Technical Report CS75018-R

DIVIDED DIFFERENCE METHODS FOR FINITE FIELDS

T. C. Wesselkamper

August 1975

Department of Computer Science
Virginia Polytechnic Institute and State University
Blacksburg, Virginia 24061

The work reported herein was supported in part by National Science Foundation Grant No. DCR74-18108.

Abstract

The Reed-Muller Decomposition Theorem is shown to be a special case of a theorem of Newton. Divided difference methods are developed for the general case of any finite field. The Newton Interpolation Theorem is proved for functions of one variable and stated for functions of two variables. Empirical results are given for some two place functions over GF(9) and GF(16).

Keywords: Divided difference methods, Shannon Decomposition Theorem, Reed-Muller Decomposition Theorem, finite field, Newton's Interpolation Theorem.

CR Catagories: 5.30, 6.31, 5.13

MR Catagories: 12C05, 41A10

I PRELIMINARIES

In 1938 Claude E. Shannon, a graduate student at MIT, published a paper entitled "A Symbolic Analysis of Relay and Switching Circuits". In this paper he proves (in different words and with a different notation) the following theorem which has come to be called the Shannon Decomposition Theorem [9].

Theorem 1:- Let $E(2) = \{0, 1\}$ and let $f: E^n(2) \to E(2)$. If $\vee$, $*$, and $\bar{}$ denote the disjunction, conjunction, and negation operators, respectively, then there exist functions $g: E^{n-1}(2) \to E(2)$ and $h: E^{n-1} \to E(2)$ such that:

$$f(x_1, x_2, \ldots, x_n) = (x_n * g(x_1, \ldots, x_{n-1})) \vee (\bar{x}_n * h(x_1, \ldots, x_{n-1})).$$

The proof of the theorem is immediate if one sets

$g(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 1)$, and

$h(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 0)$.

Shannon's choice of disjunction, conjunction, and negation as primitive operators was dictated by the circuit design considerations of the times.

In 1954 Irving S. Reed showed that if the operation of non-equivalence ("exclusive or") is substituted for disjunction ("inclusive or") then a decomposition of a function can be achieved without using negation as a primitive operation [8].

The set E(2) under the operations of disjunction and non-equivalence is isomorphic to the field GF(2). The following theorem has come to be called the Reed-Muller Decomposition Theorem.

Theorem 2:- Let $E(2) = \{0, 1\}$ and let $f: E^n(2) \to E(2)$. If + and * denote addition and multiplication over GF(2), respectively, then there exist functions $g: E^{n-1}(2) \to E(2)$ and $h: E^{n-1}(2) \to E(2)$, such that

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_{n-1}) + x_n * h(x_1, \ldots, x_{n-1}).$$

Again, the proof is easy once one sets

$$g(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 0), \text{ and}$$

$$h(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 0) + f(x_1, \ldots, x_{n-1}, 1).$$

It is quite clear that in his 1954 paper Reed was consciously using difference methods and difference notation. In the last paragraph of that paper he suggests the investigation of codes over fields of characteristic other than two.

Later writers appear to have lost sight of the very general nature of the methods related to Reed-Muller Decomposition.

If p is a prime and q is a natural number, then the integers modulo p form a field, GF(p), and there exists a unique field $GF(p^q)$. We assume that the properties of such fields are known.

There is an enormous literature on difference methods beginning with Isaac Newton in 1675-6 [6] and progressing through a spectacular array of mathematicians. This work was done in the context of the field of rationals or the field of reals. In fact a great part of the work does not depend on any topological considerations and can be directly applied to any finite field.

In this paper we sketch the beginnings of a theory of finite difference methods over finite fields. We carry the development only far enough that the reader may proceed to the classic works on finite difference methods.

Throughout this section, let p be a prime and q be a natural number. Let $k = p^q$. Let + and * denote addition and multiplication, respectively, over $GF(p^q)$. When there is no danger of confusion, we write 'ab' for 'a*b'. Finally let Σ and Π denote the extended sum and extended product in the usual way. Let $E(k) = \{0,1, \ldots, k-1\}$.

Definition 1:- For each k, let

$$Z_k(x) = \prod_{i=0}^{n=1} (x - i).$$

Note that for each $a \in E(k)$, we have $Z_k(a) = 0$.

Lemma 1:- Let $P_1(x)$ and $P_2(x)$ be two polynomials in x. $P_1(x) \equiv P_2(x) \pmod{Z_k(x)}$ if and only if for each $a \in E(k)$, $P_1(a) = P_2(a)$.

Proof:- Suppose that $P_1(x) \equiv P_2(x) \pmod{Z_k(x)}$. Suppose also that the degree of P_2 is greater than or equal to the degree of P_1. Then there exists a polynomial Q(x) of degree greater than or equal to 0, such that $P_2(x) = P_1(x) + Q(x)Z_k(x)$. Let a be an arbitrary element of E(k). Then $P_2(a) = P_1(a) + Q(a)Z_k(a)$. Since $Z_k(a) = 0$, $P_2(a) = P_1(a)$.

Conversely, suppose that for each $a \in E(k)$, $P_1(a) = P_2(a)$. Consider the polynomial $R(x) = P_2(x) - P_1(x)$. For each $a \in E(k)$, $R(a) = 0$. Hence $(x - a)$ is a divisor of $R(x)$. Since this holds for each $a \in E(k)$, $Z_k(x)$ is a divisor of $R(x)$ and so there exists a polynomial $Q(x)$ of degree greater than or equal to 0 such that $R(x) = Q(x)\, Z_k(x) = P_2(x) - P_1(x)$. Thus $P_2(x) = P_1(x) + Q(x)Z_k(x)$ and $P_2(x) \equiv P_1(x) \pmod{Z_k(x)}$.

Corollary 1:- If $P(x)$ is a polynomial of degree greater than or equal to k, then there exists a polynomial $P'(x)$ of degree less than or equal to k-1 such that for each $a \in E(k)$, $P(a) = P'(a)$.

Another way of saying this is that P and P' define the same function: $E(k) \to E(k)$. Because of this we limit our scope to polynomials of degree less than or equal to k-1, that is, to polynomials with exponents and coefficients in E(k); specifically:

$$\sum_{i=0}^{k-1} a_i x^i.$$

A simple counting argument produces the following theorem.

Theorem 3:- If p is a prime and q is a natural number and $k = p^q$, then each function $f: E(k) \to E(k)$ is uniquely defined by a polynomial $P(x) = \sum_{i=0}^{k-1} a_i x^i$, $(a_i \in E(k))$.

Proof:-Each polynomial P(x) is a sum of exactly k terms. In each term the coefficient may be chosen in k different ways. Hence there are k^k formal polynomials, just as there are k^k different functions $f: E(k) \to E(k)$. If two formally distinct polynomials, say P_1 and P_2, define the same function, then by Lemma 1 the polynomials are congruent modulo $Z_k(x)$. This means, for example, that $P_2(x) = P_1(x) + Q(x)Z_k(x)$. But either the degree of the right hand side is at least k, which contradicts the definition of P_1 and P_2, or $Q(x) = 0$, which contradicts the distinctness of P_1 and P_2.

The validity of the theorem is entirely dependent upon the fact that a field possesses no divisors of 0. The theorem is not true for a ring which is not a field, say the ring Z_n of integers modulo n where n is not prime. For example in Z_4 each function which is defined by a polynomial is defined by four polynomials.

The general problem of determining which functions $f: E(k) \to E(k)$ and $g: E^n(k) \to E(k)$ are defined by polynomials over the ring Z_k is treated in [2].

It is useful for the theorems which follow to develop a decomposition theorem for functions over a space E(k) where $k = p^q$, for some prime p and natural number q. The following decomposition theorem is in the spirit of the Shannon Theorem, although it is defined over a finite field. There is a preliminary definition.

Definition 2:- For each i in E(k) define a function $V_i: E(k) \to E(k)$ by:

$$V_i(x) = \begin{cases} 1, & \text{if } x = i; \\ 0, & \text{if } x \neq i. \end{cases}$$

In words, each V_i is a characteristic function for the set {i} in E(k). In terms of these V_i we can state:

Theorem 4:- Let p be a prime and q a natural number. Let $k = p^q$ and let + and * denote addition and multiplication in GF(k). If $f: E^n(k) \to E(k)$, then there are k functions, $g_0, g_1, \ldots, g_{k-1}$, such that for each i, $g_i: E^{n-1}(k) \to E(k)$, and

$$f(x_1, \ldots, x_n) = \sum_{j=0}^{k-1} V_j(x_n) * g_j(x_1, \ldots, x_{n-1}).$$

Proof : For each i in E(k), let

$$g_i(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, i). \qquad (A)$$

Let $F(x_1, \ldots, x_n) = \sum_{j=0}^{k-1} V_j(x_n) * g_j(x_1, \ldots, x_{n-1})$.

Suppose $x_n = j'$, an arbitrary element of E(k). Then $V_{j'}(x_n) = V_{j'}(j') = 1$, but for each $j^* \neq j'$, $V_{j^*}(x_n) = V_{j^*}(j') = 0$. In the summation of the right side of (A) each $V_j(x_n)$ is 0 except $V_{j'}(x_n)$, which is 1. Hence each term in the summation is 0, except $V_{j'}(x_n) * g_{j'}(x_1, \ldots, x_{n-1})$, which is the value of the whole sum. But

$$\begin{aligned} V_{j'}(x_n) * g_{j'}(x_1, \ldots, X_{n-1}) &= V_{j'}(j') * g_{j'}(x_1, \ldots, x_{n-1}) \\ &= 1 * f(x_1, \ldots, x_{n-1}, j') \\ &= f(x_1, \ldots, X_{n-1}, X_n). \end{aligned}$$

Since j' was chosen arbitrarily, $F(x_1, \ldots, \mathbf{x_n}) = f(x_1, \ldots, x_n)$ for all values of x_n and F = f, hence the theorem is true.

Corollary 2:- If $k = p^q$, then for each natural number n each function $f: E^n(k) \to E(k)$ is defined by a polynomial in n indeterminates over GF(k).

The uniqueness of this representation is proved in a fashion analogous to Theorem 3.

If f: $E(k) \to E(k)$, it is convenient to have a compact notation for f.

<u>Definition 3</u>:-If f: $E(k) \to E(k)$, define $f = \langle a_0 a_1 \cdots a_{k-1} \rangle$ whenever $f(0) = a_0$, $f(1) = a_1$, ..., $f(k-1) = a_{k-1}$; that is, for all $i \in E(k)$, $f(i) = a_i$.

$\langle a_0 a_1 \ldots a_{k-1} \rangle$ is called the value sequence of f.

II DIVIDED DIFFERENCE TABLES

Theorem 3 and Corollary 2 are existence proofs for the polynomial representation over $GF(p^q)$ of each function over $E(p^q)$. They offer no clue as to the values of the coefficients of the polynomial corresponding to a given function.

The classic works on difference methods assume the domain of definition to be either the rational field or the real field [4,5]. Most often in the literature the underlying field is not specified. In this paper we show that the methods work equally over a finite field. (In fact, they work over any field, but we make use of finiteness to render life particularly simple and pleasant.)

For a fixed prime p and a fixed natural number q, let $k=p^q$ and let $F = GF(k)$. Let $F[x]$ denote the ring of polynomial forms over F in the single indeterminate x and let $F(x)$ denote the field of rational forms. Recall that $F(x)$ contains an isomorphic copy of $F[x]$. Specifically, for $p \in F[x]$ the mapping $\psi : p \to p/1$ is an isomorphism from $F[x]$ onto $\{p/1 \mid p \in F[x]\} \subset F(x)$. If $f:F \to F$ is a function, then we may identify f with its polynomial representation over F.

Following the notation of [5] we state:

Definition 4:-If the sequence $x_o, x_1, \ldots, x_{k-1}$ is some permutation of the elements of F

$$[x_i x_j] = \frac{f(x_i) - f(x_j)}{x_i - x_j}, \text{ if } i \neq j;$$

$$[x_i x_{i+1} \ldots x_{i+j}] = \frac{[x_i \ldots x_{i+j-1}] - [x_{i+1} \ldots x_{i+j}]}{x_i - x_j}, \text{ if } j \geq 2.$$

In particular, we have:

$$[x_o x_1] = \frac{f(x_o) - f(x_1)}{x_o - x_1}, \text{ a first order difference;}$$

$$[x_o x_1 x_2] = \frac{[x_o x_1] - [x_1 x_2]}{x_0 - x_2}, \text{ a second order difference; and}$$

$$[x_o x_1 \ldots x_j] = \frac{[x_o x_1 \ldots x_{j-1}] - [x_1 x_2 \ldots x_j]}{x_o - x_j}, \text{ a } j^{th} \text{ order difference.}$$

Note also that $[x_i x_j] = \frac{f(x_i) - f(x_j)}{x_i - x_j} = \frac{f(x_j) - f(x_i)}{x_j - x_i} = [x_j x_i]$,

and in particular, $[x_o x_1] = [x_1 x_o]$.

The relationship between these may be seen from the following table:

x_o	$f(x_o)$	$[x_o x_1]$		
x_1	$f(x_1)$	$[x_1 x_2]$	$[x_o x_1 x_2]$	$[x_o x_1 x_2 x_3]$
x_2	$f(x_2)$	$[x_2 x_3]$	$[x_1 x_2 x_3]$	$[x_1 x_2 x_3 x_4]$
x_3	$f(x_3)$	$[x_3 x_4]$	$[x_2 x_3 x_4]$	$[x_2 x_3 x_4 x_5]$
x_4	$f(x_4)$	$[x_4 x_5]$	$[x_3 x_4 x_5]$	
x_5	$f(x_5)$		.	.
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
x_{k-1}	$f(x_{k-1})$	$[x_{k-2} x_{k-1}]$	$[x_{k-3} x_{k-2} x_{k-1}]$	$[x_{k-4} x_{k-3} x_{k-2} x_{k-1}]$

Example 1:- Let k = 5 and construct a difference table for the function with value sequence < 13231 > .

x	f (x)				
0	1				
		2/1			
1	3		2/2		
		4/1		0	
2	2		2/2		0
		1/1		0	
3	3		2/2		
		3/1			
4	1				

Example 2:- Let k = 5 and construct a difference table for:

$$V_3(x) = \begin{cases} 1, & \text{if } x=3; \\ 0, & \text{if } x\neq 3. \end{cases}$$

x	$V_3(x)$				
0	0				
		0/1			
1	0		0/2		
		0/1		3/3=1	
2	0		1/2=3		1/4=4
		1/1		1/3=2	
3	1		3/2=4		
		4/1			
4	0				

Example 3:- Same as Example 2, but permute the order of the values of x.

x	$V_3(x)$				
0	0				
		0			
2	0		0		
		0		0	
4	0		0		2/3=4
		0		2/1	
1	0		3/4=2		
		1/2=3			
3	1				

Example 4:- Let k = 4, and construct a difference table for:

$$V_2(x) = \begin{cases} 1, & \text{if } x = 2; \\ 0, & \text{if } x = 2. \end{cases}$$

The field $GF(2^2)$ is given by the two tables:

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

x	$V_2(x)$			
0	0			
		0/1=0		
1	0		2/2=1	
		1/3=2		3/3=1
2	1		3/2=2	
		1/1=1		
3	0			

The above remark, that $[x_o x_1] = [x_1 x_o]$, can be generalized into a pleasant and important result, contained in the corollary below. Regrettably there does not appear to be an equally pleasant proof. The following lemma[3, p. 10] achieves the desired result.

Lemma 2:- If $x_o, x_1, \ldots, x_j$ are distinct elements of F and if $f(x) \in F[x]$ is of degree n ($j \leq n$), then,

$$[x_o x_1 \ldots x_j] = \frac{f(x_o)}{(x_o-x_1)\,(x_o-x_2)\ldots(x_o-x_j)}$$

$$+ \frac{f(x_1)}{(x_1-x_o)\,(x_1-x_2)\ldots(x_1-x_j)},$$

$$+ \ldots.$$

$$+ \frac{f(x_j)}{(x_j-x_o)\,(x_j-x_1)\ldots(x_j-x_{j-1})}.$$

proof: The proof is by induction on j. If j = 1, then

$$[x_o x_1] = \frac{f(x_o)-f(x_1)}{x_o-x_1}$$

$$= \frac{f(x_o)}{(x_o - x_1)} + \frac{f(x_1)}{(x_1 - x_o)}$$

and the theorem is true.

As the induction hypothesis, assume that the theorem is true for differences of order j-1.

Then we have:

$$[x_o x_1 \ldots x_j] = \frac{x_o x_1 \ldots x_{j-1} - x_1 x_2 \ldots x_j}{x_o - x_j}$$

$$= \frac{f(x_o)}{(x_o-x_1)\ldots(x_o-x_{j-1})\,(x_o-x_j)}$$

$$+ \frac{f(x_1)}{(x_1-x_o)\ldots(x_1-x_{j-1})(x_o-x_j)}$$

$$+ \ldots$$

$$+ \frac{f(x_{j-1})}{(x_{j-1}-x_o)\ldots(x_{j-1}-x_{j-2})(x_o-x_j)}$$

$$- \frac{f(x_1)}{(x_1-x_2)\ldots(x_1-x_j)(x_o-x_j)}$$

$$- \ldots$$

$$- \frac{f(x_{j-1})}{(x_{j-1}-x_1)\ldots(x_{j-1}-x_j)(x_o-x_j)}$$

$$- \frac{f(x_j)}{(x_j-x_1)\ldots(x_j-x_{j-1})(x_o-x_j)}$$

The first term is exactly as required; the last becomes the required term by simultaneously changing the sign of the term and the sign of the factor (x_o-x_j) in the denominator. If the terms with like numerators are combined, the rest follows. For example, the terms with numerator $f(x_1)$ combine into:

$$\frac{(x_1-x_j)f(x_1) - (x_1-x_o)f(x_1)}{(x_1-x_o)(x_1-x_2)\cdots(x_1-x_{j-1})(x_1-x_j)(x_o-x_j)}$$

which simplifies to

$$\frac{f(x_1)}{(x_1-x_o)(x_1-x_2)\cdots(x_1-x_j)}$$

as required.

That unpleasantness over, we can obtain:

Corollary 3: If $x_o, x_1, \ldots, x_j$ are distinct elements of F and $f(x) \in F[x]$ is of degree n ($j \leq n$) and s is a permutation of the integers 0, 1, ..., j, then $[x_o x_1 \cdots x_j] = [x_{s(o)} x_{s(1)} \cdots x_{s(j)}]$. In words, the value of $[x_o x_1 \cdots x_j]$ is invariant under a permutation of its elements.

proof: Note that a permutation of the elements $\{x_i\}$ permutes the order of the terms in the expression in Lemma 2 but leaves the value unchanged.

III. DIVIDED DIFFERENCE POLYNOMIALS

The method which was employed in the previous section can be extended. Note that in Definition 4 we required that the points $x_o, x_1, \ldots, x_{k-1}$ be distinct. We wish to extend our definition by weakening this restriction.

Lemma 3: If $f(x) \in F[x]$ is of degree n $(1 \leq n \leq k-1)$ and $x_1 \in F$, then there exists a unique polynomial $q(x) \in F[x]$ of degree $n-1$ such that:

$$q(x) = \frac{f(x) - f(x_1)}{x - x_1}.$$

proof: If $f(x) \in F[x]$, then $f(x_1) \in F$ and $f(x) - f(x_1) \in F[x]$. By the Euclidean algorithm there exists a polynomial $q(x)$ of degree $n-1$ and an $r \in F$, such that $f(x) - f(x_1) = (x - x_1)q(x) + r$. Since r is a constant, setting $x = x_1$ gives $r = 0$. Since $q(x)$ is of degree less than or equal to $k-2$, $q(x)$ defines a unique function by Theorem 3.

This lemma makes the following definition reasonable.

Definition 5: Let $x_o, x_1, \ldots, x_{k-1}$ be a permutation of the elements of F. Let $f(x) \in F[x]$ be of degree n $(0 \leq n \leq k-1)$.

$$[xx_1] = \frac{f(x) - f(x_1)}{x - x_1}$$

$$[xx_1 \ldots x_j] = \frac{[xx_1 \ldots x_{j-1}] - [x_1 x_2 \ldots x_j]}{x - x_j}$$

The notation of Definition 5 is designed to lull the reader into accepting it as a simple extension of Definition 4. In the cases $x = x_i$ $(1 \leq i \leq j)$, this is exactly the case, since Definition 4 did not allow for the possibility that two of the elements of $[x_o x_1 \ldots x_j]$ might be equal. We need to prove that where Definitions 4 and 5 coincide syntactically they also coincide semantically.

Theorem 5: If the sequence $x_o, x_1, \ldots, x_{k-1}$ is a permutation of the elements of F and if $f(x) \in F[x]$ is of degree n $(0 \leq n \leq k-1)$, then when $j \leq n$, $[xx_1 \ldots x_j]$ is a polynomial $q(x)$ of degree $n-j$ and $q(x_o) = [x_o x_1 \ldots x_j]$; and when $n < j$, $[xx_1 \ldots x_j] = 0$.

proof: The proof is by induction on j. If $j = 1$, there are two cases.

Case 1, $1 = j \leq n$. By Lemma 3 there is a $q(x) \in F[x]$ of degree $n-1$ as required. Since

$$q(x) = \frac{f(x) - f(x_1)}{x - x_1}$$ letting $x = x_o$ gives

$$q(x_o) = \frac{f(x_o) - f(x_1)}{x_o - x_1} = [x_o x_1],$$ as required.

Case 2, $n < j = 1$, that is, $n = 0$. If the degree of $f(x)$ is 0, then $f(x) = c \in F$, a constant. From the definition

$[xx_1] = \frac{c - c}{x - x_1} = 0$, and the theorem is true.

Let $2 \leq j$. As the induction hypothesis assume the theorem to be true differences of order j-1. There are again two cases.

Case 1, $j \leq n$. Consider the expression

$$[xx_1 \ldots x_j] = \frac{[xx_1 \ldots x_{j-1}] - [x_1 x_2 \ldots x_j]}{x - x_j}.$$

Since $2 \leq j \leq n$, we have $1 \leq j-1 \leq n-1$. By the induction hypothesis $[xx_1 \ldots x_{j-1}]$ is a polynomial of degree $n-j+1 \geq 1$. Let $q_1(x) = [xx_1 \ldots x_{j-1}] - [x_1 x_2 \ldots x_j]$, also of degree n-j+1. By the Euclidean algorithm there exists a polynomial q(x) of degree n-j and a constant $r \in F$ such that $q_1(x) = (x - x_j)q(x) + r$. Since r is a constant, let $x = x_j$. Then $q_1(x_j) = r$. But also, $q_1(x_j) = [x_j x_1 \ldots x_{j-1}] - [x_1 \ldots x_{j-1} x_j]$. By Corollary 3 the two terms on the right are equal and r = 0. Therefore q(x) is the unique polynomial value of $[xx_1 \ldots x_j]$. Since $x_o, x_1, \ldots, x_j$ are distinct

$$q(x_o) = \frac{[x_o x_1 \ldots x_{j-1}] - [x_1 \ldots x_j]}{x_o - x_j} = [x_o \ldots x_j].$$

Case 2, $n < j$. If $n = j-1$, then by the induction hypothesis $[xx_1 \ldots x_{j-1}]$ is a polynomial of degree $n-j+1 = j-1-j+1 = 0$, that is, a constant, say $[xx_1 \ldots x_j] = c$. If $x = x_j$, then $[x_j x_1 \ldots x_{j-1}] = c$, and by Corollary 3, $[x_1 \ldots x_{j-1} x_j] = c$.

$$\text{So } [xx_1 \ldots x_j] = \frac{[xx_1 \cdots x_{j-1}] - [x_1 \ldots x_j]}{x - x_j}$$

$$= \frac{c - c}{x - x_j} = 0.$$

If $n > j-1$, then by the induction hypothesis the $(j-1)^{th}$ order differences are 0 and, as above with $c = 0$, $[xx_1 \ldots x_j] = 0$.

We know that for any finite field F each function $f: F \to F$ may be represented by a polynomial over F of degree less than or equal to k-1. We know that for each polynomial of degree n the n+1 order differences and all higher order differences are 0. Hence, we know that for the polynomial representation of each function f, the k order differences are 0. (Differences of order higher than k are not defined.)

We can now prove the main result:

Theorem 6 (Newton's Interpolation Formula with Divided Differences): If $\langle F, +, * \rangle$ is a finite field of k elements and if $f: F \to F$ is a function, and if $x_1, x_2, \ldots, x_k$ is a permutation of the elements of F, then f is given by the polynomial:

$$f(x) = f(x_1) + \sum_{i=1}^{k-1} (x - x_1)(x - x_2)\ldots(x - x_i)[x_1 x_2 \ldots x_{i+1}].$$

proof: Reversing the order of the terms on the right side of Definition 5, we obtain:

$$[xx_1 \ldots x_k] = -\frac{[x_1 x_2 \ldots x_k]}{x - x_k} + \frac{[xx_1 \ldots x_{k-1}]}{x - x_k}.$$

$$[xx_1 \ldots x_{k-1}] = -\frac{[x_1 x_2 \ldots x_{k-1}]}{x - x_{k-1}} + \frac{[xx_1 \ldots x_{k-2}]}{x - x_{k-1}}$$

$$[xx_1 \ldots x_{k-2}] = -\frac{[x_1 x_2 \ldots x_{k-2}]}{x - x_{k-2}} + \frac{[xx_1 \ldots x_{k-3}]}{x - x_{k-2}}$$

.

.

.

$$[xx_1x_2] = -\frac{[x_1x_2]}{x - x_2} + \frac{[xx_1]}{x - x_1}$$

$$[xx_1] = -\frac{f(x_1)}{x - x_1} + \frac{f(x)}{x - x_1}$$

Note that in each line except the last the numerator of the second term on the right is the left side of the succeeding line. Repeated substitutions yield:

$$[xx_1x_2\ldots x_k] = -\frac{[x_1x_2\ldots x_k]}{x - x_k} - \frac{[x_1x_2\ldots x_{k-1}]}{(x - x_k)(x - x_{k-1})}$$

$$- \frac{[x_1x_2\ldots x_{k-2}]}{(x - x_k)(x - x_{k-1})(x - x_{k-2})}$$

$$- \ldots$$

$$- \frac{[x_1x_2]}{(x - x_k)\ldots(x - x_2)}$$

$$- \frac{f(x_1)}{(x - x_k)\ldots(x - x_1)}$$

$$+ \frac{f(x)}{(x - x_k)\ldots(x - x_1)}$$

This may be rewritten:

$$f(x) = f(x_1) + (x-x_1)\,[x_1x_2] + (x-x_1)(x-x_2)\,[x_1x_2x_3]$$
$$+ \ldots$$
$$+ (x-x_1)(x-x_2)\ldots(x-x_{k-1})\,[x_1x_2\ldots x_k]$$
$$+ (x-x_1)(x-x_2)\ldots(x-x_k)\,[xx_1x_2\ldots x_k].$$

Inspecting the last term, we note that the product

$(x-x_1)(x-x_2)\ldots(x-x_k)$

is a permutation of the product $Z_k(x)$ of Definition 1. $Z_k(x) = 0$ for all x in F. Further, $[xx_1 \ldots x_k]$ is a k order difference of f, a polynomial of degree at most k-1. Hence $[xx_1 \ldots x_k]$ is 0, that is, the last term is 0; the theorem is true.

Example 1:- Let k=5 and let f and its differences be given in the table:

x	f(x)					
0	1					
		2				
1	3		1			
		4		0		
2	2		1		0	
		1		0		
3	3		1			
		3				
4	1					

Then $f(x) = 1 + 2x + x(x-1) = 1 + 2x + x(x+4) = 1 + x + x^2$.

Example 2:- Let $k = 5$ and let V_3 and its differences be given in the table:

x	$V_3(x)$				
0	0				
		0			
1	0		0		
		0		1	
2	0		0		4
		1		2	
3	1		4		
		4			
4	0				

Then $V_3(x) = x(x-1)(x-2) + 4x(x-1)(x-2)(x-3)$

$= 4x^4 + 2x^3 + x^2 + 3x$

Example 3:- The same as Example 2, but permute the order of the values of x.

x	$V_3(x)$				
0	0				
		0			
2	0		0		
		0		0	
4	0		0		4
		0		1	
1	0		2		
		3			
3	1				

Then $V_3(x) = 4x(x-2)(x-4)(x-1) = 4x(x+1)(x+3)(x+4)$

$= 4x^4 + 2x^3 + x^2 + 3x$.

Example 4:- Let $k = 4$ and let $V_2(x)$ and its differences be given in the table:

x	$V_2(x)$			
0	0			
		0		
1	0		1	
		2		1
2	1		2	
		1		
3	0			

Then $V_2(x) = x(x-1) + x(x-1)(x-2) = x(x+1) + x(x+1)(x+2)$

$= x(x+1)(1+x+2)$

$= x(x+1)(x+3)$

$= x^3 + 2x^2 + 3x$

IV. Functions of Two Variables

The notation of Definition 5 does not lend itself to generalization to the case of a function of more than one variable. We introduce here a notation closer to that which has developed for the differential calculus.

Let f: $F^2 \to F$ and let $x_0, x_1, \cdots, x_{k-1}$ and $y_0, y_1, \cdots, y_{k-1}$, be two (not necessarily distinct) permutations of F.

Definition 6:-

$$D_x^1 f(x_i,y_j) = \frac{f(x_i,y_j) - f(x_{i+1},y_j)}{x_i - x_{i+1}}$$

$$D_y^1 f(x_i,y_j) = \frac{f(x_i,y_j) - f(x_i,y_{j+1})}{y_j - y_{j+1}}$$

$$D_x^p f(x_i,y_j) = \frac{D_x^{p-1} f(x_i,y_j) - D_x^{p-1} f(x_{i+1},y_j)}{x_i - x_{i+p}}$$

$$D_y^p f(x_i,y_j) = \frac{D_y^{p-1} f(x_i,y_j) - D_y^{p-1} f(x_i,y_{j+1})}{y_j - y_{j+p}}$$

By analogy, we have in the one variable case:

$D_x^1 f(x_i) = [x_i x_{i+1}]$, and

$D_x^p f(x_i) = [x_i x_{i+1} \cdots x_{i+p}]$.

By analogy to the differential calculus, one may prove that $D_x^p D_y^q f(x_i,y_j) = D_y^q D_x^p f(x_i,y_j)$ and also develop formulae evocative of the sum, product, and quotient formulae of the differential calculus.

Finally, we may reformulate Newton's Theorem in terms of a function of two variables:

Theorem 7:- If $\langle F, +, * \rangle$ is a finite field of k elements and if $f: F^2 \to F$ is a function, and if $x_1, x_2, \ldots, x_k$ and $y_1, y_2, \ldots, y_k$ are two permutations of F, then f is given by the polynomial:

$$f(x,y) = f(x_1,y_1) + \sum_{i=1}^{k-1} D_x^i f(x_1,y_1)(x-x_1)\ldots(x-x_i) +$$

$$\sum_{i=1}^{k-1} D_y^i f(x_1,y_1)(y-y_i)\ldots(y-y_i) +$$

$$\sum_{i,j=1}^{k-1} D_x^i D_y^j f(x_1,y_1)(x-x_1)\ldots(x-x_i)(y-y_1)\ldots(y-y_j).$$

Multiplication of the terms yields a form analogous to the form of Theorem 3, namely:

$$f(x,y) = \sum_{i,j=o}^{k-1} a_{ij} x^i y^j. \qquad (*)$$

The organization on paper of difference tables is not as easy in the two variable situation, but the tables may be conveniently implemented in a high level computer language with the capacity for defining recursive functions. In order to be reasonably efficient one needs to save the values of differences as they are computed.

Each of five functions was defined by a polynomial over GF(9) and over GF(16). The last function is defined by:

$$\text{Order } (x,y) = \begin{cases} 1, & \text{if } x < y; \\ 0, & \text{if } x = y; \\ -1, & \text{if } x > y. \end{cases}$$

(Here, as usual, the high integers are taken to be negative.) The table below indicated the number of terms in each polynomial definition. The columns labelled UE are the number of terms in the polynomial in its unexpanded form, that is, in the form given by Theorem 7; the columns marked E are the number of terms in the polynomial in the form (*). The reader might note that a polynomial over GF(9) might have 81 terms while a polynomial over GF(16) might have 256 terms.

In the expanded form (*) the representation of the function is unique. In the form given in Theorem 7, the representation depends upon the particular permutation of the elements of F chosen for $x_1, \ldots, x_k$ and $y_1, \ldots, y_k$.

The most extensive bibliographies on difference methods are in [1] and [7].

Table

Function	GF(9)		GF(16)	
	UE	E	UE	E
x+y (mod k)	17	18	124	124
x*y (mod k)	17	21	129	174
x+y (mod k-1)	42	69	134	233
x*y (mod k-1)	50	48	161	206
Order (x,y)	57	55	184	163

References

1.) C.R. Adams, "Linear q-difference Equations", Bull. Amer. Math. Soc. 37 (1931), pp. 361-400.

2.) N.N. Aizenberg, I.V. Semion, and A.I. Tsitkin, "Polynomial Representations of Logical Functions" translated in Automatic Control 5 (1971), pp. 5-11.

3.) Tomlinson Fort, Finite Differences, (Oxford: Clarendon Press, 1948).

4.) Charles Jordan, Calculus of Finite Differences, (New York: Chelsa Publishing Company, 1947).

5.) L.M. Milne-Thompson, The Calculus of Finite Differences, (London: Macmillan and Sons, 1961).

6.) Isaac Newton, "Approaches to a General Theory of Finite Differences" 1675-6 in D.T. Whiteside (editor), The Mathematical Papers of Issac Newton, vol. 4, (Cambridge: The University Press, 1971), pp. 14-73.

7.) Niels Erik Norlund, Vorlesungen uber Differenzenrechnung, (Berlin: Springer, 1924).

8.) Irving S. Reed, "A Class of Multiple-error-correcting codes and the Decoding Scheme", Trans. IRE - Info. Theory PGIT-4 (1954), pp. 38-49.

9.) Claude E. Shannon, "A Symbolic Analysis of Relay and Switching Circuits", Trans. Am. Inst. Elec. Eng., 57 (1938), pp. 713-23.

T.C. Wesselkamper
Dept. of Computer Science
Virginia Polytechnic Institute and State University
Blacksburg, Virginia 24061