Discrete Mathematics 69 (1988) 225–234
North-Holland

SYMMETRIC POLYNOMIALS AND HALL'S THEOREM

Klaus G. FISCHER
~~Department of Mathematics, University of Illinois, 1409 West Green Street,~~
~~Urbana, IL 61801, U.S.A.~~

Department of Math
George Mason Univ.
Fairfax, Virginia

Received 12 June 1986
Revised 10 March 1987

If $A[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ is a polynomial ring over the commutative unitary ring A, let $\mathcal{P}$ be the ideal which vanishes on the points $(x, \sigma(x))$ in $A^{(2\cdot n)}$ for any elementary symmetric polynomial σ. It is shown that this ideal is generated by the differences of the elementary symmetric polynomials in X and Y which in consequences gives another proof of the classical result concerning symmetric polynomials. Furthermore, by associating to a complete bipartite graph on n vertices a polynomial in $\mathcal{P}$, a purely algebraic proof of the Phillip Hall matching theorem is given.

1. Introduction

Let A be a commutative ring with 1 and let $A[X, Y]$ be the polynomial ring in $2 \cdot n$ variables where $X := X_1, \ldots, X_n$ and $Y := Y_1, \ldots, Y_n$. Consider the ideal $\mathcal{P}$ in $A[X, Y]$ generated by those polynomials $P(X, Y)$ which vanish for any substitution of the Y's by some permutation of the X's. That is, those $P(X, Y)$ for which $P(X, s(X)) = 0$ for all $s \in S_n$.

In particular, let $\sigma_k(Z_1, \ldots, Z_n)$ be the kth elementary symmetric polynomial in n variables defined by

$$\sigma_k(Z_1, \ldots, Z_n) = \sum_{i_1 < \cdots < i_k} Z_{i_1} \cdots Z_{i_k}, \quad \text{for } k = 1, \ldots, n.$$

Then for each such k, $\sigma_k(X) - \sigma_k(Y)$ is a polynomial with the above described property.

Let $\mathcal{D}$ be the ideal in $A[X, Y]$ generated by these differences of the elementary symmetric polynomials. Hence

$$\mathcal{D} = \langle \sigma_k(X) - \sigma_k(Y): k = 1, 2, \ldots, n \rangle.$$

Why?

In Section 2 it is shown that the ideal $\mathcal{D} = \mathcal{P}$. An easy consequence is the well-known theorem that any symmetric polynomial in n variables is a polynomial in the elementary symmetric polynomials.

Section 3 considers a combinatorial property of this ideal $\mathcal{P}$. Given a biparitite graph G on two disjoint sets of n vertices, associate with it a polynomial $P(X, Y)$ defined by

$$P(X, Y) = \prod_{(i,j) \in G} (X_i - Y_j).$$

Here, the product is taken over those i, j for which edge (i, j) is in G. It is shown that $P(X, Y)$ belongs to the ideal $\mathscr{P}$ iff G contains a complete bipartite graph $K_{s,t}$ for which $s+t>n$. This result, applied to the associated polynomial $\bar{P}$ of the complimentary bipartite graph $\bar{G}$, gives another proof of Hall's matching theorem. Furthermore, an equivalent formulation of this theorem in terms of ideals in $\mathbb{Z}[X, Y]$ is proved.

2. The ideal $\mathscr{D}$

For any $s \in S_n$, let

$$\mathscr{P}_s = \langle (X_1 - Y_{s(1)}), \dots, (X_n - Y_{s(n)}) \rangle.$$

As long as A is a domain, $\mathscr{P}_s$ is a prime ideal in $A[X, Y]$. Clearly, $P(X, s(X)) = 0$ iff $P(X, Y) \in \mathscr{P}_s$ and therefore $\mathscr{P} = \bigcap_{s \in S_n} \mathscr{P}_s$. Theorem 1 will show that $\mathscr{D} = \bigcap_{s \in S_n} P_s$. Hence, $\mathscr{D} = \mathscr{P}$ and if the ideals $\mathscr{P}_s$ are prime, then $\mathscr{D}$ and $\mathscr{P}$ are radical ideals.

Given the variables $X_1, \dots, X_n$ and Z, the product expansion

$$\prod_{j=1}^{n} (Z - X_j) = Z^n - Z^{n-1}\sigma_1(X) + \cdots + (-1)^n \sigma_n(X) \tag{1}$$

shows that for any j,

$$X_j^n = X_j^{n-1}\sigma_1(X) - \cdots + (-1)^{n-1}\sigma_n(X). \tag{2}$$

Identical relations hold for the variables $Y_1, \dots, Y_n$. Replacing Z by Y_n in Eq. (1) we have

$$\prod_{j=1}^{n} (Y_n - X_j) = Y_n^n - Y_n^{n-1}\sigma_1(X) + \cdots + (-1)^n \sigma_n(X).$$

Substituting the expansion for Y_n^n in terms of $\sigma_k(Y)$ as given by Eq. (2) with X replaced by Y we have

$$\prod_{j=1}^{n} (Y_n - X_j) = Y_n^{n-1}[\sigma_1(Y) - \sigma_1(X)] - Y_n^{n-2}[\sigma_2(Y) - \sigma_2(X)]$$
$$+ \cdots + (-1)^{n-1}[\sigma_n(Y) - \sigma_n(X)].$$

This establishes an identity to be used in the proof of the first theorem.

Theorem 1. *Suppose* $P(X, Y) \in A[X, Y]$, *where* $X := X_1, \dots, X_n$, $Y := Y_1, \dots, Y_n$ *and* A *is a commutative ring. If* $P(X, s(X)) = 0$ *for all permutations* $s \in S_n$ *of* $X_1, \dots, X_n$, *then*

$$P(X, Y) = \sum_{k=1}^{n} a_k[\sigma_k(X) - \sigma_k(Y)],$$

where σ_k *is the* kth *elementary symmetric polynomial in* n *variables and* $a_k \in A[X, Y]$.

Proof. If $n = 1$, then by the Euclidean algorithm

$$P(X, Y) = (Y - X)H(X, Y) + P(X, X) = (Y - X)H(X, Y),$$

for some $H \in A[X, Y]$. Since $\sigma_1(X) - \sigma_1(Y) = X - Y$, the result follows in this case.

Now let $n > 1$ and assume that we have already shown that

$$P(X, Y) \equiv (Y_n - X_1) \cdots (Y_n - X_{j-1})H(X, Y) \pmod{\mathscr{D}},$$

for $1 \leqslant j \leqslant n+1$ and where $\mathscr{D}$ is the ideal of differences. (If no factor appears in the above then $j = 1$.) If $j = n+1$, then by the identity established before the theorem the result will follow.

We have $H(X, Y) = (Y_n - X_j)Q(X, Y) + R(X, Y)$ where the remainder $R(X, Y) = H(X_1, \dots, X_n, Y_1, \dots, Y_{n-1}, X_j)$ contains no Y_n. Hence

$$P(X, Y) \equiv (Y_n - X_1) \cdots (Y_n - X_j)Q(X, Y)$$
$$+ (Y_n - X_1) \cdots (Y_n - X_{j-1})R(X, Y).$$

Observe that $R(X, Y)$ vanishes for all substitutions of $Y_1, \dots, Y_{n-1}$ by a permutation $s^* \in S_{n-1}$ of $X_1, \dots, \hat{X}_j, \dots, X_n$ (X_j omitted). This is so since the result of setting $Y_n = X_j$ in $P(X, Y)$ along with the above substitutions, is equal to $P(X, s(X))$ where $s \in S_n$ is the extension of s^*. Hence, the above equation yields

$$0 = P(X, s(X)) = 0 + (X_j - X_1) \cdots (X_j - X_{j-1})R(X, s^*(X)).$$

Therefore R satisfies the hypothesis of the theorem in the variables $X_1, \dots, \hat{X}_j, \dots, X_n, Y_1, \dots, Y_{n-1}$ and coefficients in $A[X_j]$. By the inductive hypothesis it is a linear combination of terms

$$\sigma_k(X_1, \dots, \hat{X}_j, \dots, X_n) - \sigma_k(Y_1, \dots, Y_{n-1}), \quad k = 1, \dots, n-1.$$

If these are denoted by $\sigma_k(\hat{X}) - \sigma_k(\hat{Y})$, then

$$\sigma_k(\hat{X}) - \sigma_k(\hat{Y}) = [\sigma_k(X) - \sigma_k(Y)] - [X_j\sigma_{k-1}(\hat{X}) - Y_n\sigma_{k-1}(\hat{Y})]$$
$$= [\sigma_k(X) - \sigma_k(Y)] - \sigma_{k-1}(\hat{X})[X_j - Y_n] - Y_n[\sigma_{k-1}(\hat{X}) - \sigma_{k-1}(\hat{Y})].$$

Applying the same expansion on $\sigma_{k-1}(\hat{X}) - \sigma_{k-1}(\hat{Y})$ it follows that for $k = 1, \dots, n-1$, $\sigma_k(\hat{X}) - \sigma_k(\hat{Y}) \equiv 0 \pmod{\langle \mathscr{D}, Y_n - X_j \rangle}$. Hence, modulo $\mathscr{D}$, R contains a factor of $(Y_n - X_j)$ and we may write

$$R \equiv F(X, Y)(Y_n - X_j) \pmod{\mathscr{D}} \text{ and so obtain}$$
$$P(X, Y) \equiv (Y_n - X_1) \cdots (Y_n - X_j)[Q(X, Y) - F(X, Y)] \pmod{\mathscr{D}}$$

as we wanted to show. $\square$

If $P(X)$ is a symmetric polynomial in the ring $A[X_1, \dots, X_n]$ then it is well known that P may be written as a polynomial in the elementary polynomials $\sigma_k(X)$, $k = 1, \ldots, n$. This fact can be obtained easily from the above theorem, at least in the case when A equals the rationals $\mathbb{Q}$, by induction on the degree of P in the following way.

We may assume that P is homogeneous and if it is of degree 1 and symmetric, then $P(X) = a \cdot \sigma_1(X_1, \ldots, X_n)$ for some $a \in A$. If the degree of $P(X)$ is $d > 1$, then introduce the variables $Y_1, \ldots, Y_n$ and note that $P(X) - P(Y) \in A[X, Y]$ satisfies the hypothesis of the theorem. Hence

$$P(X) - P(Y) = \sum_{k=1}^{n} a_k[\sigma_k(X) - \sigma_k(Y)],$$

and setting $Y_1 = \cdots = Y_n = 0$, we see that

$$P(X) = \sum_{k=1}^{n} b_k \cdot \sigma_k,$$

where $b_k = a_k(X, 0)$ and is homogeneous of degree $n - d < n$. These b_k may not be symmetric. However, if we let $b_k^{(s)} = b_k(s(X))$, where $s \in S_n$ is a permutation of $X_1, \ldots, X_n$, then $B_k = \sum_{s \in S_n} b_k^{(s)}$ is symmetric and homogeneous of degree $n - d$. Since

$$P^{(s)}(X) = P(X) \quad \text{and} \quad \sigma_k^{(s)} = \sigma_k \quad \text{for any } s,$$

we have that

$$n!\, P(X) = \sum_{k=1}^{n} B_k \sigma_k(X).$$

Hence, the inductive hypothesis applied to B_k gives the result in the case that A contains the rationals.

Another inductive argument gives the more general result.

Corollary. *If $F(X)$ is a symmetric polynomial in $A[X_1, \ldots, X_n]$, where A is a commutative ring with 1, then $F(X) = P(\sigma_1, \ldots, \sigma_n)$, where $\sigma_1, \ldots, \sigma_n$ are the elementary polynomials and $P(T_1, \ldots, T_n)$ is a polynomial in $A[T_1, \ldots, T_n]$.*

Proof. First we assume that A is the ring of integers. By the discussion following the theorem, we know $m \cdot F(x) = P(\sigma_1, \ldots, \sigma_n)$ for some positive integer m. We claim that m divides the coefficients of P so that $F(X) = P'(\sigma_1, \ldots, \sigma_n)$ for some $P' \in \mathbb{Z}[T_1, \ldots, T_n]$, where $\mathbb{Z}$ is the ring of integers.

We may assume that $F(x)$ is homogeneous and then the result is clear if $n = 1$. It also holds, regardless of n, when $d = \deg F = 1$. Assume then, that the result holds for symmetric polynomials in less than n variables and also for those in any number of variables but for which $\deg P < d$.

We may write

$$m \cdot F(X) = P(\sigma_1, \ldots, \sigma_n) = Q(\sigma_1, \ldots, \sigma_{n-1}) + \sigma_n R(\sigma_1, \ldots, \sigma_n) \qquad (*)$$

If we set $X_n = 0$, then for $1 \leqslant k \leqslant n - 1$, $\hat{\sigma}_k = \sigma_k(X_1, \ldots, X_{n-1}, 0)$ is the kth elementary symmetric polynomial of the variables $X_1, \ldots, X_{n-1}$. Since $\sigma_n(X_1, \ldots, X_{n-1}, 0) = 0$, Eq. (*) gives

$$m \cdot F(X_1, \ldots, X_{n-1}, 0) = Q(\hat{\sigma}_1, \ldots, \hat{\sigma}_{n-1}).$$

By induction, m divides Q so that we may rewite (*) as $m \cdot [F(X) - Q'(\sigma_1, \ldots, \sigma_{n-1})] = \sigma_n R(\sigma_1, \ldots, \sigma_n)$, where $m \cdot Q' = Q$. But since $\sigma_n = X_1 \cdots X_n$, and $\mathbb{Z}[X]$ is a UFD, σ_n must divide the left side of this last equation and hence we may write

$$m \cdot F'(X) = R(\sigma_1, \ldots, \sigma_n), \quad \text{for some } F'(X).$$

Evidently, $F'(x)$ is symmetric and $\deg F' < d = \deg F$. The inductive assumption on this degree says m divides R. Since m divides Q also, Eq. (*) says m divides P.

Now let A be arbitrary. Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ be an n-tuple of nonnegative integers and write $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$. If $F(X) \in A[X]$ is symmetric and contains the term aX^α, $0 \neq a \in A$, then it must also contain the term $aX^{s(\alpha)}$, where $s \in S_n$. So if $[\alpha]$ is the equivalence class of n-tuples induced by s, $F(X)$ must contain the symmetric sum

$$a \cdot \sum_{\alpha \in [\alpha]} X^\alpha.$$

Since $F(x)$ can be written as the sum (over distinct equivalence classes) of such terms, it suffices to show the result for symmetric polynomials

$$F(x) = \sum_{\alpha \in [\alpha]} X^\alpha.$$

Over the integers such as expression can be written as $P(\sigma_1, \ldots, \sigma_n)$ for some P. Hence, if $\lambda = \operatorname{char} A$,

$$F(x) = \bar{P}(\sigma_1, \ldots, \sigma_n),$$

where $\bar{P}$ is the image of P in

$$\frac{\mathbb{Z}}{(\lambda)}[X] \subset A[X]. \qquad \square$$

Remark 1. We may use this last corollary to sharpen the result of Theorem 1. That is, assume $F(X, Y)$ vanishes for all substitutions of Y by permutations of X. Then

$$F(X, Y) = \sum a_k[\sigma_k(X) - \sigma_k(Y)].$$

But furthermore, if F is symmetric in (say) $Y_1, \ldots, Y_n$, then we may find a_k's in the above equation which are symmetric in $Y_1, \ldots, Y_n$.

To see this, note that by the corollary $F(X, Y) = P(\sigma_1(Y), \ldots, \sigma_n(Y))$, for some $P \in A[X_1, \ldots, X_n][Z]$. But since $P(\sigma_1(X), \ldots, \sigma_n(X)) = 0$, one computes directly that

$$F(X, Y) = P(\sigma_1(X), \ldots, \sigma_n(X)) - P(\sigma_1(Y), \ldots, \sigma_n(Y))$$
$$= \sum a_k[\sigma_k(X) - \sigma_k(Y)],$$

where the a_k's are polynomials in the $\sigma_k(Y)$'s with coefficients in $A[X_1, \ldots, X_n]$. Hence, they are symmetric in $Y_1, \ldots, Y_n$.

Remark 2. Let $\mathcal{S}$ be the ideal in $A[X, Y]$ generated by differences of sums so that

$$\mathcal{S} = \left\langle \sum_{i=1}^{n} X_i^k - \sum_{i=1}^{n} Y_i^k : k = 1, 2, \ldots \right\rangle.$$

The theorem shows that $\mathcal{S} \subset \mathcal{D}$. Furthermore, Newton's identities [1, p. 135] state that for $k \leq n$, and the summation taken over $i = 1, \ldots, k$,

$$0 = k\sigma_k - (\sum X_i)\sigma_{k-1} + (\sum X_i^2)\sigma_{k-2} + \cdots + (-1)^k(\sum X_i^k).$$

Since $\sum X_i = \sigma_1(X)$, there show by induction that $\sigma_k(X) = P(\sum X_i, \ldots, \sum X_i^n)$, where P is a polynomial with rational coefficients. Hence, over the rationals $\mathbb{Q}$,

$$\sigma_k(X) - \sigma_k(Y) \in \mathcal{S} \cdot \mathbb{Q}[X, Y]$$

and so $\mathcal{S} = \mathcal{D}$ in $\mathbb{Q}[X, Y]$.

3. The polynomial associated to a graph

Given a bipartite graph G on two disjoint copies of $[n] = \{1, \ldots, n\}$ as vertex-set, we may associate with G a polynomial in $\mathbb{Z}[X, Y]$ which is the product of terms $X_i - Y_j$ for all edges (i, j) in the graph.

Definition. For a bipartite graph G let

$$P(X, Y) = \prod_{(i,j) \in G} (X_i - Y_j)$$

be the associated polynomial of G. Furthermore, if a and b are non-empty sets of $[n]$, let

$$P_{a,b} = \prod_{(i,j) \in a \times b} (X_i - Y_j).$$

Then $P_{a,b}$ is the polynomial associated to the complete bipartite graph $K_{|a|,|b|}$.

Example. If $X := X_1, X_2, X_3$, $Y := Y_1, Y_2, Y_3$, $a = \{2, 3\}$, and $b = \{1, 3\}$, then $P_{a,b} = (X_2 - Y_1)(X_2 - Y_3)(X_3 - Y_1)(X_3 - Y_3)$.
Note in this case that $P_{a,b} \in \mathcal{P}$.

Lemma 1. *If $|a| + |b| = n + 1$, then $P_{a,b} \in \mathcal{P}$.*

Proof. Substituting for the Y's by some permutation of the X's requires choosing a subset of $|b|$ elements from the set $\{X_1, \ldots, X_n\}$. Since $|a| + |b| = n + 1$, such a choice would of necessity include an X_i where $i \in a$. Hence, $P(X, s(X)) = 0$ for all $s \in S_n$ and the conclusion follows from the definition of $\mathcal{P}$. □

Let $\mathcal{M}$ be the ideal generated by all polynomials $P_{a,b}$ with $|a| + |b| = n + 1$. Lemma 1 shows that $\mathcal{M} \subset \mathcal{P}$.

Lemma 2. *Let $(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)$ be a point in K^{2n}, where K is an algebraic extension field of $\mathbb{Q}$. If the point (α, β) is a zero of all polynomials in $\mathcal{M}$, then $(\beta_1, \ldots, \beta_n) = s(\alpha_1, \ldots, \alpha_n)$, for some $s \in S_n$. Consequently, the algebraic point set of $\mathcal{M}$ and $\mathcal{P}$ agree.*

Proof. We do this by induction on n. If $n = 1$, then $\mathcal{M} = \langle X_1 - Y_1 \rangle$ and hence, $\alpha_1 - \beta_1 = 0$. Suppose the result is true for $k < n$. Since (α, β) satisfies $(X_1 - Y_1) \cdots (X_1 - Y_n)$, it follows that $\beta_{j_0} = \alpha_1$ for some β_{j_0}. Since the object is to find some $s \in S_n$ so that $s(\alpha) = \beta$, it is harmless to renumber and assume that $\beta_{j_0} = \beta_1$, $\beta_1 = \alpha_1 = \cdots = \alpha_t$, and that $\beta_1 \neq \alpha_i$ for $i > t$. Since (α, β) satisfies

$$(X_1 - Y_2) \cdots (X_1 - Y_n)(X_2 - Y_2) \cdots (X_2 - Y_n)$$

then if $t > 1$ it follows (after renumbering) that $\beta_2 = \beta_1 = \alpha_1$. If it has already been shown that $\alpha_1 = \beta_1 = \cdots = \beta_s$, $s < t$, then since (α, β) satisfies $P_{a,b}$, where $a = \{1, \ldots, s+1\}$ and $b = \{s+1, \ldots, n\}$, it follows that after renumbering, $\alpha_1 = \beta_1 = \cdots = \beta_{s+1}$. Hence we may assume that $\alpha_1 = \cdots = \alpha_t = \beta_1 = \cdots = \beta_t$ and that this common value does not equal any α_i for $i > t$. Now let $a', b' \subset \{t+1, \ldots, n\}$, where $|a'| + |b'| = n - t + 1$. Then $P_{a',b'}$ is satisfied by $(\alpha_{t+1}, \ldots, \alpha_n, \beta_{t+1}, \ldots, \beta_n)$ since the point (α, β) satisfies

$$P_{a',b'} \cdot \prod_{i \in a'} (X_i - Y_1) \cdots (X_i - Y_t).$$

The first statement in the lemma now follows since by the inductive assumption, $\beta_{t+1}, \ldots, \beta_n$ is a permutaion of $\alpha_{t+1}, \ldots, \alpha_n$.
Since $\mathcal{M} \subset \mathcal{P}$, any zero (α, β) of the ideal $\mathcal{P}$ must be one of $\mathcal{M}$ and the result follows. □

Since the preceding lemma shows that the zero points in some algebraic extension of $\mathbb{Q}$, of the ideals $\mathcal{M}$ and $\mathcal{P}$ agree, it follows by a slight generalization of the Nullstellensatz [2, p. 285], that the radicals of $\mathcal{M}$ and $\mathcal{P}$ agree in $\mathbb{Q}[X, Y]$. This means that $\mathcal{P}^m \subset \mathcal{M}$ for some positive integer m. The lemma also shows that since the ideal $\mathcal{S}$ defined in Remark 2 of Section 2 also equals $\mathcal{P}$ in $\mathbb{Q}[X, Y]$, the zero point set of $\mathcal{S}$ is also that of $\mathcal{M}$ and explicitly consists of points $(\alpha, s(\alpha))$ for any $\alpha \in K^n$ and $s \in S_n$.

Lemma 3. *Let A be a unique factorization domain or a field. Suppose $M, M_1, \ldots, M_r$ are monomials in the ring $A[X, Y]$ of the form*

$$\prod_{(i,j)\in\Lambda} (X_i - Y_j), \quad \text{where } \Lambda \subset [n] \times [n].$$

If $M = c_1M_1 + \cdots + c_rM_r$ for $c_i \in A[X, Y]$, then M_j divides M for some j.

Proof. If $M = c_1M_1$, then clearly $M_1 \mid M$ since $A[X, Y]$ is also a UFD. Assume the result is true for sums of fewer than r terms. If M_1 does not divide M, then some factor $(X_s - Y_t)$ of M_1 fails to divide M. After reordering, we may assume that $(X_s - Y_t)$ divides only M_i for $i = 1, \ldots, k$, where $1 \leq k < r$. It follows that in $A[X, Y]/(X_s - Y_t)$,

$$\bar{M} = \bar{c}_{k+1}\bar{M}_{k+1} + \cdots + \bar{c}_r\bar{M}_r.$$

This ring satisfies the hypothesis of the theorem and therefore by induction, $\bar{M}_j \mid \bar{M}$ for some j, $k+1 \leq j \leq r$. This says that for any factor $(X_u - Y_v)$ of M_j there must be a factor $(X_e - Y_f)$ of M for which

$$(X_e - Y_f) \equiv (X_u - Y_v) \pmod{(X_s - Y_t)}.$$

The only way this can happen is that $(X_e - Y_f) = (X_u - Y_v)$. Hence, M_j divides M in $A[X, Y]$. □

As before, suppose that P is the associated polynomial of some bipartite graph on the set of vertices $a, b \subset [n]$. If $\bar{G}$ is the bipartite complement of G with associated polynomial $\bar{P}$, then

$$P \cdot \bar{P} = P_{[n],[n]}.$$

We say G gives a matching of the set of vertices if there exist a set of edges (i, j) providing a 1–1 correspondence between the set $[n]$ and itself. This is equivalent to saying that P contains the product $(X_1 - Y_{s(1)}) \cdots (X_n - Y_{s(n)})$ for some $s \in S_n$.

Theorem 2. *The following are equivalent*:

(i) *The graph G does not contain a matching,*
(ii) *$\bar{P}(X, s(X)) = 0$, for every $s \in S_n$,*
(iii) *$\bar{P}(X, Y)$ contains as factor some $P_{a,b}$, where $|a| + |b| = n + 1$.*

Proof. $\bar{P}(X, s(X))$ vanishes for $s \in S_n$ iff it contains a factor $(X_i - Y_{s(i)})$ for some i. This is so iff for every $s \in S_n$, $P(X, Y)$ fails to contain the product $(X_1 - Y_{s(1)}) \cdots (X_n - Y_{s(n)})$. That is, iff G contains no matching. Hence, (i) and (ii) are equivalent.

If $\bar{P}(X, s(X))$ vanishes for each $s \in s_n$, then by the remark following Lemma 2, $(\bar{P}(X, Y))^m \in \mathcal{M}$ for some m. But according to Lemma 3, $(\bar{P})^m$, and hence, $\bar{P}$ is divisible by some $P_{a,b}$, where $|a| + |b| = n + 1$. This shows that (ii) implies (iii).

The fact that (iii) implies (ii) is precisely Lemma 1. □

Definition. If G is a bipartite graph and $a \subset [n]$, let $\mathcal{R}(a) = \{j \in [n]$: there is an edge (i, j) in G such that $i \in a\}$.

Corollary (Hall's Theorem). *The graph G gives a matching iff for every set $a \subset [n]$, $|a| \leq |\mathcal{R}(a)|$.*

Proof. If G has a matching, then the condition $|a| \leq |\mathcal{R}(a)|$ is clear.

Now assume the condition and suppose G has no matching. Then by the theorem, $\bar{P}(X, Y)$ is divisible by some $P_{a,b}$ for some sets $a, b \subset [n]$ for which $|a| + |b| = n + 1$. Therefore, $\bar{G}$ contains a complete bipartite graph on the set of vertices a, b. Hence, if $i \in a$ and (i, j) is an edge in G, then it must be that $j \in \bar{b}$, where $\bar{b}$ is the complement of b in $[n]$. Hence, $\mathcal{R}(a) \subset \bar{b}$ and

$$|a| = n - |b| + 1 = |\bar{b}| + 1 > |\mathcal{R}(a)|.$$

Since this is contradictory to the assumption the corollary is proved. □

In conclusion, we wish to make explicit that the following two results are equivalent.

Theorem 3. *The following two statements are equivalent*:

(i) *In $\mathbb{Z}[X, Y]$, the radical of the ideal $\mathcal{M}$ is the ideal $\mathcal{P} = \bigcap_{s\in S_n} \mathcal{P}_s$,*
(ii) *Hall's theorem.*

Proof. The proof that (i) implies (ii) is precisely the proof of Hall's theorem in the corollary. The important fact needed there is that if $\bar{P}$ is in $\mathcal{P}$, then some power of $\bar{P}$ lies in $\mathcal{M}$. This is guaranteed by statement (i).

To show that (ii) implies (i), note that for any $F(X, Y) \in \bigcap_{s\in S_n} \mathcal{P}_s$, we have $n!$ equations in $\mathbb{Z}[X, Y]$ of the form

$$F(X, Y) = a_{1,s(1)}(X_1 - Y_{s(1)}) + \cdots + a_{n,s(n)}(X_n - Y_{s(n)}),$$

arising from each $s \in S_n$. To show that $[F(X, Y)]^{n!} \in \mathcal{M}$, it is sufficient to show that for a selection of $n!$ factors $(X_i - Y_{s(i)})$, exactly one chosen from each of the $n!$ equations above, the product $P(X, Y)$ belongs to $\mathcal{M}$.

Let G be the bipartite graph whose associated polynomial is $P(X, Y)$. That is, an edge $(i, s(i))$ belongs to G iff the factor $(X_i - Y_{s(i)})$ was selected. Let $\bar{G}$ be the complement of G. Then $\bar{G}$ contains no matching since from every possible such matching, an edge has been removed by the way edges were selected for G. Applied to $\bar{G}$, Hall's theorem then asserts the existence of sets $a, b \subset [n]$ so that $|a| > |b|$ and for which if $i \in a$ and (i, j) is an edge in $\bar{G}$, then $j \in b$. Hence, if $\bar{b}$ is the complement of b in $[n]$, it follows that for any $i \in a$ and $j \in \bar{b}$, edge (i, j) belongs to G. Hence, G must contain the complete graph $K_{|a|,|\bar{b}|}$, for which

$$|a| + |\bar{b}| = |a| + n - |b| > n.$$

It follows that $P(X, Y)$ contains as factor some element of $\mathcal{M}$. Hence, $P(X, Y)$ and, therefore, $[F(X, Y)]^{n!}$ belongs to $\mathcal{M}$. □

Acknowledgments

Many discussions with Jim Lawrence proved invaluable to the formation of this paper and his help is gratefully acknowledged. Theorem 1 was also proved independently by Moshi Roitman. I also appreciated the careful reading of this paper by the referee.

References

[1] N. Jacobson, Basic Algebra, I (Freeman, San Francisco, 1974).
[2] D.G. Northcott, Lessons on Rings, Modules and Multiplicities (Cambridge University Press, Cambridge, 1968).