "enumeration" -complete) for such problems [11] (see the next Section for formal definitions). Valiant proves that all known  $\mathcal{NF}$ -complete problems have "enumeration versions" that are  $\mathcal{F}$ -complete. An impressive result by Valiant is that the problem of computing the permanent of a 0-1 matrix is such a problem. This result is important because it shows that there exist polynomial problems, namely the bipartite matching problem [10], which have  $\mathcal{F}$ -complete enumeration versions. (Counting the number of complete bipartite matchings in a bipartite graph is easily seen to be equivalent to computing the permanent of the adjacency matrix of the graph). In fact, Valiant has pointed out that the intractability of the symbolic evaluation of determinants can be shown using his result about the permanent [12]. Our proof, however, is direct, independently discovered, and gives an interesting insight in Hamilton's problem as well.

## 2. Definitions from Complexity Theory.

For definitions of Turing machines see [1], [6]. Let  $\Sigma$  be an alphabet adequate for the encoding of combinatorial objects - the details of such encodings are as usual uninteresting and inconsequential (see [1], [3], [10]). A recognition problem is a function  $f$  from  $\Sigma^*$  to  $\{0,1\}$  ( $\Sigma^*$  denotes the set of strings of symbols in  $\Sigma$ ). A recognition problem is said to be in the class  $\mathcal{NF}$  if there exists a nondeterministic Turing machine  $M$  and an integer  $d > 0$  such that  $M$  on input  $x \in \Sigma^*$  has an accepting computation of length  $|x|^d$  or less iff  $f(x) = 1$ . A counting problem is a function  $C$  from  $\Sigma^*$  to the set of natural numbers. A counting problem

is said to be in the class  $\mathcal{F}$  if there exists a nondeterministic Turing machine  $M$  and an integer  $d > 0$  such that  $M$  on input  $x \in \Sigma^*$  has exactly  $C(x)$  accepting computations of length  $|x|^d$  or less (here by  $|x|$  we denote the length of the string  $x$ ).

A transformation  $T$  from a recognition problem  $f$  to another  $g$  (resp. counting problem  $C$  to another  $D$ ) is a function  $T$  from  $\Sigma^*$  to  $\Sigma^*$  such that (1)  $T$  can be computed by a deterministic Turing machine in polynomial time, and (2) for each  $x \in \Sigma^*$  we have

$$f(x) = g(T(x)) \text{ (resp. } C(x) = D(T(x))).$$

A recognition problem  $f$  is said to be  $\mathcal{NF}$ -complete if

- 
- (a)  $f \in \mathcal{NF}$
  - (b) Each problem  $g \in \mathcal{NF}$  is transformable to  $f$ .

A counting problem  $C$  is said to be  $\mathcal{F}$ -complete if

- (a)  $C \in \mathcal{F}$
- (b) Each problem  $D \in \mathcal{F}$  is transformable to  $C$ .

For example, the satisfiability problem, the traveling salesman problem, quadratic Diophantine equations, and Hamilton's problem are all  $\mathcal{NF}$ -complete. The problem of computing the permanent of a 0-1 matrix, and that of counting the number of Hamilton paths from a node  $s$  to another  $t$  in a graph  $G$  are  $\mathcal{F}$ -complete. In the next Section we show that the problem of computing the coefficient of a specific term in a multivariate determinant is  $\mathcal{F}$ -complete.

### 3. The Main Result

We now formulate the multivariate determinant problem as a counting problem  $D$ . Let  $E$  be a function which encodes multivariate matrices and monic monomials as strings in  $\Sigma^*$ . Then  $D$  is defined to be the function such that for any  $n \times n$  ma-

trix  $M$  with entries equal to 0, 1, or  $x_j$  for  $j=1, \dots, v$ , and each term  $\tau = \prod_{j=1}^v x_j^{d_j}$ , we have

$$D(E(M, \tau)) = c + n!$$

where  $c$  is the coefficient of  $\tau$  in the determinant of  $M$ . The addition of  $n!$  in the definition of  $D$  is necessary because  $c$  can be negative. For all  $x$  that are not encodings of such  $M$  and  $\tau$  we let by convention  $D(x) = 1$ .

This section is dedicated to the proof of the following:

**Theorem. 1.**  $D$  is  $\mathcal{F}$ -complete.

**Proof.** We first show that  $D \in \mathcal{F}$  by designing a non-deterministic Turing machine  $T$  which computes  $D$ . This is easy to do.  $T$  starts by checking whether its input  $x$  is of the form  $E(M, \tau)$ ; if not,  $T$  halts (a total of  $1 = D(x)$  halting computations). Otherwise,  $T$  nondeterministically chooses a permutation  $\pi$  of  $1, 2, \dots, n$  - where  $M$  is  $n \times n$  - and tests whether  $\prod_{j=1}^n M_{j, \pi(j)} = \pm \tau$ . If it is  $+\tau$ , then  $T$  branches once and halts, adding 2 to the count of accepting computations. If it is  $-\tau$ , then  $T$  diverges, adding 0. If it is neither, then  $T$  halts adding 1. It follows that  $T$  has  $n! + c$  accepting computations of length at most  $|x|^d$ , for some appropriate  $d > 0$ .

We now have to show that all counting problems in  $\mathcal{F}$  are polynomially transformable to  $D$ . It suffices to show how to transform to  $D$  the known  $\mathcal{F}$ -complete problem of counting the Hamilton circuits of a directed graph. Given a directed graph  $G = (V, E)$  and two nodes  $s, t \in V$  we shall show how to construct a matrix  $M$  of 0's, 1's and indeterminates, and a term  $\tau$ , such that the number of Hamilton paths from  $s$  to  $t$  in  $G$  equals the coefficient of  $\tau$  in  $\det(M)$ . In the end of the proof we sketch the modifications needed

for accommodating the definition of  $D$  above, in which the coefficient is increased by  $n!$

Let us assume without loss of generality that  $|V|$  is odd. From  $G=(V,E),s,t$  we first construct a labeled directed graph  $G'=(V',E',L)$ , that is, a directed graph  $(V', E')$  and a mapping  $L$  from  $E'$  to  $V$ , as follows

- (1)  $V' = \{s,t\} \cup (V-\{s,t\}) \times \{1,2,\dots,|V|-2\}$
- (2)  $E' = \{(s,(v,1)):v \in V-\{s,t\},(s,v) \in E\} \cup \{(v,|V|-2), t):v \in V-\{s,t\},(v,t) \in E\} \cup \{(u,j),(v,j+1):u,v \in V-\{s,t\},(u,v) \in E,1 \leq j \leq |V|-3\} \cup \{(t,s)\}$ .
- (3)  $L((u,v))=s$  if  $u=s,t$  if  $u=t$ , and  $w$  if  $u=(w,j)$ .

An illustration of the construction is shown in Figure 1.

---

Let  $M(G')$  be the  $|V'| \times |V'|$  matrix with rows and columns indexed by the elements of  $V'$ , such that the  $(u,v)$ -th entry of  $M(G')$  is the variable  $L((u,v))$  whenever  $(u,v) \in E'$ , and 0 otherwise. Then the matrix  $M$  and the term  $\tau$  can be defined as follows:

$$M = M(G') + I$$

$$\tau = \prod_{v \in V} v$$

(see Figure 1c). Notice that we treat the vertices of  $G$  as indeterminates.

We claim that the number of Hamilton paths from  $s$  to  $t$  in  $G$  equals the coefficient of  $\tau$  in  $\det(M)$ .  $(s, v_1, v_2, \dots, v_{|V|-2}, t)$  is a Hamilton path in  $G$  iff  $(s, (v_1, 1), (v_2, 2), \dots, (v_{|V|-2}, |V|-2), t)$  is a cycle in  $G'$  and the  $v_j$ 's are all distinct; furthermore there are no other cycles in  $G'$ . Hence there is a one-to-one correspondence between Hamilton paths from  $s$  to  $t$  in  $G$  and such cycles in  $G'$ .

It follows directly from the construction of  $M$  that any monomial in  $\det(M)$  different from 1 will be of the form

s.t.  $\prod_{j=1}^{|V|-2} v_j$ , where  $(s, (v_1, 1), \dots, (v_{|V|-2}, |V|-2), t)$  is a path in  $G$ . All these monomials will have coefficient  $+1$ , because  $|V|$  was taken to be odd. Thus there is a one-to-one correspondence between monomials equal to  $\tau$  and cycles of the form  $(s, (v_1, 1), \dots, (v_{|V|-2}, |V|-2), t)$  in  $G'$ , where all  $v_j$ 's are distinct; that is, Hamilton paths in  $G$ . This completes the proof of the claim.

Finally, to accommodate our definition of  $D$ , we first note that the Hamilton path problem, remains  $\mathfrak{F}$ -complete even though the graph is restricted to have at least one given Hamilton path (see [9]). To complete the proof, we simply label one of the arcs of  $G$  that correspond to the distinguished Hamilton path, by  $|V|+1 \cdot x$ , instead of  $x$ .

We finally note that our reduction raises the following question about Hamilton's problem: Let  $G = (V, E)$  be a directed graph. Consider the set  $E(G)$  of all Eulerian graphs  $G = (V_e, E_e)$  such that:

- (a)  $E_e$  is a multiset of edges from  $E$ , and
- (b)  $|E_e| = |V|$ .

Let  $\mathfrak{F}(G)$ , the set of patterns of  $G$ , be defined as follows:

$$\mathfrak{F}(G) = \{(d_1, \dots, d_{|V|}) \in \mathbb{N}^{|V|} : \text{for some } G_e \in E(G)$$

the in-degree of  $v_j$  in  $G_e$  is  $d_j$   $j = 1, \dots, |V|\}$

From the proof of Theorem 1 and Zippel's algorithm, we have the following result:

**Corollary.** *There is a probabilistic algorithm [4] for counting the Hamilton circuits of any directed graph  $G$ , which runs in polynomial time in the size of  $G$  and  $|\mathfrak{F}(G)|$ .*

It remains an open question whether there are interesting classes of directed graphs which have a polynomially bounded number of patterns.

## References

- [1] A.V. Aho, J.E. Hopcroft, J.D. Ullman, The Design and Analysis of Computer Algorithms, Addison-Wesley, 1974.
- [2] F.R. Gantmacher Matrix Theory Vol. 1, Chelsea 1959, Chapter 2.
- [3] M.R. Garey, D.S. Johnson Computers and Intractability: A Guide in the Theory of NP-completeness, Freeman, 1979.
- [4] J.Gill "Complexity of Probabilistic Turing Machines" SIAM J. Computing, Vol. 6, No. 4, 1977, pp 675-695.

---

- [5] R.M. Karp "Reducibility among Combinatorial Problems" in Complexity of Computer Computations R.E.Miller and J.W. Thatcher (eds), Plenum, 1972.
- [6] H.R. Lewis, C.H. Papadimitriou Elements of the Theory of Computation, Prentice-Hall 1981.
- [7] MATHLAB Group "MACSYMA Reference Manual-Version 9", M.I.T., 1977.
- [8] J. Moses "The Evolution of Algebraic Manipulation Algorithms", in Best Computer Papers, pp.197-214- Auerbach, 1976.
- [9] C.H. Papadimitriou, K. Steiglitz "The Complexity of Local Search for the Travelling Salesman Problem", SIAM J. Computing, 6, 1, 1977 pp. 76-83.
- [10] C.H. Papadimitriou, K. Steiglitz Combinatorial Optimization: Algorithms and Complexity Prentice-Hall, 1982.
- [11] L.G. Valiant "The Complexity of Computing the Perma-