On Two Problems in Abstract Algebra Connected with Horner's Rule[1]

by

A. Ostrowski

In order to calculate the value of the polynomial of degree n

$$(1) \qquad f_n(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

it is very useful to introduce the whole sequence of polynomials

$$(2) \qquad f_\nu(x) = a_0 x^\nu + a_1 x^{\nu-1} + \ldots + a_\nu$$

and to use the identical relation

$$(3) \qquad f_{\nu+1} = x f_\nu + a_{\nu+1} \qquad (\nu = 0, 1, \ldots, n-1).$$

In this way the value of $f_n(x)$ can be obtained by exactly n additions and n multiplications. This procedure constitutes what is usually called Horner's Rule, although it already was known to Newton[2].

Practically, the usefulness of this rule is not restricted to the case of computation "by hand". Horner's rule is even more useful if modern computational machinery is employed since its "coding" is simpler than in the case of the direct computation implying the calculation of the different powers of x.

---

[1] The preparation of this paper was sponsored (in part) by the Office of Naval Research.

[2] It is given in Newton's Analysis Per Quantitatum Series, Fluctiones ac Differentias: Cum Enumeratione Linearum Tertii Ordinis, Londini. Ex Officina Pearsoniana. Anno MDCCXI, p. 10, 4th paragraph.

Newton gives there for the polynomial $y^4 - 4y^3 + 5y^2 - 12y + 17$ the expression

$$\overline{\overline{\overline{y-4} \times y + 5} \times y - 12} \times y + 17,$$

where the bars in the notation of Newton's time correspond to the modern parentheses. In Newton's collected papers, the edition 1779, the meaning of this formula is further developed in a footnote, vol. I, p. 270–271:

"Sensus est aequationem propositam ita generandam esse, si apotomen $y-4$ cum y multiplicaveris: factum quinario auctum cum y rursum multiplicaveris: Novum factum duodenario imminutum in y rursum multiplicaveris, factoque rursum novo deniseptenarium tandem adjeceris."

Horner's rule is today often called synthetic division.

Theoretically, the question arises whether this rule could be improved or essentially modified, i. e., whether it is possible to calculate $f_n(x)$ with less than n additions or with less than n multiplications and further whether any rule for the calculation of $f_n(x)$ employing only n multiplications reduces to Horner's Rule.

It is very easy to show that no "polynomial" rule involving only operations of multiplication and addition can involve less than n additions.

In order to formulate the corresponding problems concerning the multiplications we generalize the problem in allowing an indefinite number of additions and also an indefinite number of multiplications by numerical constants. Thus the problem is reduced to the consideration of a chain of moduli M_ν defined in such a way that each modulus $M_{\nu+1}$ is obtained from the preceding one M_ν by "adjunction" of a product of two elements of M_ν. Then it appears that our problems are answered by two theorems about the index and the structure of the *first modulus* M_ν containing $f_n(x)$.

The proofs of these theorems appear to present certain difficulties and we give them only for some small values of n ($n \leqq 4$, and $n \leqq 3$). The proof of these theorems for a general n remains an open problem.

We use explicitly as the coefficient field of the moduli M_ν the field of all complex numbers but the partial results given below remain correct in the case of the most general abstract coefficient field of the characteristic 0 or p.

In the last sections (12 and 13) of this note the extension of Horner's rule to polynomials in several variables is discussed. In any case the application of Horner's rule involves $N-1$ multiplications and the same number of additions where N is the number of terms in the corresponding "complete" polynomial.

1. In what follows, small greek letters will always denote numerical constants.

We define a modulus M as a set such that with any element e it contains the products of e with all numerical constants and that with any two elements e_1, e_2 of M their sum $e_1 + e_2$ is also contained in M.

If an expression A is not contained in a modulus M, then the set of all expressions

$$\alpha A + e$$

where e runs through all elements of M, forms a new modulus $M(A)$ obtained from M by "adjunction" of A. The modulus $M(A)$ can be obtained from M by adjunction of any element of $M(A)$ which is not contained in M.

We start from the modulus

$$M_0 = [1, x, a_0, a_1, a_2, \ldots] \tag{4}$$

consisting of all integral linear functions in the *indeterminates* $x, a_0, a_1, a_2, \ldots$ with arbitrary numerical coefficients. We form then a chain of moduli M_n in which each modulus M_{n+1} $(n \geqq 0)$ is obtained from the preceding modulus M_n by adjunction of a *product* $m_n m_n'$ of two elements m_n, m_n' of M_n — provided this product is not already contained in M_n.

The elements of M_0 will be denoted generally by the letter L, sometimes with various subscripts and superscripts.

2. We show first that it is impossible to give a general "polynomial" rule for the calculation of $f_n(x)$ implying less than n additions. To prove this, take $x = 1$. Then $f_n(x)$ becomes

$$a_0 + a_1 + a_2 + \ldots + a_n$$

and it is sufficient to show that even *the* more general *expression*

$$\sum_{\nu=0}^{n} \alpha_\nu a_\nu, \qquad \alpha_0 \alpha_1 \ldots \alpha_n \neq 0,$$

cannot be calculated by less than n additions combined with an arbitrary number of multiplications by numerical constants.

This assertion is obvious for $n = 1$. Suppose, that it has been already proved for $n = 1, 2, \ldots, m-1$. Then, in calculating $\sum_{\nu=0}^{m} \alpha_\nu a_\nu$ let the *last* addition be

$$L_1(a_0, \ldots, a_m) + L_2(a_0, \ldots, a_m),$$

where L_1 and L_2 are linear forms in the a_ν with numerical constants as coefficients. Let m_1, m_2 be the numbers of the indeterminates a_ν actually contained in L_1 and L_2. Then certainly $m_1 + m_2 \geqq m + 1$. If m_1, m_2 are both $\leqq m$, the calculation of L_1 and L_2 requires at least $m_1 - 1$ and $m_2 - 1$ additions, and we have the total of at least

$$m_1 - 1 + m_2 - 1 + 1 = m_1 + m_2 - 1 \geqq m$$

additions. If $m_1 = m + 1$ then the calculation of L_1 requires at least $m - 1$ additions and the total is again at least m additions.

3. What can be said about the *number of multiplications* necessary in any general rule for the calculation of $f_n(x)$? It appears natural to assume that this number is also n and cannot be reduced even if an arbitrary number

of additions as well as an arbitrary number of multiplications with numerical constants is allowed. If this is true, we have, in using the terminology of section 1, the following *First Fundamental Theorem*:

For no integer $n > 1$ there exists a chain of moduli M_ν in the sense of section 1 such that $f_n(x)$ is contained in a modulus M_k with $k < n$.

In what follows we shall use the notation $D(E)$ for the total degree of a polynomial E in the variables $x, a_0, a_1, \ldots,$ *with respect to all of these variables.*

4. For $n = 2$ the theorem is almost obvious. If f_2 were contained in $M_1 = M_0(A_1)$, $D(f_2)$ could not be > 2, since A_1 as a product of two linear polynomials is at most quadratic.

Consider next the case $n = 3$. If f_3 were contained in $M_2 = M_1(A_2)$, $D(A_2)$ must be 4 and A_2 could be taken as a product of two quadratic expressions from $M_1 = M_0(A_1)$. We have then

$$A_2 = (\alpha A_1 + L_1)(\gamma A_1 + L_2), \qquad \alpha\gamma \neq 0,$$

and therefore

$$f_3 \equiv a_0 x^3 + \ldots = \lambda(\alpha A_1 + L_1)(\gamma A_1 + L_2) + \sigma A_1 + L.$$

Let H be the homogeneous aggregate of terms of A_1 that are of the degree 2 with respect to x, a_0, a_1, a_2, a_3. Then we have $a_0 x^3 = \lambda\alpha\gamma H^2$ and this is impossible.

5. We consider finally the case $n = 4$. If f_4 is contained in $M_3 = M_2(A_3)$, we can assume $A_3 = p' p''$ where p' and p'' belong to M_2, and we have the relation

$$f_4 \equiv a_0 x^4 + a_1 x^3 + \ldots + a_4 = \alpha p' p'' + p'''$$

where p', p'', p''' belong to M_2. Obviously $D(p')$, $D(p'')$, $D(p''')$ are $\leqq 4$. On the other hand f_4 contains the term $a_0 x^4$ of the degree 5. It follows that $D(p' p'') = 5$ and we have to consider the two cases

A) $D(p') = 2, \quad D(p'') = 3;$ B) $D(p') = 1, \quad D(p'') = 4.$

In the case A) we write $p'' = p_3$, $p' = p_2$. p_3 lies in M_2 but not in M_1. Therefore, we can assume that $M_2 = M_1(p_3)$. As to p_2, it lies in M_2 and even in M_1 because otherwise $D(p_2)$ would be 3. We have therefore $M_1 = M_0(p_2)$. Our expression for f_4 becomes

$$(5) \qquad f_4 \equiv a_0 x^4 + a_1 x^3 + \ldots + a_4 = \alpha p_2 p_3 + \beta p_3 + \gamma p_2 + L \qquad \alpha \neq 0.$$

Consider now the variable a_3. If the degrees of p_2 and p_3 with respect to a_3 were both $\geqq 1$, then $\alpha p_2 p_3$ would contain a term of degree $\geqq 2$ with respect to a_3 that does not cancel itself out while f_4 is only *linear* with respect to a_3. Therefore a_3 is not contained in more than one of the expressions p_2, p_3. But if a_3 is contained in p_2, then the total coefficient of a_3 in the right hand expression of (5) is

$$\alpha p_3 u + \beta u + \delta$$

where u is the coefficient of a_3 in p_2 and δ its coefficient in L. But this cannot be $= x$. If, on the other hand, a_3 is contained in p_3, the total coefficient of a_3 in the right hand expression of (5) would be

$$\alpha p_2 u + \gamma u + \delta,$$

where u is the coefficient of a_3 in p_3 and δ in L. This expression again is certainly $\neq x$.

On the other hand, if a_3 is contained neither in p_2 nor in p_3, the only term in the right hand expression of (5) containing a_3 would be δa_3 and therefore $\neq a_3 x$. We see that case A) is impossible.

6. Consider the case B). Here we can write $p'' = p_4$, $p' = p_1$ where the indices indicate the exact total degrees of the corresponding expressions. We have obviously $M_2 = M_1(p_4)$. On the other hand $M_1 = M_0(p_2)$ where $D(p_2) = 2$. Then we must have

$$p_4 = (\alpha p_2 + L_1)(\beta p_2 + L_2) + \gamma p_2 + L_3, \qquad \alpha \beta \neq 0,$$

and obtain the identity

$$f_4 \equiv a_0 x^4 + \ldots = p_1 p_4 + \delta p_4 + \varepsilon p_2 + L_4.$$

In putting $p_1 + \delta = L_0$ we obtain finally

$$f_4 = L_0 (\alpha p_2 + L_1)(\beta p_2 + L_2) + \sigma p_2 + L_5. \tag{6}$$

Let h_1, h_2 be the homogeneous aggregates of the terms of the highest degree in L_0 and p_2. Then we have

$$a_0 x^4 = \alpha \beta h_1 h_2^2,$$

and therefore

$$h_1 = \lambda a_0, \qquad h_2 = \varkappa x^2, \qquad \lambda \varkappa \neq 0.$$

In comparing the coefficients of x^4, we obtain from (6)

$$a_0 = L_0 \alpha \beta \varkappa^2, \qquad L_0 = \frac{1}{\alpha \beta \varkappa^2} a_0.$$

But then, if we put $a_0 = 0$ in (6), the right side expression becomes of the total degree 2 while the left hand expression is of the total degree 4. Therefore the case B) is also impossible.

7. It appears natural to assume that Horner's Rule (3) gives the only way to calculate the value of f_n with exactly n multiplications. However, if we take the point of view of the theory of moduli M_ν, i. e., allow an indefinite

number of additions and multiplications with numerical constants, some modifications of this rule are still possible since at every step we can carry out a linear transformation of x with numerical coefficients. We must therefore formulate the corresponding theorem as the following *Second Fundamental Theorem*:

If for a certain chain of moduli M_ν the expression $f_n(x)$, $n > 1$, is contained in M_n, then we have for a suitable choice of the A_ν:

(7) $M_{\nu+1} = M_\nu(A_{\nu+1})$; $A_{\nu+1} = (\alpha_\nu x + \beta_\nu) A_\nu + m_\nu)$ $(\nu = 0, 1, \ldots, n-1)$

where each m_ν belongs to the corresponding modulus M_ν.

8. We prove this theorem only for $n = 2, 3$. Consider the case $n = 2$. We can assume that $M_1 = M_0(H_2)$ where H_2 is a *homogeneous* polynomial of dimension 2 with respect to x, a_0, a_1, a_2.

Since the $D(f_2) = 3$, we can take $M_2 = M_1(f_2)$ and have therefore

$$f_2 = L_1(H_2 + L_0') + \alpha H_2 + L_0. \tag{8}$$

Put $L_1 = K + \beta$ where K is a homogeneous linear polynomial. Then (8) becomes

$$f_2(x) \equiv (K + \beta)(H_2 + L_0') + \alpha H_2 + L_0. \tag{9}$$

In comparing the terms of dimension 3 on both sides we obtain $a_0 x^2 = K H_2$ and see that K is either of the form γa_0 or γx. If K is of the form γa_0, we have $H_2 = (1/\gamma) x^2$ and it follows from (8) with $a_0 = 0$ that

$$a_1 x + a_2 \equiv (\beta/\gamma) x^2 + \beta L_0' + (\alpha/\gamma) x^2 + L_0.$$

But in this relation the right side expression cannot contain the term $a_1 x$. Therefore, we have $K = \gamma x$ and this proves our theorem for $n = 2$.

9. We take now $n = 3$. Then we have

$$f_3 = \alpha A_3 + \beta A_2 + \gamma H_2 + L_0, \qquad \alpha \neq 0, \tag{10}$$

where $M_3 = M_2(A_3)$, $M_2 = M_1(A_2)$, $M_1 = M_0(H_2)$ and H_2 is a homogeneous polynomial of the total degree 2.

We obviously have $2 \leqq D(A_2) \leqq 4$ and we consider therefore the three cases:

A) $D(A_2) = 2$; B) $D(A_2) = 4$; C) $D(A_2) = 3$.

Consider first the case A) $D(A_2) = 2$. Here we can assume that A_2 is a homogeneous polynomial $\overline{H}_2$ of degree 2. Since f_3 can be taken as A_3, we have

$$f_3 \equiv a_0 x^3 + \ldots = (\varkappa H_2 + \lambda \overline{H}_2 + L)(\varkappa' H_2 + \lambda' \overline{H}_2 + L') + \delta H_2 + \varepsilon \overline{H}_2 + L_0.$$

It follows by comparison of terms of highest degree

$$a_0 x^3 = (\varkappa H_2 + \lambda \overline{H}_2)(\varkappa' H_2 + \lambda' \overline{H}_2)$$

and we see, that one of the expressions $\varkappa H_2 + \lambda \overline{H}_2$, $\varkappa' H_2 + \lambda' \overline{H}_2$ is a numerical multiple of $a_0 x$ and the other of x^2. Since we may replace H_2 and $\overline{H}_2$ by two linear combinations which are linearly independent, we can take

$$H_2 = a_0 x, \qquad \overline{H}_2 = x^2.$$

Our representation of f_3 can be then written in the form

$$f_3 = (a_0 x + L)(x^2 + L_1) + \delta a_0 x + \varepsilon x^2 + L_0. \tag{11}$$

If we replace a_0 and a_1 by zero, L, L_1 and L_0 become respectively the linear expressions $L^{(0)}$, $L_1^{(0)}$, and $L_0^{(0)}$ and we obtain from (11)

$$a_2 x + a_3 = L^{(0)} (x^2 + L_1^{(0)}) + \varepsilon x^2 + L_0^{(0)}.$$

Here $L^{(0)}$ must be a numerical constant since otherwise the right-hand expression would be of degree 3. But then, on comparing the coefficients of x^2 we have $L^{(0)} = -\varepsilon$, the right-hand expression becomes $-\varepsilon L_1^{(0)} + L_0^{(0)}$ and cannot therefore contain the term $a_2 x$. The case A) is impossible.

10. Consider now the case B) $D(A_2) = 4$. Then A_2 is a product of two expressions from M_1 and therefore we have

$$A_2 = \varkappa_0 H_2^2 + L_1 H_2 + L_0 L_0', \qquad \varkappa_0 \neq 0.$$

If now $D(A_3)$ is < 4, we have from (10)

$$a_0 x^3 = \beta \varkappa_0 H_2^2$$

which is impossible.

And if $D(A_3) = 4$, we can also take for A_3 a product of two expressions from M_1 and obtain

$$A_3 = \varkappa_1 H_2^2 + L_2 H_2 + L_3 L_3'.$$

But then we have again

$$a_0 x^3 = (\alpha \varkappa_1 + \beta \varkappa_0) H_2^2$$

and we see that the case B) is impossible.

11. Consider finally the case C). It follows from (10) that $D(A_3) = 4$. Therefore, A_3 is either obtained as a product of a linear and a cubic polynomial or as a product of two quadratic polynomials. In the last case both factors must belong to M_1. We have in this case

$$A_3 = (\delta_1 H_2 + L_0')(\delta_2 H_2 + L_0'')$$

and the comparison of the terms of degree 4 on both sides of (10) gives here

$$a_0 x^3 = \alpha \delta_1 \delta_2 H_2^2$$

which is impossible.

Therefore A_3 is a product of a linear polynomial with a cubic one, which can be taken as A_2. We obtain

$$A_3 = L_2 A_2, \qquad A_2 = L_1 (H_2 + L_3) + \delta H_2 + L_4.$$

Let the homogeneous parts of L_1, L_2 be K_1, K_2 and the corresponding constants $\varkappa_1, \varkappa_2$. Then we have

$$A_3 = (K_2 + \varkappa_2) A_2, \qquad A_2 = (K_1 + \varkappa_1)(H_2 + L_3) + \delta H_2 + L_4.$$

The comparison of the highest terms on both sides of (10) gives

$$K_1 K_2 H_2 = a_0 x^3. \tag{12}$$

Therefore K_1, K_2, H_2 do not contain a_1 and the only terms of the right-side expression in (10) containing a_1 are

$$L_0 + \beta L_4 + \beta (K_1 + \varkappa_1) L_3 + \alpha (K_2 + \varkappa_2)(K_1 + \varkappa_1) L_3 + (K_2 + \varkappa_2) L_4.$$

Here the term $a_1 x^2$ of the degree 3 can only be contained in $\alpha K_2 K_1 L_3$ and in virtue of (12) K_1 and K_2 must be multiples of x. Our theorem is proved for $n = 3$.

12. Horner's rule can of course be also applied to the computation of polynomials in more than one variable. Let

$$f(x, y) = \sum_{\nu=0}^{n} A_\nu(y)\, x^{n-\nu} \tag{13}$$

be of degree n with respect to x and the general coefficient $A_\nu(y)$ of degree m_ν with respect to y.

We can begin by computing the polynomials $A_\nu(x)$ and need for that by Horner's rule $\sum\limits_{\nu=0}^{n} m_\nu$ multiplications and the same number of additions. To complete the computation of f by Horner's rule, applied to a polynomial in x, n more multiplications and n more additions are necessary and we see that the value of f certainly can be computed by $\sum\limits_{\nu=0}^{n} m_\nu + n$ multiplications and the same number of additions.

But this expression is by 1 less than the total number of terms in $f(x,y)$, provided this polynomial is "complete", i. e., that in each $A_\nu(y)$ no power of y of degree $< m_\nu$ is missing and in $f(x,y)$ no power of x of degree $< n$. In case there are "gaps" they must be "filled up" in a suitable way. If for instance a power of x of degree $< n$ is missing, i. e., the corresponding coefficient $A_\nu(y) \equiv 0$, then this power of x is counted as one term of f. While, if there are gaps in $A_\nu(y) \neq 0$, $m_\nu + 1$ must be still considered as the total number of terms in $A_\nu(y)$ and in $A_\nu(y)\, x^{n-\nu}$.

13. In the same way Horner's rule may be applied to polynomials in any number of variables and its application requires $N - 1$ multiplications and the same number of additions where N is the total number of terms of our polynomial. For the calculation of N the polynomial must of course be "completed" in the way explained above.

However, this number N of terms depends on the order of the variables. For instance

$$c_n x^n y^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0, \qquad (c_n \cdot c_{n-1} \cdots c_0 \neq 0)$$

has $2n + 1$ terms if ordered first by powers of x, while if ordered first by powers of y the total number of terms is to be taken as $3n$.

U.S. National Bureau of Standards
and
University of Basle