Computing the Bell Number by Using Gröbner Bases

Yongbin Li[1] *and Andrew Y.Z. Wang*[2]
[1]yongbinli@uestc.edu.cn and [2]yzwang@uestc.edu.cn
School of Mathematical Sciences
University of Electronic Science and Technology of China
Chengdu 611731
P.R. China

Abstract

In this paper, we show that the Bell number $B(n)$ counts the total number of zeros of certain polynomial set over the finite field $\mathbb{F}_2$. An alternative method for computing $B(n)$ is presented by using Gröbner bases. The new method makes a theoretical contribution to discuss the partitions of $[n]$ in Combinatorics by using Computer Algebra without considering the complexity. Given a zero of the polynomial set, we also give an approach to determine the type of the corresponding partition by computing the characteristic polynomial. Our method is also helpful to enhance the interest of learning Computer Algebra and using computer algebra systems in teaching and studying.

1 Introduction

There is a simple bijection between the equivalence relations $\sim$ on a set S and the partitions of S, viz., the equivalence classes of $\sim$ form a partition of S. We denote by Π_n the set of all partitions of the n-set $[n] := \{1, 2, \dots, n\}$. The total number of partitions of an n-set is called a *Bell number* and is denoted $B(n)$. Thus the cardinality of Π_n is $B(n)$. The following is a basic formula concerning $B(n)$ in Combinatorics,

$$B(n+1) = \sum_{i=0}^{n} \binom{n}{i} B(i), \quad n \geq 0.$$

See [3, 6] for more on $B(n)$.

Let $\mathbb{F}_2 = \{0, 1\}$ be the finite field with 2 elements and denote $\mathbb{F}_2^{n^2}$ the n^2-dimensional affine space, which consists of all vectors of length n^2 with entries in $\mathbb{F}_2$:

$$\mathbf{a} = (a_{1,1}, \dots, a_{1,n}, a_{2,1}, \dots, a_{2,n}, \dots, a_{n,1}, \dots, a_{n,n}).$$

For convenience, we identify the vector $\mathbf{a} \in \mathbb{F}_2^{n^2}$ with the matrix $A = (a_{i,j}) \in M_n(\mathbb{F}_2)$.

Let $\mathbb{F}_2[x_{i,j} \mid 1 \leq i, j \leq n]$ (or $\mathbb{F}_2[(x_{i,j})_{n\times n}]$) denote the ring of polynomials in n^2 variables $x_{i,j}$ over $\mathbb{F}_2$. It is sometimes convenient to write $f \in \mathbb{F}_2[(x_{i,j})_{n\times n}]$ as $f((x_{i,j}))$, and $f(A) \triangleq f(\mathbf{a})$ if $A = (a_{i,j}) \in \mathbb{F}_2^{n^2}$.

A *polynomial set* is a finite set $\mathbb{P}$ of nonzero polynomials in $\mathbb{F}_2[(x_{i,j})_{n\times n}]$. The set of all zeros of $\mathbb{P}$ in $\mathbb{F}_2^{n^2}$ is defined as

$$\mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}) \triangleq \{A=(a_{i,j})\in\mathbb{F}_2^{n^2} \mid f(A)=f((a_{i,j}))=0,\, \forall f\in\mathbb{P}\}.$$

In this paper, we construct a polynomial set $\mathbb{P}_n$ over $\mathbb{F}_2$ in order to discuss the partitions Π_n by the symbolic method. Using Gröbner basis, the Bell number $B(n)$ can be obtained by considering a quotient algebra determined by $\mathbb{P}_n$. When one compute the Gröbner basis with respect to a special term ordering, all $B(k)\,(2\le k\le n)$ can be obtained at the same time. Furthermore, given a zero of $\mathbb{P}_n$, we also present an approach to determine the type of the corresponding partition by computing the characteristic polynomial.

The complexity of our approach to compute the Bell number is mainly depended on computing Gröbner bases. It is not good in complexity compared with the above formula in Combinatorics.

The virtue of our approach is to make a theoretical contribution to discuss the partitions of $[n]$ in Combinatorics by using Computer Algebra. It is also helpful to motivate the interest of learning Computer Algebra and using computer algebra systems in teaching and studying.

2 Main Results

The following polynomial set constructed in $\mathbb{F}_2[(x_{i,j})_{n\times n}]$ plays a crucial role in this paper,

$$\mathbb{P}_n=\{x_{i,i}+1;\ x_{j,k}(x_{i,j}+x_{i,k});\ (x_{j,k}+1)x_{i,j}x_{i,k};\ x_{i,j}+x_{j,i};\ 1\le i<j<k\le n\}.$$

One can implement the following Maple procedure for finding $\mathbb{P}_n$.

```
PS:=proc(n)
  local i,j,k,x,S1,S2,S3,P;
    S1:={seq(x[k,k]+1,k=1..n)};
    S2 := ‘minus‘(‘mod‘({seq(seq(x[i,j]+x[j,i],i=1..n),j=1..n)},2),{0});
    S3:={};
    for k to n do for  j to k-1 do
       S3:=‘union‘(S3,{seq(x[j,k]*(x[i,j]+x[i,k]),i=1..j-1)})
       end do
    end do
    for k to n do for j to k-1 do
       S3:=‘union‘(S3,{seq(x[i,j]*x[i,k]*(1+x[j,k]),i=1..j-1)})
       end do
    end do
    P:=‘union‘(S1,S2,S3);
    eval(P)
  end proc;
```

Theorem 1 *The total number of zeros of* $\mathbb{P}_n$ *is* $B(n)$, *i.e.*, $B(n)=|\mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)|$.

Proof.

For any zero $A = (a_{i,j}) \in \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$, it is obvious that the matrix $A = (a_{i,j}) \in M_n(\mathbb{F}_2)$ satisfying that $A^T = A$ and

$$a_{i,i} = 1,\ a_{j,k}(a_{i,j} + a_{i,k}) = 0,\ (a_{j,k} + 1)a_{i,j}a_{i,k} = 0$$

for all $1 \leq i < j < k \leq n$.

To show $B(n) = |\mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)|$, we construct the following mapping $\Delta : \Pi_n \to \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$ defined by the i, jth entry of the matrix $\Delta(\beta)$ is 1 if i, j are in some common block of the partition $\beta \in \Pi_n$; 0 otherwise.

In order to claim that Δ is well-defined, let $\sim_\beta$ denote the equivalence relation on $[n]$ induced by the partition β. For convenience, let $\Delta(\beta) = A \in M_n(\mathbb{F}_2)$. The reflexivity and symmetry of $\sim_\beta$ imply that $a_{i,i} = 1$ and $a_{i,j} + a_{j,i} = 0$, respectively. The transitivity shows that $a_{i,k} = 1$ if $a_{i,j} = a_{j,k} = 1$, so $a_{j,k}(a_{i,j} + a_{i,k}) = 0$; and $a_{j,k} = 1$ if $a_{i,j} = a_{i,k} = 1$, so $(a_{j,k} + 1)a_{i,j}a_{i,k} = 0$. Thus our claim holds.

It remains to show that Δ is bijective. Given $A \in \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$, we define two elements $i, j \in [n]$ to be A-equivalent, denoted $i \sim_A j$, if $a_{i,j} = 1$ for $1 \leq i, j \leq n$. Now we check that $\sim_A$ is an equivalence relation. The reflexivity and symmetry follow from $a_{i,i} = 1$ and $a_{i,j} + a_{j,i} = 0$, respectively. The transitivity follows from $a_{j,k}(a_{i,j} + a_{i,k}) = 0$ and $(a_{j,k} + 1)a_{i,j}a_{i,k} = 0$. Thus $\sim_A$ is an equivalence relation on $[n]$. The equivalence classes of $\sim_A$ yield a partition of $[n]$. Therefore Δ is surjective.

Finally, suppose that we have $\Delta(\beta_1) = \Delta(\beta_2)$. It follows from the above definition that $\beta_1 = \beta_2$. Hence Δ is bijective, which completes the proof. ■

Example 2 Let $\mathbb{P}_3 = \{p_1, p_2, p_3, q_1, q_2, f_1, f_2\}$ with

$$\begin{array}{lll} p_1 = x_{1,1} + 1, & q_1 = x_{1,2} + x_{2,1}, & f_1 = x_{2,3}(x_{1,2} + x_{1,3}), \\ p_2 = x_{2,2} + 1, & q_2 = x_{1,3} + x_{3,1}, & f_2 = (x_{2,3} + 1)x_{1,2}x_{1,3}. \\ p_3 = x_{3,3} + 1, & q_3 = x_{2,3} + x_{3,2}, & \end{array}$$

We list all the zeros of $\mathbb{P}_3$ in the following

$$A_1 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, A_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}, A_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, A_4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, A_5 = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The correspondence between $A_i \in \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_3)$ and the partition β_i of [3] is as follows:

$$\begin{array}{lcl} A_1 & \longleftrightarrow & \beta_1 = \{\{1, 2, 3\}\} \in \Pi_3, \\ A_2 & \longleftrightarrow & \beta_2 = \{\{1\}, \{2, 3\}\} \in \Pi_3, \\ A_3 & \longleftrightarrow & \beta_3 = \{\{1, 3\}, \{2\}\} \in \Pi_3, \\ A_4 & \longleftrightarrow & \beta_4 = \{\{1\}, \{2\}, \{3\}\} \in \Pi_3, \\ A_5 & \longleftrightarrow & \beta_5 = \{\{1, 2\}, \{3\}\} \in \Pi_3. \end{array}$$

We proceed to give an alternative method to count $B(n)$ using Gröbner basis theory which was introduced and developed by Buchberger in [1]. We first introduce some necessary notations and known results.

For any polynomial set $\mathbb{P} \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ where $\mathbb{F}_q$ denotes the finite field with q elements, define $\mathbb{J}_\mathbb{P}$ to be the ideal generated by all elements of $\mathbb{P}$ and the polynomials $x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n$, i.e.,

$$\mathbb{J}_\mathbb{P} =< \mathbb{P} > + < x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n > .$$

It is easy to see that

Lemma 3 *The ideal $\mathbb{J}_\mathbb{P}$ is zero-dimensional for any polynomial set $\mathbb{P} \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_n]$.*

By the ring-theoretic version of the Chinese Remainder Theorem [5], one can easily prove the following result which can help us to obtain $|\mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)|$ without needing to compute all zeros of $\mathbb{P}_n$ in $\mathbb{F}_2^{n^2}$.

Proposition 4 *Let $\mathbb{P}$ be a polynomial set in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$. Then*

$$|\mathrm{Zero}_{\mathbb{F}_q}(\mathbb{P})| = \dim(\mathbb{F}_q[x_1, x_2, \ldots, x_n]/\mathbb{J}_\mathbb{P}).$$

Using a Gröbner basis, one can easily find an $\mathbb{F}_2$-linear basis for $\mathbb{F}_2[(x_{i,j})_{n\times n}]/\mathbb{J}_\mathbb{P}$ by Macaulay's Basis Theorem in [5].

Proposition 5 *With the above situation, let $\mathbb{G}$ be a Gröbner basis of $\mathbb{J}_\mathbb{P}$ with respect to some monomial order. Then an $\mathbb{F}_q$-linear basis of $\mathbb{F}_q[x_1, x_2, \ldots, x_n]/\mathbb{J}_\mathbb{P}$ is given by the set of monomials*

$$\{x_1^{k_1} \ldots x_n^{k_n} \mid \overline{x_1^{k_1} \ldots x_n^{k_n}}^{\mathbb{G}} = x_1^{k_1} \ldots x_n^{k_n}\}$$

which is called a Macaulay's basis of $\mathbb{F}_q[x_1, x_2, \ldots, x_n]/\mathbb{J}_\mathbb{P}$.

As an immediate consequence, let $\mathbb{J}_{\mathbb{P}_n} =< \mathbb{P}_n > + < x_{1,1}^2 - x_{1,1}, x_{1,2}^2 - x_{1,2}, \ldots, x_{n,n}^2 - x_{n,n} >$ in $\mathbb{F}_2[x_{i,j} \mid 1 \leq i, j \leq n]$, we have

Theorem 6 *For any positive integer n, let $\mathbb{G}$ be a Gröbner basis of $\mathbb{J}_{\mathbb{P}_n}$ with respect to some monomial order. Then*

$$B(n) = |\{x_{1,1}^{k_1} x_{1,2}^{k_2} \ldots x_{n,n}^{k_n} \mid \overline{x_{1,1}^{k_1} x_{1,2}^{k_2} \ldots x_{n,n}^{k_n}}^{\mathbb{G}} = x_{1,1}^{k_1} x_{1,2}^{k_2} \ldots x_{n,n}^{k_n}\}|.$$

We next give an illustration for $B(4)$.

Example 7 Let $\mathbb{P}_4 = \{p_1, \ldots, p_4, q_1, \ldots, q_6, f_1, \ldots, f_8\}$ with

$$\begin{array}{ll}
p_1 = x_{1,1} + 1, & q_6 = x_{3,4} + x_{4,3}, \\
p_2 = x_{2,2} + 1, & f_1 = x_{2,3}(x_{1,2} + x_{1,3}), \\
p_3 = x_{3,3} + 1, & f_2 = (x_{2,3} + 1)x_{1,2}x_{1,3}, \\
p_4 = x_{4,4} + 1, & f_3 = x_{2,4}(x_{1,2} + x_{1,4}), \\
q_1 = x_{1,2} + x_{2,1}, & f_4 = (x_{2,4} + 1)x_{1,2}x_{1,4}, \\
q_2 = x_{1,3} + x_{3,1}, & f_5 = x_{3,4}(x_{1,3} + x_{1,4}), \\
q_3 = x_{1,4} + x_{4,1}, & f_6 = (x_{3,4} + 1)x_{1,3}x_{1,4}, \\
q_4 = x_{2,3} + x_{3,2}, & f_7 = x_{3,4}(x_{2,3} + x_{2,4}), \\
q_5 = x_{2,4} + x_{4,2}, & f_8 = (x_{3,4} + 1)x_{2,3}x_{2,4}.
\end{array}$$

Hence

$$\mathbb{J}_{\mathbb{P}_4} =< p_1, \dots, p_4, q_1, \dots, q_6, f_1, \dots, f_8, x_{i,j}^2 - x_{i,j}, 1 \le i, j \le 4 > .$$

Using Maple, we can easily compute a Gröbner basis with respect to lex order where $x_{1,1} > x_{1,2} > x_{2,2} > x_{2,1} > x_{1,3} > x_{2,3} > x_{3,3} > x_{3,2} > x_{3,1} > x_{1,4} > x_{2,4} > x_{3,4} > x_{4,4} > x_{4,3} > x_{4,2} > x_{4,1}$ as follows:

$$\begin{aligned}\mathbb{G}_4 \;=\; \{ & x_{3,4}^2 + x_{3,4},\ x_{2,4}^2 + x_{2,4},\ x_{1,4}^2 + x_{1,4},\ x_{3,4}x_{2,3} + x_{3,4}x_{2,4} + x_{2,3} + x_{2,4}, \\ & x_{3,4} + x_{2,3} + x_{3,4}x_{2,4} + x_{2,3}x_{2,4},\ x_{2,3}^2 + x_{2,3},\ x_{3,4}x_{1,3} + x_{3,4}x_{1,4} + x_{1,3} + x_{1,4}, \\ & x_{3,4} + x_{1,3} + x_{3,4}x_{1,4} + x_{1,3}x_{1,4},\ x_{1,3}^2 + x_{1,3},\ x_{2,4}x_{1,2} + x_{2,4}x_{1,4} + x_{1,2} + x_{1,4}, \\ & x_{2,4} + x_{1,2} + x_{2,4}x_{1,4} + x_{1,2}x_{1,4},\ x_{2,3}x_{1,2} + x_{2,3}x_{1,3} + x_{1,2} + x_{1,3}, \\ & x_{2,3} + x_{1,2} + x_{2,3}x_{1,3} + x_{1,2}x_{1,3},\ x_{1,2}^2 + x_{1,2}\}.\end{aligned}$$

The following monomials constitute a Macaulay's basis of $\mathbb{F}_2[(x_{i,j})_{4\times 4}]/\mathbb{J}_{\mathbb{P}_4}$

$$1, x_{1,2}, x_{1,3}, x_{1,4}, x_{2,3}, x_{2,4}, x_{3,4}, x_{1,4}x_{2,4}x_{3,4}, x_{1,2}x_{3,4},$$
$$x_{1,3}x_{2,3}, x_{1,3}x_{2,4}, x_{1,4}x_{2,3}, x_{1,4}x_{2,4}, x_{1,4}x_{3,4}, x_{2,4}x_{3,4}.$$

Thus, $B(4) = 15$.

Using Maple, the following commands are implemented for computing $B(4)$ in the above example.

```
with(Groebner):
G4:=Basis(JP4,plex(x[1,1],x[1,2],x[1,3],x[1,4],x[2,1],x[2,3],x[2,4],x[3,1],
    x[3,2],x[3,3],x[3,4],x[4,1],x[4,2],x[4,3],x[4,4]),characteristic=2):
N4:=NormalSet(G4,plex(x[1,1],x[1,2],x[1,3],x[1,4],x[2,1],x[2,3],x[2,4],x[3,1],
    x[3,2],x[3,3],x[3,4],x[4,1],x[4,2],x[4,3],x[4,4])):
B4:=nops(N4[1]);
 15.
```

Based on the next result, we can obtain all $B(k)$ for $2 \le k < n$ when a Gröbner basis of $\mathbb{J}_{\mathbb{P}_n}$ with respect to the given lex order.

Theorem 8 *For any positive integer $n > 2$, if $\mathbb{MB}_n$ is the collection of a Macaulay's basis of $\mathbb{F}_2[(x_{i,j})_{n\times n}]/\mathbb{J}_{\mathbb{P}_n}$, then*

$$B(k) = |\mathbb{F}_2[(x_{i,j})_{k\times k}] \cap \mathbb{MB}_n|$$

for $2 \le k < n$.

Proof. Suppose that $\mathbb{G}_n$ is a Gröbner basis of $\mathbb{J}_{\mathbb{P}_n}$ with respect to the above term ordering. It follows from the Elimination Theorem in [2] that the following set is the Gröbner basis of $\mathbb{J}_{\mathbb{P}_k}$

$$\mathbb{G}_n \cap \mathbb{F}_2[(x_{i,j})_{k\times k}]$$

for $2 \le k < n$. Note that all monomials of $\mathbb{MB}_n$ is the Macaulay's basis of $\mathbb{F}_2[(x_{i,j})_{n\times n}]/\mathbb{J}_{\mathbb{P}_n}$. We have that all elements of $\mathbb{F}_2[(x_{i,j})_{k\times k}] \cap \mathbb{MB}_n$ is an $\mathbb{F}_2$-basis of $\mathbb{F}_2[(x_{i,j})_{k\times k}]/\mathbb{J}_{\mathbb{P}_k}$. Thus

$$B(k) = |\mathbb{F}_2[(x_{i,j})_{k\times k}] \cap \mathbb{MB}_n|.$$

■

Example 9 (*Continued to Example 7*) We know that $\mathbb{G}_4 \cap \mathbb{F}_2[(x_{i,j})_{3\times 3}]$ is a Gröbner basis of $\mathbb{J}_{\mathbb{P}_4}$ by the Elimination Theorem. Thus we can get a Macaulay's basis of $\mathbb{F}_2[(x_{i,j})_{3\times 3}]/\mathbb{J}_{\mathbb{P}_3}$ as follows,

$$\mathbb{F}_2[(x_{i,j})_{3\times 3}] \cap \mathbb{MB}_4 = \{1,\ x_{1,2},\ x_{1,3},\ x_{2,3},\ x_{1,3}x_{2,3}\}.$$

This implies $B(3) = 5$.

The complexity of our approach to compute the Bell number mainly depends on computing Gröbner bases. Applying the efficient algorithm for computing Gröbner bases such as F_5 in [4], $B(n)$ can be computed when n is larger by our approach. Theorem 6 is also advantageous to estimate for the Gröbner basis of $\mathbb{J}_{\mathbb{P}_n}$ and the Macaulay's basis of $\mathbb{F}_2[(x_{i,j})_{n\times n}]/\mathbb{J}_{\mathbb{P}_n}$ if n is very large using the method of Combinatorics.

3 Other Results

Now we identify the set $\mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$ as a subset of the matrix ring $M_n(\mathbb{F}_2)$.

Given a matrix $A = (a_{i,j}) \in \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$, let $\mathbf{r}_i$ denote the ith row vector of A. It is clear that the ith position $\mathbf{r}_{ii}$ of $\mathbf{r}_i$ is 1. If $\mathbf{r}_{ii}$ is the first position of $\mathbf{r}_i$ equalling 1, i.e., i is the smallest integer j with $\mathbf{r}_{ij} = 1$, we record the column index j such that $\mathbf{r}_{ij} = 1$, assuming they are

$$c_1, c_2, \ldots, c_{s_i}.$$

Then the submatrix whose entries are a_{ij} where $i, j \in \{c_1, c_2, \ldots, c_{s_i}\}$ is a all-one matrix of order s_i, called a *block* of size s_i.

For every such i, we can determine a block of A. Suppose there are α_i blocks of size i in A, then A is called a matrix of *type* $1^{\alpha_1}2^{\alpha_2}\cdots n^{\alpha_n}$ where $\sum i\alpha_i = n$ and $\alpha_i \geq 0$ for each i.

Example 10 Given a matrix $A \in \Gamma_4$,

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix},$$

the entries $a_{2,2}, a_{2,4}, a_{4,2}, a_{4,4}$ form a block of size 2 and the type of A is $1^2 2^1 3^0 4^0$.

It is easy to see that two elements $A, B \in \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$ have the same type if and only if they are *conjugate* in $\mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$, i.e., there exists a permutation matrix $Q \in S_n$ such that $A = QBQ^T$, where S_n is the symmetric group.

Lemma 11 *Assume that n is a fixed positive integer, then Π_n and $\mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$ are S_n-sets.*

Proof. It is easy to check that the following map Φ establishes an action on Π_n

$$\Phi:\ S_n \times \Pi_n \longrightarrow \Pi_n,\ (Q, \beta) \longrightarrow Q \star \beta \triangleq \bigcup_k \{Q(i) \mid i \in B_k\},$$

with $\beta = \bigcup_k B_k \in \Pi_n$ which implies that Π_n is an S_n-set.

To show that $\mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$ is an S_n-set, we claim that $QAQ^T \in \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$ for any $Q \in S_n$ and $A \in \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$.

For any $f((x_{i,j})) \in \mathbb{P}_n$, it is easy to see that $f(Q(x_{i,j})Q^T) \in \mathbb{P}_n$ by the symmetry of $\mathbb{P}_n$. Assume that $A \in \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$, then A is a zero of $f(Q(x_{i,j})Q^T)$ since $f(Q(x_{i,j})Q^T) \in \mathbb{P}_n$. Thus for any $f((x_{i,j})) \in \mathbb{P}_n$, we have $f(QAQ^T) = 0$, which means that $QAQ^T \in \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$.

Thus the following map

$$\Psi : S_n \times \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n) \longrightarrow \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n),\ (Q, A) \longrightarrow Q \circ A \triangleq QAQ^T$$

shows that $\mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$ is also an S_n-set. ■

Furthermore we have

Proposition 12 *Given an integer $n > 0$, we have Π_n and $\mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$ are isomorphic S_n-sets.*

Proof. In the proof of Theorem 1, we know that $\Delta : \Pi_n \to \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$ is bijective. It remains to show that Δ is also an S_n-isomorphic map. For any $Q \in S_n$ and $\beta = \bigcup_k B_k \in \Pi_n$, with the same notations in the proof of Lemma 11, we have

$$\Delta(Q \star \beta) = \Delta(\bigcup_k \{Q(i) \mid i \in B_k\}) = QAQ^T = Q \circ \Delta(A).$$

This completes the proof. ■

Let $\mathbb{R}$ denote the real number field. Now we establish the following map

$$\Psi : M_n(\mathbb{F}_2) \to M_n(\mathbb{R})$$

$$A = (a_{i,j}) \mapsto (\bar{a}_{i,j})$$

with $\bar{a}_{i,j} = 1$ if $a_{i,j} = 1$; $\bar{a}_{i,j} = 0$ else.

And for a matrix $C \in M_n(\mathbb{R})$, the characteristic polynomial of C is denoted $\mathrm{ch}(C)$.

Theorem 13 *For $A \in \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$, if*

$$\mathrm{ch}(\Psi(A)) = x^m(x-1)^{k_1}(x-2)^{k_2} \cdots (x-n)^{k_n},$$

where $m, k_i \geq 0$, then A has exactly k_i blocks of size i for $i = 1, 2, \ldots, n$.

Proof. Given a matrix $A = (a_{i,j}) \in \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_n)$, $\Psi(A)$ is conjugate to a block diagonal matrix C by Proposition 12, i.e., there exists some $Q \in S_n$ such that

$$C = Q\Psi(A)Q^T = \mathrm{diag}(C_1, C_2, \ldots, C_s),$$

where $C_i \in M_{n_i}(\mathbb{R})$ is a all-one matrix.

Since $\mathrm{ch}(C_i) = x^{n_i - 1}(x - n_i)$ and $\mathrm{ch}(C) = \mathrm{ch}(C_1)\mathrm{ch}(C_2)\cdots\mathrm{ch}(C_s) = \mathrm{ch}(A)$, we have that there exist exactly k_i blocks of size i in C. Then the desired result follows from the fact that $\Psi(A)$ and C have the same type. ■

Example 14 Let

$$A_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, A_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \in \mathrm{Zero}_{\mathbb{F}_2}(\mathbb{P}_4).$$

It is easy to check that

$$\mathrm{ch}(\Psi(A_1)) = \mathrm{ch}(\Psi(A_2)) = x(x-1)^2(x-2).$$

Thus both A_1 and A_2 have two blocks of size 1 and one block of size 2.

Acknowledgement 15 *This work was supported by National Natural Science Foundation of China (Grant No. 11401080,61272175,61572109). The authors would like to thank the referees for their helpful comments, and to Prof. Thomas Sturm, Dr. Maximilian Jaroschek, Dr. Chenqi Mou and Dr. Changbo, Chen for their helpful suggestions at the CDZ Workshop GZ1115.*

References

[1] B. Buchberger, Gröbner bases: An algorithmic method in polynomial ideal theory, Chapter 6 in: Multidimensional Systems Theory (N.K. Bose, Ed.), 184–232, D. Reidel Publishing Company, 1985.

[2] D. Cox, J. Little and D. O'Shea, Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, Springer, 2006.

[3] L. Comtet, Advanced Combinatorics, D. Reidel Publishing Company, 1974.

[4] J. Faugére, A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5), In: *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation.* ACM Press, New York, 2002, 75–83.

[5] M. Kreuzer and L. Robbiano, Computational Commutative Algebra 1, Springer, 2000.

[6] R. Stanley, Enumerative Combinatorics, Vol 1, Cambridge University Press, 2012.