THE RESULTANT MATRIX OF TWO POLYNOMIALS*

BY M. M. FLOOD

1. *Introduction.* Frobenius† has shown that if P is a matrix whose characteristic function is $P(x)$ and if $P_0(x)$ is a second polynomial, then their resultant is the determinant of the matrix $P_0(P)$. In particular, if P is non-derogatory,‡ the present author§ has shown that the degree of the highest common factor of $P(x)$ and $P_0(x)$ is the same as the nullity‖ of $P_0(P)$.

In this paper the matrix P is taken to be the companion matrix¶ of $P(x)$, and it is shown that all the remainders in the euclidean algorithm for $P(x)$ and $P_0(x)$ can easily be found from the "resultant matrix" $P_0(P)$. The proof is strictly rational and quite elementary. Finally, the results are applied to a numerical example.

2. *The Algorithm.* The euclidean algorithm for the polynomials $P_0(x)$ and $P_1(x) = P(x)$ may be written in the form

$$(1) \qquad P_{k-1}(x) = R_k(x)P_k(x) - P_{k+1}(x), \qquad (k = 1, 2, \cdots, r),$$

where $P_{r+1}(x) = 0$, and the degree of $P_{k+1}(x)$ is less than the degree of $P_k(x)$. Set $S_1(x) = 1$, $S_2(x) = R_1(x)$, $P_{-1}(x) = 0$, $P_{-2}(x) = 1$, and define polynomials $S_k(x)$ and $P_{-k}(x)$ by the relations

$$\left.\begin{aligned} S_{k+1}(x) &= R_k(x)S_k(x) - S_{k-1}(x) \\ P_{-(k+1)}(x) &= R_k(x)P_{-k}(x) - P_{-(k-1)}(x) \end{aligned}\right\}, \quad (k = 2, 3, \cdots, r).$$

A simple induction** now yields the identities

$$(2) \quad P_k(x) = S_k(x)P_1(x) - P_{-k}(x)P_0(x), \quad (k = 1, 2, \cdots, r + 1).$$

* Presented to the Society, February 29, 1936. A special case of the principal result of this paper was considered by the present author in a paper having the same title and published in the American Mathematical Monthly, vol. 44 (1937), p. 309.

† Frobenius, Journal für Mathematik, vol. 84 (1878), p. 11.

‡ Sylvester has called a matrix "non-derogatory" when its characteristic function and minimum function are the same.

§ American Mathematical Monthly, vol. 43 (1936), p. 562.

‖ The "nullity" of a matrix is the difference between its order and rank

¶ The "companion matrix" of $P(x)$ is the matrix P_1 defined in §3.

** Netto, *Vorlesungen über Algebra*, §62.

For convenience, set

$$P_j(x) = \sum_{k=0}^{p_j} P_{jk}x^k, \qquad (|\,j\,| = 0, 1, 2, \cdots, r+1)$$

and suppose that $p_0 \geqq p_1$ and that $P_{1p_1} = 1$. If $R_k(x)$ is of degree $r_k = r_{-k}$, then

$$r_k = p_{k-1} - p_k = p_{-(k+1)} - p_{-k}, \qquad (|\,k\,| = 2, 3, \cdots, r),$$

and it follows that

$$p_{-k} = p_1 - p_{k-1}, \qquad (|\,k\,| = 2, 3, \cdots, r+1).$$

The euclidean algorithm for the polynomials $P_0(x) = Q_0(x)$ and $P_1(x) = Q_1(x)$ written in the customary form would be

$$Q_{k-1}(x) = \overline{R}_k(x)Q_k(x) + Q_{k+1}(x), \qquad (k = 1, 2, \cdots, r),$$

where $Q_{r+1}(x) = 0$, and the degree of $Q_{k+1}(x)$ is less than the degree of $Q_k(x)$. It is possible to pass easily from one form of the algorithm to the other with the help of the relations

$$\left.\begin{aligned} Q_k(x) &= (-1)^{k(k-1)/2}P_k(x) \\ \overline{R}_k(x) &= (-1)^{k-1}R_k(x) \end{aligned}\right\}, \qquad (k = 0, 1, 2, \cdots, r+1).$$

3. *The Companion Matrix.* The companion matrix of $P_1(x)$ is the matrix

$$P_1 = \left\| \begin{matrix} -P_{1\,p_1-1} & -P_{1\,p_1-2} & -P_{1\,p_1-3} & \cdots & -P_{12} & -P_{11} & -P_{10} \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{matrix} \right\|.$$

So if n is a non-negative integer less than p_1, then the last $p_1 - n$ rows of P_1^{n+1} are the same as the first $p_1 - n$ rows of P_1 itself. Hence, if V_j is the matrix formed from the last r_j rows of $P_j(P_1)$, and if $2 \leqq |j| \leqq r$, then

$$V_j = \left\| \begin{matrix} P_{jp_j} \cdots P_{j2}P_{j1}P_{j0} & & & \\ & P_{jp_j} \cdots P_{j2}P_{j1}P_{j0} & & \\ & & \cdots\cdots\cdots & \\ & & & P_{jp_j} \cdots P_{j2}P_{j1}P_{j0} \end{matrix} \right\|.$$

This matrix has p_1 columns of which the first p_{-i} are zero, of course.

4. *The Resultant Matrix.* If P_1 is substituted for x in the identity (2), since $P_1(P_1)=0$, it follows that

$$P_k(P_1) = -P_{-k}(P_1)P_0(P_1), \qquad (k = 2, 3, \cdots, r).$$

Now if $W=-P_0(P_1)$, then the last r_k rows of this equation may be written in the form

$$V_k = V_{-k}W, \qquad (k = 2, 3, \cdots, r).$$

Hence if T is defined by the first of the following equations, TW will have the value given by the second of these equations:

$$T = \begin{Vmatrix} V_{-r} \\ \cdots \\ V_{-3} \\ V_{-2} \end{Vmatrix}, \qquad TW = \begin{Vmatrix} V_r \\ \cdots \\ V_3 \\ V_2 \end{Vmatrix}.$$

Let $M_{jk}(-W)$ denote the minor of order j made up from the last j rows, first $j-1$ columns, and (p_1-k)th column of $P_0(P_1)$ for $j=1, 2, \cdots, p_1$, and $k=0, 1, 2, \cdots, p_1-j$. Of course $M_{jk}(-W)=0$ if $j>p_1-p_r$ since the nullity of W is p_r. Now set

$$M_j(-W, x) = \sum_{k=0}^{p_1-j} M_{jk}(-W)x^k, \qquad (j = 1, 2, \cdots, p_1).$$

Because of the triangular form of T, it follows that

$$(3) \qquad M_j(TW, x) = (-1)^j\left[\prod_{k=2}^{s-1} c_{-k}\right](P_{-sp_{-s}})^t M_j(-W, x), \qquad (j = 1, 2, \cdots, p_1 - p_r),$$

where $c_{-k}=(P_{-kp_{-k}})^{r_k}$ and t and s are determined by the inequality $0 \leqq t=j-p_{-s}<r_s$.

An inspection of TW shows that $M_j(TW, x)=0$ unless j is either $p_{-(s+1)}$ or $p_{-s}+1$ for some value of s such that $2 \leqq s \leqq r$. In these exceptional cases, it follows that

$$\left.\begin{aligned} M_{p_{-(s+1)}}(TW, x) &= (-1)^{\sigma_s}\prod_{k=2}^{s} c_k P_s(x)/P_{sp_s} \\ M_{p_{-s}+1}(TW, x) &= (-1)^{\sigma_{s-1}+p_{-s}}\prod_{k=2}^{s} c_k P_s(x)/c_s \end{aligned}\right\}, (s=2, 3, \cdots, r),$$

where σ_k denotes the sum of the products of the integers $r_2, r_3, \cdots, r_k$ taken two at a time, and $\sigma_1 = \sigma_2 = 0$. With the help of (3) these relations yield

$$(4)\quad \left.\begin{aligned} P_s(x) &= (-1)^{\sigma_s + p_{-(s+1)}} P_{s p_s} \left[\prod_{k=2}^{s} c_{-k}/c_k\right] M_{p_{-(s+1)}}(-W, x) \\ P_s(x) &= (-1)^{\sigma_{s-1}+1} P_{-s\,p_{-s}}(c_s/c_{-s}) \left[\prod_{k=2}^{s} c_{-k}/c_k\right] M_{p_{-s}+1}(-W, x) \end{aligned}\right\}, \qquad (s = 2, 3, \cdots, r),$$

which shows that the remainders in the euclidean algorithm (1) are *proportional* to the non-zero distinct polynomials in the sequence $M_1(-W, x), M_2(-W, x), \cdots, M_{p_1}(-W, x)$, and the factors of proportionality are independent of x.

Equations (4) may also be written in the equivalent form

$$(5)\quad Q_s(x) = A_s M_{p_{-(s+1)}}(-W, x) = B_s M_{p_{-s}+1}(-W, x), \qquad (s = 2, 3, \cdots, r),$$

where A_s and B_s are constants independent of x and are given by the relations

$$(6)\quad \left.\begin{aligned} A_s &= (-1)^{\sigma_s + p_{-(s+1)} + s(s-1)/2} P_{s p_s} \prod_{k=2}^{s} c_{-k}/c_k \\ B_s &= (-1)^{\sigma_{s-1}+1+s(s-1)/2} P_{-s\,p_{-s}}(c_s/c_{-s}) \prod_{k=2}^{s} c_{-k}/c_k \end{aligned}\right\}, \qquad (s = 2, 3, \cdots, r).$$

Expressions equivalent to (4) and (6) would be obtained from them if σ_s were replaced by $q_s = n_s(n_s - 1)/2$, where n_s denotes the number of odd integers in the sequence $r_2, r_3, \cdots, r_s$.

5. *The Constants A_s and B_s.* For many applications, it is only necessary to know the remainders in the algorithm to within *positive* factors of proportionality. For example, in order to find the number of real zeros of a polynomial $P_0(x)$ within a given interval, it is sufficient to know the Sturm functions of $P_0(x)$ except for possible *positive* factors. So it is desirable to determine the signs of A_s and B_s in order that the resultant matrix of $P_0(x)$ and $P_0'(x)$ may be used to determine the Sturm functions $P_k(x)$ of $P_0(x)$ for $k = 0, 1, \cdots, r$.

If e_k denotes the sign of P_{kp_k}, it follows easily from (1) and the definition of $P_{-k}(x)$ that $e_{k-1}e_{-k}=1$ for $k=2, 3, \cdots, r+1$. For simplicity, let α_s and β_s denote the signs of A_s and B_s respectively. Then

$$(7)\qquad \left.\begin{aligned} \alpha_s &= (-1)^{\sigma_s+p_{-(s+1)}+s(s-1)/2}e_s\prod_{k=2}^{s}(e_ke_{-k})^{r_k} \\ \beta_s &= (-1)^{\sigma_{s-1}+1+s(s-1)/2}e_{-s}\prod_{k=2}^{s-1}(e_ke_{-k})^{r_k} \end{aligned}\right\},\quad (s=2,3,\cdots,r).$$

If $r_k\equiv 1 \pmod 2$ for $k=2, 3, \cdots, r$, it follows from (7) that $\alpha_s=\beta_s=1$ for $s=2, 3, \cdots, r$, since in this special case we have $\sigma_s\equiv(s-1)(s-2)/2 \pmod 2$ and $p_{-s}\equiv(s-2) \pmod 2$. In the general case, where not every r_k is odd, it is simpler and more satisfactory to determine β_s than α_s, and so the discussion which follows is given only for β_s.

Let μ_s and ρ_s denote the signs of the leading coefficients of the polynomials $M_{p_{-s}+1}(-W, x)$ and $Q_s(x)$ respectively. It follows that $\rho_s=(-1)^{s(s-1)/2}e_s$ and from (5) that $\rho_s=\beta_s\mu_s$, whence $e_s=(-1)^{s(s-1)/2}\beta_s\mu_s$ for $s=2, 3, \cdots, r$. Now $\beta_2=1, \beta_3=(-\mu_2)^{r_2-1}$, and so the β_{s+1} are given by the recursion formula

$$(8)\qquad \beta_{s+1}=(\beta_s\beta_{s-1}\mu_s\mu_{s-1})^{r_s-1}(-1)^{r_s(p_{-s}+s-1)+1}\beta_s,\qquad (s=3,4,\cdots,r-1).$$

This can be simplified, by treating the odd and even cases separately, to

$$(9)\qquad \left.\begin{aligned} \beta_{s+1} &= (-1)^{m_s}\beta_s \quad \text{if } r_s\equiv 1 \pmod 2 \\ \beta_{s+1} &= -\beta_{s-1}\mu_s\mu_{s-1} \quad \text{if } r_s\equiv 0 \pmod 2 \end{aligned}\right\},\ (s=3,4,\cdots,r-1),$$

where m_s is the number of even integers in the sequence $r_2, r_3, \cdots, r_{s-1}$. Although the argument has been given only for the constants B_s, it is also possible to determine the signs of the constants A_s directly from the resultant matrix in a similar fashion.

6. *Numerical Example.* Consider the two polynomials $Q_0(x)=x^7+2x^5+x^3-x^2-1$ and $Q_1(x)=x^7+x^5-x^2-1$. Then

$$Q_1 = \begin{Vmatrix} 0 & -1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{Vmatrix},$$

$$Q_0(Q_1) = \begin{Vmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \end{Vmatrix}.$$

It follows immediately that $Q_2(x) = M_1(Q_0(Q_1),\ x) = x^5+x^3$. Hence $\mu_2 = 1$, $r_2 = 2$, $p_{-3} = 2$, and $Q_3(x) = (-\mu_2)^{r_2-1} M_3(Q_0(Q_1), x) = -(x^2+1)$. Finally, $\mu_3 = 1$, $r_3 = 3$, $p_{-4} = 5$, and so $Q_4(x) = M_6(Q_0(Q_1), x) \equiv 0$. The first remainder is therefore x^5+x^3 and the second and last remainder is $-x^2-1$, and this is also the highest common factor of $Q_0(x)$ and $Q_1(x)$.

PRINCETON UNIVERSITY