Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Linear Algebra and its Applications 375 (2003) 197–209
LINEAR ALGEBRA AND ITS APPLICATIONS
www.elsevier.com/locate/laa

On the number of different permanents of some sparse (0, 1)-circulant matrices

Giovanni Resta*, Giovanni Sburlati

Istituto di Informatica e Telematica, Area della Ricerca CNR, via Moruzzi 1, 56124 Pisa, Italy

Received 16 April 2003; accepted 29 May 2003

Submitted by R.A. Brualdi

Abstract

Starting from known results about the number of possible values for the permanents of (0, 1)-circulant matrices with three nonzero entries per row, and whose dimension n is prime, we prove corresponding results for n power of a prime, n product of two distinct primes, and $n = 2 \cdot 3^h$. Supported by some experimental results, we also conjecture that the number of different permanents of $n \times n$ (0, 1)-circulant matrices with k nonzero per row is asymptotically equal to $n^{k-2}/k! + O(n^{k-3})$.

AMS classification: 15A15; 65F50

Keywords: Sparse circulant matrix; Matrix permanent

1. Introduction

The computation of the permanent of a (0, 1)-matrix is known to be a $\sharp P$-complete problem (see [8,9]), where $\sharp P$ is the class of functions which are computable by a counting nondeterministic Turing machine in polynomial time. The fastest algorithm among those presently known for computing the permanent of a generic matrix takes $O(n2^n)$ operations [7], n denoting the matrix size. The computation of the permanent of a matrix with at most three nonzero entries in each row and column is still a $\sharp P$-complete problem [4], while Codenotti and Resta [3] showed that

* Corresponding author.
E-mail addresses: g.resta@iit.cnr.it (G. Resta), g.sburlati@iit.cnr.it (G. Sburlati).

0024-3795/$ - see front matter
doi:10.1016/S0024-3795(03)00649-9

the permanent Per(M) of any (0, 1)-circulant matrix M with three nonzero entries per row is the sum of four determinants of suitable sparse matrices, and thus it is computable in polynomial time.

In [1] it was proved that for any prime $n > 2$ the expression Per(M_n) can take at most $\lceil n/6 \rceil$ different values, where M_n is an $n \times n$ (0, 1)-circulant matrix with three nonzero entries per row.

In this paper, a deeper investigation provides more general results on the number of the possible values taken by Per(M_n). In particular, we obtain inequalities for the cases $n = p^h$, $n = 2^h$, $n = pq$, $n = 2p$, and $n = 2 \cdot 3^h$, where p and q are distinct odd primes. These results are obtained starting from a general, if not tight, inequality holding for any odd n.

The paper is organized as follows. In Section 2, we introduce the notation used in the rest of the paper and in Section 3 we review some known results for the case of matrices of size equal to an odd prime [1]. In Section 4 we study the cases in which n is a power of a prime, n is product of two distinct primes and $n = 2 \cdot 3^h$, making relevant use of elementary number theory. Finally in Section 5 we make some concluding remarks and we present some experimental results which show that our inequalities are tight for $n \leqslant 121$, and that suggest related conjectures for the (0, 1)-circulant matrices with more than three nonzero entries per row.

2. Preliminaries

Let Σ denote the set of all permutations of the first n integers. Given an $n \times n$ square matrix A, the permanent of A is the number

$$\mathrm{Per}(A) = \sum_{\sigma \in \Sigma} \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

For any $n \times n$ (0, 1)-matrix A, if we denote by $D(A)$ and $G[A]$, respectively, the digraph whose adjacency matrix is A and the $2n$-node bipartite graph associated with A in the standard way, then the permanent of A is equal to the number of cycle covers of $D(A)$ and simultaneously to the number of perfect matchings of $G[A]$.

In the rest of the paper, we denote by P_n the $n \times n$ circulant (0, 1)-matrix with the only 1's in positions $(n, 1)$ and $(i, i + 1)$, $i = 1, 2, \ldots, n - 1$. We will omit the subscript 'n' when the dimension of the matrix is clear from the context.

In general, a circulant matrix with three nonzero entries per row can be expressed as $P_n^i + P_n^j + P_n^h$, where $0 \leqslant i < j < h < n$. Since P_n is also a permutation matrix, we have $\mathrm{Per}(P_n^i + P_n^j + P_n^h) = \mathrm{Per}(P_n^{-i}(P_n^i + P_n^j + P_n^h)) = \mathrm{Per}(I + P_n^{j-i} + P_n^{h-i})$, and thus we can confine ourself to the study of the number of values taken by $\mathrm{Per}(I + P^i + P^j)$ for $1 \leqslant i < j < n$.

We will denote with (a, b) the greatest common divisor of a and b.

For $n \in \mathbf{N}$, the symbol $\mathbf{Z}_n^*$ denotes the set of invertible elements in $\mathbf{Z}_n$, and $\varphi(n)$ (φ Euler's arithmetic function) is the number of elements of $\mathbf{Z}_n^*$. We define the arithmetic function η as follows:

$$\eta(n) = \left|\{i \in \mathbf{N} : [(1 \leqslant i \leqslant n) \wedge (i, n) = (i+1, n) = 1]\}\right| \quad \forall n \in \mathbf{N}.$$

Equivalently, $\eta(n) = |\{z \in \mathbf{Z}_n^* : z + 1 \in \mathbf{Z}_n^*\}|$ for every $n \in \mathbf{N}$. For generic $n = \prod_t p_t^{h_t} \geqslant 2$, the p_t's being distinct primes, the following formulas hold:

$$\varphi(n) = \prod_t p_t^{h_t - 1}(p_t - 1), \quad \eta(n) = \prod_t p_t^{h_t - 1}(p_t - 2).$$

The following 'reduction lemma' will be useful for matrices whose size is a composite number.

Lemma 1 [2]. *Let $A = I_n + P_n^{di} + P_n^{dj}$, with d a divisor of n and $1 \leqslant i < j \leqslant (n/d) - 1$. Then*

$$\operatorname{Per}(A) = \left[\operatorname{Per}\left(I_{n/d} + P_{n/d}^i + P_{n/d}^j\right)\right]^d.$$

3. Equivalence classes for $G[I + P^i + P^j]$

In [1] the authors provide detailed analysis of the relationship among the permanents of different circulants $A = I_n + P_n^i + P_n^j$ (with $1 \leqslant i < j \leqslant n-1$) of size n, when n is an odd prime. In particular, for any fixed prime $n > 2$, they determine the maximum number of different values that $\operatorname{Per}(A)$ can take, passing through the determination of the *equivalence class* of A, i.e. the set of matrices $B = I + P_n^h + P_n^k$ such that $\operatorname{Per}(B) = \operatorname{Per}(A)$.

Given an $n \times n$ matrix $A = I_n + P_n^i + P_n^j$ (with $1 \leqslant i < j \leqslant n-1$), where n is an odd prime, it is easy to see that the bipartite graph $G[A]$ can be drawn as a cycle of length $2n$ with n additional chords. The edges on the cycle will correspond to the ones in $P^i + P^j$ while the chords correspond to I. The chord length (the number of cycle edges spanned by each chord) is equal to

$$D = D(n, i, j) = n - \left|n - 2[i(j-i)^{-1}]_{(\mathrm{mod}\ n)} - 1\right|, \tag{1}$$

see [1,2], where inversion is computed in $\mathbf{Z}_n^*$ and $[M]_{(\mathrm{mod}\ n)}$ denotes the integer $M' \in \mathbf{N}$ with $0 \leqslant M' \leqslant n-1$ and $M' \equiv M \pmod{n}$.

It is clear that if two circulant matrices A and B of size n share the same value of D, then the graphs $G[A]$ and $G[B]$ are isomorphic, implying $\operatorname{Per}(A) = \operatorname{Per}(B)$.

Given a matrix $A = I + P^i + P^j$, the possibility to draw the graph $G[A]$ as a "cycle + chords" depends on the fact that $P^i + P^j$ corresponds to a cycle in $G[A]$ and in turn this is possible since $(n, j-i) = 1$.

When n is a prime odd number, it is always possible to draw similar representations of $G[A]$ using $I + P^j$ or $I + P^i$ for the cycle and the remaining component for the chords, as exemplified in Fig. 1.

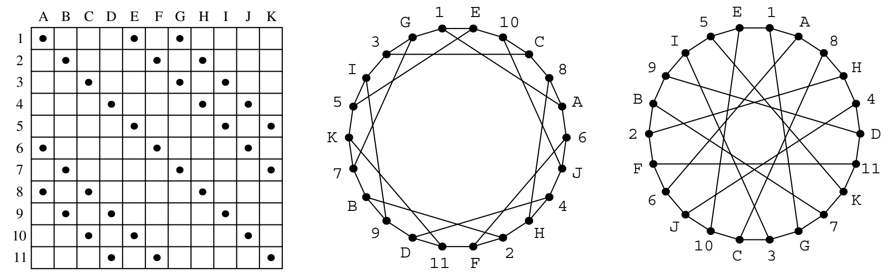

Fig. 1. The matrix $A = I + P^4 + P^6$, for $n = 11$, and two equivalent drawings of $G[A]$, with $d = 5$ and 9.

The lengths $D'(n, i, j)$ and $D''(n, i, j)$ of the chords in these two alternative representations of $G[A]$ are

$$D'(n, i, j) = D(n, j - i, n - i) = n - \left|n - 2[(j - i)(n - j)^{-1}]_{(\text{mod } n)} - 1\right|, \tag{2}$$

$$D''(n, i, j) = D(n, n - j, n + i - j) = n - \left|n - 2[(n - j)i^{-1}]_{(\text{mod } n)} - 1\right|. \tag{3}$$

Thus, given a matrix A we obtain a triple of values $\{D, D', D''\}$. If two matrices A and B have one or more values in common in their triples, then the corresponding graphs $G[A]$ and $G[B]$ are isomorphic and $\text{Per}(A) = \text{Per}(B)$. Building upon this characterization, in [1] the authors showed that the permanent of $I_n + P_n^i + P_n^j$ takes at most $\lceil n/6 \rceil$ values, when n is an odd prime. In the following section we generalize this approach to the case of composite n.

4. Generalization to n composite

Given an $n \times n$ matrix $A = I_n + P_n^i + P_n^j$ with $n \geqslant 3$ and $1 \leqslant i < j \leqslant n - 1$, if $i - j \in \mathbf{Z}_n^*$ then, as in the previous section for n prime, we can draw the bipartite graph $G[A]$ as a cycle (obtained using P^i and P^j) and n chords (corresponding to I) whose length is D as in (1).

Analogously, if $i, j \in \mathbf{Z}_n^*$, then there are two other possible "cycle + chords" representations of $G[A]$, whose lengths will be D' and D'' as in (2) and (3).

To better explicitate the different cases (with respect to the appartenence of i, j and $j - i$ to $\mathbf{Z}_n^*$) we use the following definition.

Definition 1. For any fixed $n \in \mathbf{N}$, $n \geqslant 3$, we denote by $N(n)$ (resp. $N'(n)$, $N''(n)$) the number of different values taken by $\text{Per}(I_n + P_n^i + P_n^j)$ under the condition

$i, j, i-j \in \mathbf{Z}_n^*$ (resp. $|\{i, j, i-j\} \cap \mathbf{Z}_n^*| \geqslant 2$, $|\{i, j, i-j\} \cap \mathbf{Z}_n^*| \geqslant 1$). The symbol $N_{\text{tot}}(n)$ indicates the number of possible values for $\text{Per}(I_n + P_n^i + P_n^j)$ with no constraints on $|\{i, j, i-j\} \cap \mathbf{Z}_n^*|$.

A generic n being fixed, for $1 \leqslant i < j \leqslant n-1$, if $i - j \in \mathbf{Z}_n^*$ let us define $a_{i,j} = (j-i)^{-1}i$. If $i, j \in \mathbf{Z}_n^*$, let us define $b_{i,j} = (n-j)^{-1}(j-i)$, $c_{i,j} = i^{-1}(n-j)$. When $i, j, i-j \in \mathbf{Z}_n^*$ we can consider the triple $T_{i,j} = (a_{i,j}, b_{i,j}, c_{i,j}) \in (\mathbf{Z}_n^*)^3$. Equalities (1)–(3) show that $D(n, i, j)$, $D'(n, i, j)$ and $D''(n, i, j)$, when they are defined, depend just on $a_{i,j}, b_{i,j}, c_{i,j}$, respectively. Thus if two triples $T_{i,j}$ and $T_{h,k}$ share a value, then $\text{Per}(I_n + P_n^i + P_n^j) = \text{Per}(I_n + P_n^h + P_n^k)$.

Before characterizing the set of triples associated with a generic $n > 3$ (Theorem 1 below), we need the following lemma.

Lemma 2. *Let p be any prime number, let $h, m \in \mathbf{N}$; let us assume that $p \nmid m$. Then the equation $x^m \equiv 1 \pmod{p^h}$ has exactly $(m, p-1)$ solutions.*

Proof. For any $p, h, m \in \mathbf{N}$ with p prime, from Theorem 2.27 in [6] we obtain that the equation $x^m \equiv 1 \pmod{p}$ has $(m, p-1)$ solutions. Since $p \nmid m$, using the methods in [5, pp. 66–68], we deduce that $(m, p-1)$ is also the number of solutions of the equation $x^m \equiv 1 \pmod{p^h}$. □

Theorem 1. *Let an odd $n = \prod_t p_t^{h_t} > 3$ be fixed.*

1. *If $i - j \in \mathbf{Z}_n^*$ then $1 \leqslant a_{i,j} \leqslant n-2$; if $i, j \in \mathbf{Z}_n^*$ then $1 \leqslant b_{i,j}, c_{i,j} \leqslant n-2$. Moreover, for each z with $1 \leqslant z \leqslant n-2$ there exist i, j, i', j', i'', j'', with $i-j, j', i'' \in \mathbf{Z}_n^*$, such that $a_{i,j} = b_{i',j'} = c_{i'',j''} = z$.*
2. *If $i, j, i-j, h, k, h-k \in \mathbf{Z}_n^*$ and the two triples $T_{i,j}$ and $T_{h,k}$ have one element in common, then all their elements coincide.*
3. *If $i, j, i-j \in \mathbf{Z}_n^*$, the triple $T_{i,j}$ contains either (a) three distinct values or (b) an element repeated three times. Calling s the number of distinct triples $T_{i,j}$ verifying (b), we have*

$$s = \begin{cases} 0 & \text{if } [(9|n) \vee (\exists t : p_t \equiv 2 \pmod 3)], \\ 2^r & \text{if } [(9 \nmid n) \wedge (\forall t,\, p_t \not\equiv 2 \pmod 3)], \end{cases}$$

where r is the number of prime factors greater than 3 of n.

Proof. In this proof we will indicate $x \equiv y \pmod{n}$ simply by $x \equiv y$, for the sake of brevity.

1. When $i - j \in \mathbf{Z}_n^*$, clearly $a_{i,j} = (j-i)^{-1}i \not\equiv 0$; moreover, the equality $a_{i,j} \equiv n-1$ would imply $j - i \equiv -i$, hence $j \equiv 0$, which is absurd. The proofs for $b_{i,j}, c_{i,j}$ in the case $i, j \in \mathbf{Z}_n^*$ are similar. In particular, for any z such that $1 \leqslant z \leqslant n-2$, we have $a_{z,z+1} = b_{n-z-1,n-1} = c_{1,n-z} = z$.

2. If $i, j, i-j, h, k, h-k \in \mathbf{Z}_n^*$, then: $[a_{i,j} = a_{h,k}] \Leftrightarrow [(j-i)^{-1}i \equiv (k-h)^{-1}h] \Leftrightarrow [(k-h)i \equiv (j-i)h] \Leftrightarrow [ik \equiv jh]$. We also have: $[b_{i,j} = b_{h,k}] \Leftrightarrow [(n-j)^{-1}(j-i) \equiv (n-k)^{-1}(k-h)] \Leftrightarrow [-k(j-i) \equiv -j(k-h)] \Leftrightarrow [ik \equiv jh]$ and $[c_{i,j} = c_{h,k}] \Leftrightarrow [i^{-1}(n-j) \equiv h^{-1}(n-k)] \Leftrightarrow [-hj \equiv -ik] \Leftrightarrow [ik \equiv jh]$. Therefore: $[a_{i,j} = a_{h,k}] \Leftrightarrow [b_{i,j} = b_{h,k}] \Leftrightarrow [c_{i,j} = c_{h,k}]$. Analogously, one can prove that $[a_{i,j} = b_{h,k}] \Leftrightarrow [b_{i,j} = c_{h,k}] \Leftrightarrow [c_{i,j} = a_{h,k}]$ and that $[a_{i,j} = c_{h,k}] \Leftrightarrow [b_{i,j} = a_{h,k}] \Leftrightarrow [c_{i,j} = b_{h,k}]$.
3. Let $i, j, i-j \in \mathbf{Z}_n^*$. It follows: $[a_{i,j} = b_{i,j}] \Leftrightarrow [(j-i)^{-1}i \equiv (n-j)^{-1}(j-i)] \Leftrightarrow [-ji \equiv (j-i)^2] \Leftrightarrow [i^2 + j^2 \equiv ij]$; $[a_{i,j} = c_{i,j}] \Leftrightarrow [(j-i)^{-1}i \equiv i^{-1}(n-j)] \Leftrightarrow [i^2 \equiv -j(j-i)] \Leftrightarrow [i^2 + j^2 \equiv ij]$ and $[b_{i,j} = c_{i,j}] \Leftrightarrow [(n-j)^{-1}(j-i) \equiv i^{-1}(n-j)] \Leftrightarrow [i(j-i) \equiv (-j)^2] \Leftrightarrow [i^2 + j^2 \equiv ij]$. Thus if $[i^2 + j^2 \equiv ij]$ then $a_{i,j}, b_{i,j}, c_{i,j}$ coincide, otherwise $T_{i,j}$ has three distinct elements.

   Since $a_{i,j}b_{i,j}c_{i,j} = 1$, if $a_{i,j} = b_{i,j} = c_{i,j} = u$ then u must be a cubic root of 1 in $\mathbf{Z}_n$; using the expressions of $a_{i,j}$, $b_{i,j}$ and $c_{i,j}$, from $a_{i,j} = b_{i,j} = c_{i,j} = u$ one can easily derive $u^2 + u \equiv -1 \pmod{p_t}$ for every t, and consequently $u \not\equiv 1 \pmod{p_t}$ for any t such that $p_t > 3$. By Lemma 2 in the case $m = 3$, if there exists some t with $p_t \equiv 2 \pmod 3$ then for such t the equalities $a_{i,j} = b_{i,j} = c_{i,j} = u$ (for any u) would imply (since u would also be a cubic root of 1 in $\mathbf{Z}_{p_t}$ and the class 1 is the only cubic root of 1 in $\mathbf{Z}_{p_t}$) that $u \equiv 1 \pmod{p_t}$, which is impossible for what we stated above. All this implies that if $\exists t : p_t \equiv 2 \pmod 3$ then there are no triples $T_{i,j}$ with an element repeated three times, i.e. $s = 0$.

   When $9|n$ (i.e. for a t, $p_t^{h_t} = 3^h$ with $h \geqslant 2$), if $a_{i,j} = b_{i,j} = c_{i,j} = u$ for a u then one could derive $u^2 + u \equiv -1 \pmod 9$, which is absurd since $z^2 + z \not\equiv -1 \pmod 9$ for every $z \in \mathbf{Z}_9$. Thus for any n such that $9|n$ we have proved that $s = 0$.

   If $[(9 \nmid n) \wedge (\forall t, p_t \not\equiv 2 \pmod 3)]$ (i.e. if $n = \prod_{w=1}^{r} p_w^{h_w}$ or $n = 3 \cdot \prod_{w=1}^{r} p_w^{h_w}$ with $p_w \equiv 1 \pmod 3$ for all w) then, using Lemma 2 in the case $m = 3$, one deduces that for each w there are two nontrivial cubic roots of 1 in $\mathbf{Z}_{p_w^{h_w}}$; this fact, together with the Chinese Remainder Theorem, implies that there exist exactly 2^r cubic roots u of 1 in $\mathbf{Z}_n$ satisfying $\forall w, u \not\equiv 1 \pmod{p_w^{h_w}}$ (and then $\forall w, u \not\equiv 1 \pmod{p_w}$ by [5, pp. 66–68]); if u is such a cubic root, it is sufficient to take $i = 1$ and $j = -u$ and use the relation $u^2 \equiv -u - 1 \pmod n$ (which holds since the relation $\forall w$, $u \not\equiv 1 \pmod{p_w}$ implies $\forall w, u^2 + u + 1 \equiv 0 \pmod{p_w^{h_w}}$) for obtaining $a_{i,j} = b_{i,j} = c_{i,j} = u$. □

Remark 1. The statements 1–3 in Theorem 1 are satisfied even for $n = 3$, trivially. The statement 1 in Theorem 1 and its proof hold even when n is an even integer greater than 2.

From equalities (1)–(3) it is immediate to see that the relation $[(a_{i,j} = a_{h,k}) \vee (a_{i,j} = n - 1 - a_{h,k})]$ implies $D(n, i, j) = D(n, h, k)$ and that the converse also holds. Analogous properties for $b_{i,j}$ and $c_{i,j}$ are verified in similar way. Now, for a fixed odd $n > 3$, let us call E' the subset of $E = \{3, 5, 7, \ldots, n\}$ spanned by the values $D(n,i,j)$, $D'(n,i,j)$, $D''(n,i,j)$ with $i, j, i-j \in \mathbf{Z}_n^*$. By means of the expressions of $a_{i,j}$, $b_{i,j}$ and $c_{i,j}$ in the case $i, j, i-j \in \mathbf{Z}_n^*$, it is easy to prove that the subset of $\mathbf{Z}_n^*$ spanned by the $a_{i,j}$'s, $b_{i,j}$'s and $c_{i,j}$'s with $i, j, i-j \in \mathbf{Z}_n^*$ is equal to the subset of $\mathbf{Z}_n^*$ spanned just by the $a_{i,j}$'s (with $i, j, i-j \in \mathbf{Z}_n^*$), which is exactly the set of the elements z of $\mathbf{Z}_n^*$ such that $z+1 \in \mathbf{Z}_n^*$. From this fact, recalling the definition of the function η and the relation $[(D(n,i,j) = D(n,h,k)) \Leftrightarrow ((a_{i,j} = a_{h,k}) \vee (a_{i,j} = n-1-a_{h,k}))]$, it follows that $|E'| = [\eta(n)+1]/2$.

Now (for $n > 3$, n odd) let us consider a collection $\mathscr{T}(n)$ of sets of chord lengths which guarantee that different matrices have the same permanent:

$$\mathscr{T}(n) = \big\{\{D(n,i,j), D'(n,i,j), D''(n,i,j)\},\\ (1 \leqslant i < j \leqslant n-1) \wedge (i, j, i-j \in \mathbf{Z}_n^*)\big\}.$$

Using the results of Theorem 1 we deduce the following properties of $\mathscr{T}(n)$.

Theorem 2. *Let $n = \prod_t p_t^{h_t}$ be odd and greater than* 3; *let r be the number of prime factors of n greater than* 3.

- *If* $[(9|n) \vee (\exists t : p_t \equiv 2 \pmod 3)]$, *then $\mathscr{T}(n)$ consists of one couple* (*the set* $\{3, n\}$) *and* $[\eta(n)-3]/6$ *triples.*
- *If* $[(9\nmid n) \wedge (\forall t, p_t \not\equiv 2 \pmod 3)]$, *then $\mathscr{T}(n)$ contains 2^{r-1} singletons*, *one couple* (*the set* $\{3, n\}$) *and* $[\eta(n)-3-2^r]/6$ *triples.*

In both cases, *the sets in $\mathscr{T}(n)$ provide a partition of E'.*

Proof. If the sets $F_{i,j} = \{D(n,i,j),\ D'(n,i,j),\ D''(n,i,j)\}$ and $F_{h,k} = \{D(n,h,k),\ D'(n,h,k),\ D''(n,h,k)\}$ share a value, then one of the numbers $a_{i,j}$, $b_{i,j}$, $c_{i,j}$ must be equal either to one of the numbers $a_{h,k}$, $b_{h,k}$, $c_{h,k}$ or to one of the numbers $n-1-a_{h,k}$, $n-1-b_{h,k}$, $n-1-c_{h,k}$. In the first case, $F_{i,j} = F_{h,k}$ follows directly from Theorem 1 and equalities (1)–(3), while in the second case similar arguments lead to the same result. Then, E' is partitioned by the $F_{i,j}$'s.

If $[(9|n) \vee (\exists t : p_t \equiv 2 \pmod 3)]$, by Theorem 1 the numbers $a_{i,j}$, $b_{i,j}$, $c_{i,j}$ are distinct for any fixed i, j. The only possibility to obtain repeated values in $F_{i,j}$ is that one of the sums $a_{i,j}+b_{i,j}$, $a_{i,j}+c_{i,j}$, $b_{i,j}+c_{i,j}$ is equal to $n-1$. By the definitions of $a_{i,j}$, $b_{i,j}$, $c_{i,j}$, simple calculations show that this can happen only when $\{a_{i,j}, b_{i,j}, c_{i,j}\} = \{1, (n-1)/2, n-2\}$, which implies $F_{i,j} = \{3, n\}$. Out of such special case (which can always be obtained by taking, for example, $i = 1$ and $j = 2$), the $F_{i,j}$'s are all triples of distinct elements; the number of such triples must be $(|E'|-2)/3$. Since $|E'| = [\eta(n)+1]/2$, the thesis follows for any n such that $[(9|n) \vee (\exists t : p_t \equiv 2 \pmod 3)]$.

Even if $[(n = \prod_{w=1}^r p_w^{h_w}) \vee (n = 3 \cdot \prod_{w=1}^r p_w^{h_w})]$, with $p_w \equiv 1 \pmod 3$ for all w, the only set of the form $F_{i,j}$ with $a_{i,j}$, $b_{i,j}$, $c_{i,j}$ distinct which is not a triple is the set $\{3, n\}$ (repeat the argument above). By Theorem 1, the case $a_{i,j} = b_{i,j} = c_{i,j} = u$ happens for 2^r different u's, giving rise to exactly 2^{r-1} distinct singletons in $\mathscr{T}(n)$, since the set of such 2^r values u can be partitioned into 2^{r-1} subsets, each of which is of the form $\{u_1, u_2\}$ with $u_1 + u_2 = n - 1$ (this latter fact can be easily deduced using the Chinese Remainder Theorem and the property that, for every w, the sum of the two nontrivial cubic roots of 1 in $\mathbf{Z}_{p_w^{h_w}}$ is equal to the class -1). Out of these cases, all $F_{i,j}$'s contain three distinct elements; the number of distinct triples of the form $F_{i,j}$ must be $(|E'| - 2 - 2^{r-1})/3$, and we obtain the thesis for n such that $[(9\not| n) \wedge (\forall t,\ p_t \not\equiv 2 \pmod 3)]$. $\square$

Theorem 3. *Let n and r be as in Theorem 2. For $1 \leqslant i < j \leqslant n - 1$ and $i, j, i - j \in \mathbf{Z}_n^*$, if $[(9|n) \vee (\exists t : p_t \equiv 2 \pmod 3)]$ then $\mathrm{Per}(I_n + P_n^i + P_n^j)$ can take at most $[\eta(n)+3]/6$ (i.e. $\lceil \eta(n)/6 \rceil$) different values, while if $[(9\not| n) \wedge (\forall t,\ p_t \not\equiv 2 \pmod 3)]$ it can take at most $[\eta(n) + 3 + 2^{r+1}]/6$ distinct values.*

Proof. Clearly the number $N(n)$ of possible values of $\mathrm{Per}(I_n + P_n^i + P_n^j)$ cannot exceed the number of sets in $\mathscr{T}(n)$. By Theorem 2 if $[(9|n) \vee (\exists t : p_t \equiv 2 \pmod 3)]$, $\mathscr{T}(n)$ is composed of one couple and $[\eta(n) - 3]/6$ triples, so the permanent can take at most $\frac{\eta(n)-3}{6} + 1 = \frac{\eta(n)+3}{6}$ different values.

If $[(9\not| n) \wedge (\forall t,\ p_t \not\equiv 2 \pmod 3)]$, $\mathscr{T}(n)$ contains 2^{r-1} singletons, one couple and $[\eta(n) - 3 - 2^r]/6$ triples, and then in this case $N(n) \leqslant \frac{\eta(n)-3-2^r}{6} + 1 + 2^{r-1} = \frac{\eta(n)+3+2^{r+1}}{6}$. $\square$

Remark 2. The result of Theorem 3 (which holds even for $n = 3$, with $r = 0$), in the case $n = p^h$ (with p generic odd prime) or $n = 3p^h$ (with p prime greater than 3) is equivalent to $N(n) \leqslant \lceil (\eta(n) + 3)/6 \rceil$, i.e. $N(n) \leqslant \lceil (p^{h-1}(p - 2) + 3)/6 \rceil$ (in particular, it simplifies to $N(n) \leqslant \lceil (n + 1)/6 \rceil = \lceil n/6 \rceil$ when n is an odd prime).

For the case $n = p_1^{h_1} p_2^{h_2}$ (with p_1, p_2 odd distinct primes and $p_1^{h_1}, p_2^{h_2} > 3$) or $n = 3 \cdot p_1^{h_1} p_2^{h_2}$ (with p_1, p_2 distinct primes greater than 3), the result of Theorem 3 is equivalent to

$$N(n) \leqslant \begin{cases} \lceil \eta(n)/6 \rceil + 1 & \text{if } p_1 \equiv p_2 \equiv 1 \pmod 3, \\ \lceil \eta(n)/6 \rceil & \text{otherwise.} \end{cases}$$

What happens in the case $n = p^h > 3$ (p odd prime), if we just assume that $|\{i, j, i - j\} \cap \mathbf{Z}_n^*| \geqslant 1$ instead of $i, j, i - j \in \mathbf{Z}_n^*$? Since there are no $i, j \in \mathbf{Z}_{p^h}$ such that $|\{i, j, i - j\} \cap \mathbf{Z}_{p^h}^*| = 1$, we deduce that at least two of the numbers $i, j, i - j$ must lie in $\mathbf{Z}_n^*$. Now we prove that for $n = p^h > 3$ and $|\{i, j, i - j\} \cap \mathbf{Z}_n^*| \geqslant 2$ (with $1 \leqslant i < j \leqslant n - 1$) the number $N'(n)$ of possible values for the expression $\mathrm{Per}(I_n + P_n^i + P_n^j)$ is at most $\lceil (p^{h-1}(p + 1))/6 \rceil$.

First, for any fixed $i, j \in \mathbf{Z}_n^*$ (with $1 \leqslant i < j \leqslant n - 1$) such that $i - j \notin \mathbf{Z}_n^*$, recalling that the numbers $b_{i,j}$, $c_{i,j}$, $D'(n, i, j)$, $D''(n, i, j)$ are defined (while $a_{i,j}$, $D(n, i, j)$ are not), we claim that $D'(n, i, j) \neq D''(n, i, j)$. Indeed, for such i, j

the equality $D'(n, i, j) = D''(n, i, j)$ would imply $[(b_{i,j} = c_{i,j}) \vee (b_{i,j} = n - 1 - c_{i,j})]$, from which (by the definition of $b_{i,j}$ and $c_{i,j}$) simple calculations and arithmetic considerations would show that $i - j \in \mathbf{Z}_n^*$, contrary to what was supposed above. Analogously one can prove that if $i, i - j \in \mathbf{Z}_n^*$ and $j \notin \mathbf{Z}_n^*$ then $D(n, i, j) \neq D''(n, i, j)$, while if $j, i - j \in \mathbf{Z}_n^*$ and $i \notin \mathbf{Z}_n^*$ then $D(n, i, j) \neq D'(n, i, j)$.

In any case, when (for some fixed i, j) exactly two of the numbers $i, j, i - j$ lie in $\mathbf{Z}_n^*$, the two possible "cycle + chords" representations of $I_n + P_n^i + P_n^j$ have two different chord lengths. Resorting to Remark 2, we know that the case $i, j, i - j \in \mathbf{Z}_n^*$ gives rise to at most $\lceil(\eta(n) + 3)/6\rceil$ different values of $\mathrm{Per}(I_n + P_n^i + P_n^j)$. From the assumption $|\{i, j, i - j\} \cap \mathbf{Z}_n^*| \geqslant 2$ and the results just proved for the i, j's such that $|\{i, j, i - j\} \cap \mathbf{Z}_n^*| = 2$, we easily deduce that, adding the number $(|E| - |E'|)/2$ (i.e. $[n - 2 - \eta(n)]/4$, which is integer) to $\lceil(\eta(n) + 3)/6\rceil$, we obtain an upper bound for $N'(n)$. Therefore

$$N'(n) \leqslant \left\lceil \frac{\eta(n) + 3}{6} + \frac{n - 2 - \eta(n)}{4} \right\rceil = \left\lceil \frac{3n - \eta(n)}{12} \right\rceil = \left\lceil \frac{p^{h-1}(p + 1)}{6} \right\rceil. \tag{4}$$

(In fact (4) hold even in the case $n = 3$, with $p = 3$ and $h = 1$.)

Remark 3. Let $n = p^h > 3$ (p odd prime). If one defines $\tilde{\mathscr{T}}(n)$ rearranging appropriately, for the case $|\{i, j, i - j\} \cap \mathbf{Z}_n^*| = 2$, the definition of $\mathscr{T}(n)$ given for the case $i, j, i - j \in \mathbf{Z}_n^*$, it can be easily proved that $\mathscr{T}(n) \cap \tilde{\mathscr{T}}(n) = \emptyset$ and the sets in $\mathscr{T}'(n) = \mathscr{T}(n) \cup \tilde{\mathscr{T}}(n)$ provide a partition of $E = \{3, 5, 7, \ldots, n\}$.

Now, let $n = p^h$ (p odd prime) and let us assume $i, j, i - j \notin \mathbf{Z}_n^*$ (with $1 \leqslant i < j \leqslant n - 1$). By Lemma 1, the value $\mathrm{Per}(I_n + P_n^i + P_n^j)$ can be expressed in the form $[\mathrm{Per}(I_{p^t} + P_{p^t}^{i'} + P_{p^t}^{j'})]^{p^{h-t}}$ for suitable t, i', j' with $1 \leqslant t \leqslant h - 1$ and $|\{i', j'\} \cap \mathbf{Z}_{p^t}^*| \geqslant 1$ (implying $|\{i', j', i' - j'\} \cap \mathbf{Z}_{p^t}^*| \geqslant 2$). For each possible t, since the inequality $|\{i', j', i' - j'\} \cap \mathbf{Z}_{p^t}^*| \geqslant 2$ holds, by (4) (replacing h with t) there are at most $\lceil p^{t-1}(p + 1)/6\rceil$ possible values for $\mathrm{Per}(I_{p^t} + P_{p^t}^{i'} + P_{p^t}^{j'})$ (and then for $[\mathrm{Per}(I_{p^t} + P_{p^t}^{i'} + P_{p^t}^{j'})]^{p^{h-t}}$). All this implies that the number of possible values for $\mathrm{Per}(I_n + P_n^i + P_n^j)$ cannot exceed the sum $\sum_{t=1}^{h-1} \lceil p^{t-1}(p + 1)/6\rceil$, which is equal to

$$\begin{cases} \frac{(p+1)(p^{h-1}-1)}{6(p-1)} + \frac{2(h-1)}{3} & \text{if } p \equiv 1 \pmod 3, \\ \left\lceil \frac{(p+1)(p^{h-1}-1)}{6(p-1)} \right\rceil & \text{if } p \not\equiv 1 \pmod 3. \end{cases}$$

After fixing $n = p^h$ (p odd prime), the result just obtained for the case $i, j, i - j \notin \mathbf{Z}_n^*$, together with (4) deduced for the case $|\{i, j, i - j\} \cap \mathbf{Z}_n^*| \geqslant 2$, implies that the number $N_{\text{tot}}(n)$ of possible values for $\text{Per}(I_n + P_n^i + P_n^j)$ with $1 \leqslant i < j \leqslant n-1$ and no constraint on $|\{i, j, i-j\} \cap \mathbf{Z}_n^*|$ cannot exceed the sum $\sum_{t=1}^{h} \lceil p^{t-1}(p+1)/6 \rceil$, i.e.

$$N_{\text{tot}}(n) \leqslant \begin{cases} \frac{(p+1)(p^h-1)}{6(p-1)} + \frac{2h}{3} = \frac{(p+1)(n-1)}{6(p-1)} + \frac{2\log_p n}{3} & \text{if } p \equiv 1 \pmod 3, \\ \left\lceil \frac{(p+1)(p^h-1)}{6(p-1)} \right\rceil = \left\lceil \frac{(p+1)(n-1)}{6(p-1)} \right\rceil & \text{if } p \not\equiv 1 \pmod 3 \end{cases}$$

(in particular, if we take $n = 3^h$ we obtain $N_{\text{tot}}(n) = 3^{h-1} = n/3$).

Let us briefly consider the case $n = 2^h \in \mathbf{N}$ (with $h \geqslant 2$). Applying to such case quite similar arguments with respect to those used (for $|\{i, j, i-j\} \cap \mathbf{Z}_n^*| \leqslant 2$) in the case n is a power of an odd prime, and making direct calculations in the single case $n = 8$, one can determine that the number $N_{\text{tot}}(n)$ of possible values for $\text{Per}(I_n + P_n^i + P_n^j)$, with $1 \leqslant i < j \leqslant n-1$ and no conditions on $|\{i, j, i-j\} \cap \mathbf{Z}_n^*|$, is equal to 1 when $n = 4$, and satisfies the relation

$$N_{\text{tot}}(n) \leqslant 3 + \sum_{t=4}^{h} (2^{t-2} + 1) = 2^{h-1} + h - 4 = (n/2) + (\log_2 n) - 4,$$

when $n = 2^h \geqslant 8$.

Now we return to the case of generic $n \in \mathbf{N}$, n odd, $n = \prod_t p_t^{h_t} \geqslant 3$; as we stated in Definition 1, $N''(n)$ denotes the number of possible different values for $\text{Per}(I_n + P_n^i + P_n^j)$ (with $1 \leqslant i < j \leqslant n-1$) under the constraint $|\{i, j, i-j\} \cap \mathbf{Z}_n^*| \geqslant 1$. By means of methods similar to those used above under the assumption $i, j, i-j \in \mathbf{Z}_n^*$, and to those specifically used in the particular case $n = p^h$ with p odd prime, one can prove that $N''(n) \leqslant B(n)$, where

$$B(n) = \begin{cases} \frac{3n+\eta(n)}{6} - \frac{\varphi(n)}{2} + 2^{s-1} - 1 \\ \qquad \text{if } [(9|n) \vee (\exists t : p_t \equiv 2 \pmod 3)], \\ \frac{3n+\eta(n)+2^{r+1}}{6} - \frac{\varphi(n)}{2} + 2^{s-1} - 1 \\ \qquad \text{if } [(9\nmid n) \wedge (\forall t,\ p_t \not\equiv 2 \pmod 3)], \end{cases} \tag{5}$$

where r is the number of prime factors greater than 3 of n and s is the number of prime factors of n.

If $n = p^h q^k$ with p, q odd distinct primes, simple arithmetical properties show that $i, j, i-j \notin \mathbf{Z}_n^*$ implies $(i, j, n) > 1$. Then, by Lemma 1 this implies that, for any i, j (with $1 \leqslant i < j \leqslant n-1$) such that $i, j, i-j \notin \mathbf{Z}_n^*$, the value $\text{Per}(I_n + P_n^i + P_n^j)$ is equal to $[\text{Per}(I_d + P_d^{i'} + P_d^{j'})]^{n/d}$ for suitable d, i', j' with d divisor of n, $3 \leqslant d < n$ and $|\{i', j', i'-j'\} \cap \mathbf{Z}_d^*| \geqslant 1$. For each possible d, since $|\{i', j', i'-j'\} \cap \mathbf{Z}_d^*| \geqslant 1$ there are $N''(d)$ possible values for $\text{Per}(I_d + P_d^{i'} + P_d^{j'})$, and then for $[\text{Per}(I_d + P_d^{i'} + P_d^{j'})]^{n/d}$. Therefore, for $n = p^h q^k$ with p, q odd distinct primes, the total number $N_{\text{tot}}(n)$ of possible values for $\text{Per}(I_n + P_n^i + P_n^j)$, with $1 \leqslant i < j \leqslant n-1$ and no constraint on $|\{i, j, i-j\} \cap \mathbf{Z}_n^*|$, satisfies the inequality $N_{\text{tot}}(n) \leqslant \sum_{d|n, d\geqslant 3} N''(d)$; consequently we have $N_{\text{tot}}(n) \leqslant \sum_{d|n, d\geqslant 3} B(d)$.

In particular, taking $n = pq$ with p, q odd distinct primes, we obtain $N_{\text{tot}}(pq) \leqslant B(p) + B(q) + B(pq)$. The values $B(p)$ and $B(q)$ are equal, respectively, to $\lceil p/6 \rceil$ and $\lceil q/6 \rceil$ (this is consistent with what was shown in Remark 2 in the case n odd prime); moreover, replacing n with pq in (5), simple calculations lead to the equality $B(pq) = \lceil (p+1)(q+1)/6 \rceil + 2$ if $p \equiv q \equiv 1 \pmod 3$, and to the equality $B(pq) = \lceil (p+1)(q+1)/6 \rceil + 1$ if $[(p \not\equiv 1 \pmod 3)) \vee (q \not\equiv 1 \pmod 3))]$. Therefore

$$N_{\text{tot}}(pq) \leqslant \left\lceil \frac{p}{6} \right\rceil + \left\lceil \frac{q}{6} \right\rceil + \left\lceil \frac{(p+1)(q+1)}{6} \right\rceil + \begin{cases} 2 & \text{if } p \equiv q \equiv 1 \pmod 3, \\ 1 & \text{otherwise.} \end{cases} \tag{6}$$

Corollary 1. *If we replace q with 3 in the second of inequalities (6), we obtain that, for any prime $p > 3$, $N_{\text{tot}}(3p) \leqslant 5\lceil p/6 \rceil$ if $p \equiv 1 \pmod 3$, while $N_{\text{tot}}(3p) \leqslant 5\lceil p/6 \rceil + 2$ if $p \equiv 2 \pmod 3$.*

Similar arguments to those used in the case $n = pq$ can be applied in the case $n = 2p \in \mathbf{N}$, with p odd prime, leading to the following inequality:

$$N_{\text{tot}}(2p) \leqslant \frac{p+1}{2} + \lceil p/6 \rceil .$$

Using a similar approach for $n = 2 \cdot 3^h \in \mathbf{N}$, we can prove the following inequality:

$$N_{\text{tot}}(n) \leqslant 4 \cdot 3^{h-1} - 1 = (2n/3) - 1.$$

5. Conclusions and further work

In this paper we have proved inequalities concerning the number of possible values of $\text{Per}(I_n + P_n^i + P_n^j)$ (where $1 \leqslant i < j \leqslant n-1$) when n belong to a subset of the composite numbers, generalizing and extending similar results for the case in which n is prime.

All the upper bounds for $N_{\text{tot}}(n)$ found in the previous section are consistent with the values we obtained experimentally using the method of [3], which are tabulated in Table 1, for $n \leqslant 121$.

Some questions are still open and worth investigating. First of all, the case of matrices of the form $I_n + P_n^i + P_n^j + P_n^h$, with $1 \leqslant i < j < h \leqslant n-1$, can be considered: for $n \geqslant 5$, n prime, one can construct equivalence classes (in each of which all matrices have the same permanent) in a way similar to that shown in the previous section for the matrices with three nonzero entries per row, except the fact that the triples of the form $\{D(n,i,j),\ D'(n,i,j),\ D''(n,i,j)\}$ are replaced with 6-tuples of the form $\{(D_{\alpha,1}(n,i,j,h),\ D_{\alpha,2}(n,i,j,h)),\ 1 \leqslant \alpha \leqslant 6\}$, in which each α corresponds to a particular choice of two elements in the set $\{0, i, j, h\}$. The number

Table 1
The number of different values taken by the permanent of $\mathrm{Per}(I_n + P_n^i + P_n^j)$, for $3 \leqslant n \leqslant 121$

n	♯	n	♯	n	♯	n	♯	n	♯	n	♯
3	1	23	3	43	8	63	29	83	14	103	18
4	1	24	21	44	21	64	34	84	85	104	59
5	1	25	6	45	22	65	19	85	23	105	60
6	3	26	10	46	15	66	45	86	30	106	36
7	2	27	9	47	8	67	12	87	27	107	18
8	3	28	16	48	45	68	32	88	50	108	90
9	3	29	5	49	12	69	21	89	15	109	19
10	3	30	24	50	22	70	43	90	84	110	60
11	2	31	6	51	17	71	12	91	26	111	35
12	8	32	17	52	26	72	69	92	41	112	77
13	3	33	12	53	9	73	13	93	30	113	19
14	6	34	12	54	35	74	26	94	32	114	74
15	7	35	12	55	16	75	33	95	26	115	29
16	8	36	29	56	37	76	36	96	89	116	52
17	3	37	7	57	20	77	21	97	17	117	46
18	11	38	14	58	20	78	54	98	44	118	40
19	4	39	15	59	10	79	14	99	39	119	30
20	10	40	26	60	63	80	57	100	59	120	148
21	10	41	7	61	11	81	27	101	17	121	24
22	7	42	34	62	22	82	28	102	66		

These experimental data coincide with the bounds obtained in Section 4, when they are applicable.

$B_4(n)$ of distinct equivalence classes for a fixed n, which clearly represents an upper bound for the number $N_{\mathrm{tot},4}(n)$ of different values of the permanents, has been experimentally verified to satisfy, for n prime less or equal to 251, the formula

$$B_4(n) = \left\lceil \frac{(n-3)(n-5)}{24} \right\rceil + \left\lceil \frac{n-3}{4} \right\rceil$$

and it is conceivable to think that such formula holds for any prime $n \geqslant 5$. Moreover, we have verified that $N_{\mathrm{tot},4}(n) = B_4(n) - 1$ for $n = 7, 11, 13, 17$, $N_{\mathrm{tot},4}(n) = B_4(n)$ for $n = 5, 19, 23, 29, 31$, and we expect that $B_4(n) - N_{\mathrm{tot},4}(n) \leqslant 1$ holds also for any prime $n \geqslant 37$.

Similarly, in the case of $n \times n$ (0, 1)-circulant matrices with n prime and five or six nonzero entries per row, the numbers of different values of the permanents seem to satisfy the following inequalities:

$$N_{\mathrm{tot},5}(n) \leqslant \left\lceil \frac{(n+1)(n-3)(n-7)}{120} \right\rceil + \left\lceil \frac{n-3}{4} \right\rceil,$$

$$N_{\mathrm{tot},6}(n) \leqslant \left\lceil \frac{(n+1)(n-3)(n-5)(n-7)}{720} + \frac{(n-3)(n-5)}{24} + K(n) \right\rceil,$$

where $K(n) = (n-1)/9$ when $n \equiv 1 \pmod 3$ and $K(n) = 0$ otherwise.

We can thus enunciate the following conjecture.

Conjecture 1. *For any fixed* $k \in \mathbf{N},\ k \geqslant 3$, *and n ranging over the set of primes not lower than* k, *we conjecture that*

$$N_{\text{tot},k}(n) = \frac{n^{k-2}}{k!} + \mathrm{O}(n^{k-3}),$$

where $N_{\text{tot},k}(n)$ *is the number of different values for the permanents of* $n \times n$ $(0, 1)$-*circulant matrices with k nonzero entries per row.*

Returning to the case of matrices with three nonzero entries per row, a significant open problem is the following: in the present paper we lack tight upper bounds for matrices whose side is an arbitrary composite number, not of the forms studied in the previous section. In particular it would be interesting to analyze the cases in which $i, j, i - j \notin \mathbf{Z}_n^*$. In this cases it is not possible to draw as a "cycle + chords" the bipartite graph associated to the matrix and alternative representations should be studied.

Another interesting question might consist in determining lower bounds for the number of different values taken by the permanent, even in the cases in which n is prime. This face of the problem will probably require a completely different approach, since the isomorphism of the graphs associated to two matrices implies the equality of their permanents, while the converse is clearly not granted.

References

[1] A. Bernasconi, B. Codenotti, V. Crespi, G. Resta, How fast can one compute the permanent of circulant matrices? Linear Algebra Appl. 292 (1999) 15–37.

[2] B. Codenotti, V. Crespi, G. Resta, On the permanent of certain (0, 1) Toeplitz matrices, Linear Algebra Appl. 267 (1997) 65–100.

[3] B. Codenotti, G. Resta, Computation of sparse circulant permanents via determinants, Linear Algebra Appl. 355 (2002) 15–34.

[4] P. Dagum, M. Luby, M. Mihail, U. Vazirani, Polytopes, permanents and graphs with large factors, Proc. 29th IEEE Sympos. Found. Comput. Sci. (1988) 412–421.

[5] W.J. LeVeque, Fundamentals of Number Theory, Dover Publications, 1996.

[6] I. Niven, H.S. Zuckerman, An Introduction to the Theory of Numbers, John Wiley, 1980.

[7] H.J. Ryser, Combinatorial Mathematics, Carus Mathematical Monograph No. 14, 1963.

[8] L.G. Valiant, The complexity of computing the permanent, Theoret. Comput. Sci. 8 (1979) 189–201.

[9] L.G. Valiant, Completeness classes in algebra, ACM Sympos. Theory Comput. (1979) 249–261.