R. M. Robinson, whose IBM 701 program produced the factorization (5), and to D. H. Lehmer, whose suggestions have materially assisted in the planning of this work.

University of San Francisco
San Francisco, California

1. John Brillhart & G. D. Johnson, "On the factors of certain Mersenne numbers," *Math. Comp.*, v. 14, 1960, p. 365–369.
2. John Brillhart, "Concerning the numbers $2^{2p} + 1$, p prime," *Math. Comp.*, v. 16, 1962, p. 424–430. (Reference is there made to the earlier table by M. Kraitchik.)
3. A. J. C. Cunningham & H. J. Woodall, *Factorizations of* $(y^n \mp 1)$, Hodgson, London, 1925, p. 19.
4. D. H. Lehmer, "Tests for primality by the converse of Fermat's theorem," *Bull., Amer. Math. Soc.*, v. 33, 1927, p. 327–340.
5. R. M. Robinson, "A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers," *Proc., Amer. Math. Soc.*, v. 9, 1958, p. 673–681.

EDITORIAL NOTE: Rudolph Ondrejka has shown that $10^{37} - 1$ is divisible by 2028119. (*Recreational Math. Mag.*, Feb. 1962, p. 47.)

A Note on Octic Permutation Polynomials

By S. R. Cavior

1. Introduction. A polynomial $f(x)$ with coefficients in the finite field $GF(q)$, $q = p^n$, is called a permutation polynomial if the set $\{f(a): a \, \varepsilon \, GF(q)\}$ is a permutation of $GF(q)$. The object of this paper is to extend some known results about permutation polynomials of even degree over fields with odd characteristic p.

We shall frequently use the following theorem which is given by Dickson [1, p. 77].

Theorem. *If $f(x)$ is a polynomial of degree m over $GF(q)$, and if $m \mid q - 1$, then $f(x)$ does not permute $GF(q)$.*

To begin our discussion, we note immediately, by the Theorem, that a quadratic polynomial cannot permute $GF(q)$. Dickson, in [1], showed that a quartic cannot permute $GF(q)$ for $q > 7$ (although two do for $q = 7$), and that a sextic cannot permute $GF(q)$ for $q > 11$ (although several do for $q = 11$.) A natural question to ask, then, is whether there is an upper bound for the order of a finite field which an octic can permute.

The present investigation, however, is restricted to the following special octics:

$$f(x) = x^8 + ax^t \qquad t = 1, 3, 5, 7; \; a \, \varepsilon \, GF(q). \tag{1}$$

The case $t = 7$ can be settled at once, for if $f(x) = x^8 + ax^7$, where $a \, \varepsilon \, GF(q)$, then $f(-a) = f(0) = 0$. That is, $f(x)$ is not a permutation polynomial. With the aid of a computer it was discovered that the only polynomials of the form (1) which permute $GF(p)$ for $p < 500$ are

$$x^8 + ax \qquad a = \pm 4, \pm 10; \; p = 29 \tag{2}$$

Received October 12, 1962, revised April 26, 1963. This research was supported in part by National Science Foundation. The computations involved were carried out in the Duke University Computing Laboratory, which is supported in part by National Science Foundation.

and

$$x^8 + ax^3 \qquad a = \pm 4, \pm 9; p = 11. \tag{3}$$

2. Dickson's Method. The method we use to decide whether a polynomial of the form (1) permutes $GF(q)$ is the one Dickson used in [1]. The basis of it is this fact: If $f(x)$ is a permutation polynomial over $GF(q)$, and is raised to a power less than $q - 1$, the coefficient of x^{q-1} becomes 0 after reducing exponents by the identity $x^q = x$. Therefore, to demonstrate that $f(x)$ is not a permutation polynomial, one must simply show that when it is raised to some (well chosen) power, x^{q-1} does not vanish.

For example, let us take $f(x) = x^8 + ax$ over the field $GF(q)$, $q = 8m + 5$. Raising to the power $(m + 4)$, we have

$$\begin{aligned}(x^8 + ax)^{m+4} = x^{8m+32} &+ a\binom{m+4}{m+3}x^{8m+25} + a^2\binom{m+4}{m+2}x^{8m+18} \\ &+ a^3\binom{m+4}{m+1}x^{8m+11} + a^4\binom{m+4}{m}x^{8m+4} + \cdots\end{aligned} \tag{4}$$

For $q > 29$ none of the exponents can reduce to $8m + 4$ by the identity $x^q = x$. Therefore, if $f(x)$ is to be a permutation polynomial over $GF(q)$, the coefficient of x^{8m+4} must be 0; i.e.,

$$a^4\binom{m+4}{m} \equiv 0 (\mathrm{mod}\, p) \quad \text{or} \quad p \mid a^4(m+4)(m+3)(m+2)(m+1). \tag{5}$$

However, we shall show that this is impossible if $a \neq 0$. First, $p \nmid m + 1$. For if $p \mid m + 1$, then $p \mid 8m + 8 = p^n + 3$, and $p \mid 3$. But $p = 8l + 5$, so $p \nmid 3$. In a similar way we can show that $p \nmid m + 2$, $p \nmid m + 3$, and $p \nmid m + 4$. So $p \mid a$. This shows, then, that $x^8 + ax$ cannot permute $GF(q)$ if $q = 8m + 5 > 29$.

3. Results. Combining the results in (2) and (3) with other results derived by Dickson's method, we present the following information which indicates upper bounds for the size q of a finite field which the special octics permute.

The polynomial $f(x) = x^8 + ax$, $a \in GF(q)$, does not permute $GF(q)$ if $q = 8m + 3$ or $8m + 7$. If $q = 8m + 5$ the only field permuted is $GF(29)$.

The polynomial $g(x) = x^8 + ax^3$ does not permute $GF(q)$ if $q = 8m + 5$ or $8m + 7$. If $q = 8m + 3$, and if some $g(x)$ permutes $GF(q)$, then q must equal 11^n. By the Theorem we see that no octic can permute $GF(11^{2m})$, and it is an open question whether $g(x)$ can permute $GF(11^{2m+1})$.

The polynomial $h(x) = x^8 + ax^5$ does not permute $GF(q)$ if $q = 8m + 3$. If $q = 8m + 5$, and if $h(x)$ permutes $GF(q)$, then $q = 13^n$. By the Theorem we see that no octic can permute $GF(13^{2m})$, and it is an open question whether $h(x)$ can permute $GF(13^{2m+1})$. If $q = 8m + 7$, and if $h(x)$ permutes $GF(q)$, then $q = 7^n$. Again we see by the Theorem that no octic can permute $GF(7^{2m})$, and again it remains an open question whether $h(x)$ can permute $GF(7^{2m+1})$.

We now present these results in tabular form.

polynomial	$q = p^n$	$GF(q)$ which are permuted
$x^8 + ax$	$8m + 3$	none
	$8m + 5$	$GF(29)$ and no others
	$8m + 7$	none
$x^8 + ax^3$	$8m + 3$	$GF(11)$ and possibly $GF(11^n)$ for odd n
	$8m + 5$	none
	$8m + 7$	none
$x^8 + ax^5$	$8m + 3$	none
	$8m + 5$	possibly $GF(13^n)$ for odd n
	$8m + 7$	possibly $GF(7^n)$ for odd n

In conclusion we might ask whether, for each integer k, there exists a bound $N = N_k$ such that if $f(x)$ is of degree $2k$ over $GF(q)$, $f(x)$ will not permute $GF(q)$ if $q > N_k$.

Duke University
Durham, North Carolina

1. L. E. Dickson, "Analytic representation of substitutions, *Ann. of Math.*, v. 11, 1896–97, p. 65–120.

Multistep Integration Formulas

By A. C. R. Newbery

A multistep formula for the approximate solution of an ordinary differential equation $x' = f(x, t)$ has the form $\sum_{i=0}^{k} a_i x_i = h \sum_{i=0}^{k} b_i x_i'$. The formula is assumed to be stable, and to have optimum precision subject to this restriction; this means that a truncation error of the form $Hh^{k+2}x^{(k+2)}(z) + 0(h^{k+3})$ is associated with the formula [1], where $x(t)$ is the exact solution of the differential equation and H is a constant, which, like the b_i, depends on the choice of the constants a_i. A closed expression for the b_i has already been given in [2, page 39], but it is considered worthwhile to tabulate the matrices which transform the a_i into the b_i, to give an improved derivation of these matrices, and to extend the argument so that predictor coefficients can also be readily calculated.

The first task is, for a given k, to compute the elements c_{ij} of a $(k + 2) \times k$ 'corrector matrix' C_k, such that $b = C_k a$, where $b = \{b_0, b_1, \cdots b_k, H\}'$ and $a = \{a_1, a_2, \cdots a_k\}'$. (Note that a_0 is determined by the consistency condition $\sum_0^k a_i = 0$.) Using the notation of Antosiewicz and Gautschi [4, page 327] the relation between the required b_i and the given a_i is equivalent to the requirement that the linear functional $Lx(t) \equiv \sum_{i=0}^{k} [a_i x(i) - b_i x'(i)]$ should annihilate all

Received November 1, 1962.