The Algebraic Representation of Partial Functions

by

T. C. Wesselkamper

Technical Report CS78009-R

August 1978

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

Abstract

The paper presents a generalization of the theorem which states that any (everywhere defined) function from a finite field $GF(p^n)$ into itself may be represented at a polynomial over $GF(p^n)$. The generalization is to partial functions over $GF(p^n)$ and exhibits representations of a partial function f by the sum of a polynomial and a sum of terms of the form $a/(x-b)^i$, where b is one of the points at which f is undefined. Three such representation theorems are given. The second is the analog of the Mittag-Leffler Theorem of the theory of functions of a single complex variable. The main result of the paper is that the sum of the degree of the polynomial part of the representation and the degrees of the principal parts of the representation need be no more than $\max(|A|, |B|)$ where A is the set upon which the function is defined and B is the set upon which the function is undefined.

Key Words: Partial function, representation, finite field, principal part.

CR Categories: 6.1, 8.9

MR Categories: 12C99, 02C05

Theoretical Computer Science is, in part, concerned with finite spaces of words, that is, with n-tuples each element of which is from a space $E(p) = \{0, 1, \ldots, p-1\}$. Traditionally $p = 2$ and $E(p) = \{0, 1\}$, but recent advances in integrated circuit technology make it practical to consider $p = 3$, $p = 4$, and even higher values [1, 2, 3]. Herein we shall be concerned with n position p-ary words, that is with the space $E^n(p)$ for some prime p and some natural number n. Since there is a natural isomorphism between $E^n(p)$ and $E(p^n)$, we may consider our words to be elements of the latter.

Over such a space $E(p^n)$ we are concerned with partial functions, that is, with a subset, say f, of the Cartesian product $E(p^n) \times E(p^n)$ such that if $(a, b) \in f$ and $(a, c) \in f$, then $b = c$. If for each a in $E(p^n)$ there exists an element b in $E(p^n)$ such that $(a, b) \in f$, then f is called a function or a total function in the usual way. Intuitively, a partial function is a mapping which is somewhere defined and somewhere undefined. The usual method used for representation of a partial function is to replace the partial function by some polynomial which coincides with the partial function on its domain of definition. In many cases this is not a very satisfactory approach. It is preferable to have a representation which is defined where the partial function is defined and undefined where the partial function is undefined.

In this paper we develop a sequence of representations for partial functions of the form $f = P + Q$, where P is a polynomial over $GF(p^n)$ and Q is a sum of terms of the form $a/(x-b)^i$.

1. Preliminaries

Definition 1: If p is a prime and n is a natural number let $k = p^n$ and $K = k-1$.

Definition 2: If $A \subset E(k)$, then $|A|$ denotes the cardinality of the set A.

Definition 3: If $P(x) = \sum_{i=0}^{K} a_i x^i$, a polynomial over $GF(k)$, then $|P| = \max \{i: a_i \neq 0\}$, that is $|P|$ is the degree of the polynomial P. The degree of a nonzero constant is zero. As is usual, the degree of the constant zero is defined: $|0| = -1$.

Definition 4: If $(c_1, c_2, \ldots, c_r)$ is a sequence of r elements of $E(k)$ then $(c_1, c_2, \ldots, c_r) = 0$ if and only if for all i, $(1 \leq i \leq r)$, $c_i = 0$.

Definition 5: If $b \in E(p^n)$ and $(c_1, c_2, \ldots, c_K) \neq 0$ is a sequence of elements of $E(k)$, then h_b, called a principal part of b, is defined by: $h_b(x) = \sum_{i=0}^{K} c_i/(x-b)^i$.

Definition 6: If $b \in E(k)$ and h_b is a principal part of b, then $|h_b| = \max\{i: c_i \neq 0\}$, the degree of the principal part h_b.

It is always clear from the context which of the uses of the vertical bars is intended.

Throughout this paper we use the following lemma which is proved in [4].

Lemma 1: If f is a partial function defined on $A \subset E(k)$, then there exists a polynomial P of degree $|P| \leq |A| - 1$, such that if $x \in A$, then $f(x) = P(x)$.

The proof of the lemma is a straightforward construction using Newton's Divided Difference Method. We say in this case that P represents f on A.

There are two representation theorems which may be proven very simply.

Theorem 1: If f is a partial function defined on A and undefined on $E - A = B = \{b_1, b_2, \ldots, b_r\}$ then there is a polynomial P of degree $|P| = |A| - 1$, such that $f(x) = P(x) + \sum_{i=1}^{r} (x - b_i)^{-1}$.

proof: Let $g(x) = \sum_{i=1}^{r} (x - b_i)^{-1}$. Now g(x) is defined on A and undefined on B. Hence f - g is defined on A and undefined on B, and by Lemma 1 there is a polynomial P of degree $|P| \leq |A| - 1$, which represents f - g on A. For each x in E(k), $f(x) = P(x) + g(x)$, while for each x in B, P + g is undefined.

The second theorem is the finite field counterpart of a classical theorem from the theory of functions of a single complex variable, where it is called the Mittag-Leffler Theorem [5].

Theorem 2: If f is a partial function defined on $A \subset E(k)$ and undefined on $E - A = B = \{b_1, b_2, \ldots, b_r\}$, and if $\{h_{b_i} : 1 \leq i \leq r\}$ is a set of principal parts of the elements b_i, then there is a polynomial P of degree $|P| \leq |A| - 1$, such that for all $x \in E(k)$

$$f(x) = P(x) + \sum_{i=1}^{r} h_{b_i}(x).$$

proof: Let $g(x) = \sum_{i=1}^{r} h_{b_i}(x)$. Exactly as in Theorem 1, represent f - g on A by a polynomial P of degree $|P| \leq |A| - 1$. Now for all x, $f(x) = P(x) + g(x)$, for if x is in B, g(x) is undefined, while if x is in A, $P(x) = f(x) - g(x)$.

Note that in the case of Theorem 1, the degree $|P| + |g| \leq |A| - 1 + |B| = k - 1$. For Theorem 2, for each b_i the degree $|h_{b_i}| \geq 1$. Hence $|g| \geq r = |B|$ and $|P| \leq |A| - 1$. Thus there is no precise way to predict the degree $|P| + |g|$ of the representation. One somehow feels that making the degree of g high ought to enable one to choose P with a low degree. The next section gives a precise formulation to this intuitive feeling about the degree of the representation.

2. The Main Theorem.

In proving the main theorem of this paper we use the following lemma.

Lemma 2: If $r < k$ and A is an r by r matrix over $GF(k)$, $\det(A) \neq 0$, and $\bar{x} = (x_1, \ldots, x_r)^T$ and $\bar{b} = (b_1, \ldots, b_r)^T$, then the system $A\bar{x} = \bar{b}$ has a solution $\bar{x} = \bar{c} = (c_1, \ldots, c_r)^T$, such that $c_i \neq 0$, $(1 \leq i \leq r)$. This is called a strictly nonzero solution of the system.

proof: If $\bar{x} = \bar{d} = (d_1, \ldots, d_r)^T$ is a solution to the homogeneous system $A\bar{x} = 0$, and $\bar{x} = \bar{e} = (e_1, \ldots, e_r)$ is a solution to the inhomogeneous system $A\bar{x} = \bar{b}$, then for each $\alpha \in E(k)$, $\alpha\bar{d} + \bar{e}$ is a solution of $A\bar{x} = \bar{b}$. Partition these k solutions into $r+1 \leq k$ classes, $S_0, S_1, \ldots, S_r$, as follows: a solution $\alpha\bar{d} + \bar{e}$ is in class S_i if $\alpha d_i + e_i = 0$ and for all $j < i$, $\alpha d_j = e_j \neq 0$; if $\alpha\bar{d} + \bar{e}$ contains no nonzero component it is placed in class S_0. If there is a solution is class S_0 that solution is strictly nonzero and the lemma is proved, so suppose that S_0 is empty. Then the k (>r) solutions are partitioned into the r class $S_1, \ldots, S_r$, and by the pigeon hole principle some class S_i contain two solutions, say $\alpha\bar{d} + \bar{e}$ and $\beta\bar{d} + \bar{e}$, and each of these has its i^{th} component equal to zero: $\alpha d_i + e_i = \beta d_i + e_i = 0$. But since e_i and d_i cancel, we have $\alpha = \beta$, which is a contradiction.

Hence S_0 is not empty and there exists at least one strictly non-zero solution to $A\bar{x} = \bar{b}$.

Theorem 3: If f is a partial function defined on $A \subset E(k)$ and undefined on $E - A = B = \{b_1, \ldots, b_r\}$ and if c_0 is a non-negative integer and $c_1, \ldots, c_r$ are natural numbers such that $\sum_{i=0}^{r} ci = \max(|A|, |B|)$, then there exist a polynomial P and principal parts h_{b_i} such that $f = P + \sum_{i=1}^{r} h_{b_i}$ and $|P| < c_0$ and for all i, $(1 \leq i \leq r)$, $|h_{b_i}| \leq c_i$.

proof: There are six cases.

Case 1: $A = \phi$

Let $P = 0$ and let $h_{b_i}(x) = 1/(x-b_i)$ for each b_i in $B = E(k)$.

Then $f(x) = P(x) + \sum_{i=1}^{k} h_{b_i}(x) = \sum_{i=1}^{k} h_{b_i}(x)$, which is everywhere undefined.

For all i, $|h_{b_i}| = 1 \leq c_i$, since the c_i are natural numbers, and $|P| = -1 < c_0$, since c_0 is non-negative.

Case 2: $B = \phi$.

Since f is everywhere defined, f is represented by a polynomial of degree at most K, by Lemma 1.

Case 3: $|A| = |B|$. Let $A = \{a_1, \ldots, a_r\}$.

This can occur, of course, only if $p = 2$. Consider the system of equations $D\bar{x} = (f(a_1), f(a_2), .., f(a_r))^T$ (*)

where $\bar{x} = (x_1, x_2, \ldots, x_r)^T$ and $D = (d_{ij})$, $d_{ij} = 1/(a_i - b_j)$.

The matrix D is an example of an alternant [6, pp. 321-363], and

$$\det(D) = \pm \prod_{i<j} (a_i - a_j) \prod_{i<j} (b_i - b_j) / \prod_{i,j=1}^{r} (a_i - b_j).$$

Since A and B are disjoint sets, each of the factors $(a_i - b_j)$ is nonzero, hence det(D) exists. Since $i < j$ implies that $a_i - a_j \neq 0$ and $b_i - b_j \neq 0$, $\det(D) \neq 0$, and the system (*) has a solution. By Lemma 3 the system has a strictly nonzero solution, say $\bar{x} = \bar{d} = (d_1, \ldots, d_r)$. Let $P = 0$ and for each i let $h_{b_i}(x) = d_i/(x - b_i)$.

For each $a_j \in A$ we have

$$\sum_{i=1}^{r} h_{b_i}(x) = \sum_{i=1}^{r} d_i/(a_j - b_i) = f(a_j),$$ and for each $b_j \in B$, h_{b_j} is undefined. Finally $|P| = -1 < c_0$ and for each i, $|h_{b_i}| = 1 \leq c_i$.

Case 4: $|A| < |B|$. Let $A = \{a_1, \ldots, a_s\}$.

Consider the s equations:

$$\sum_{i=1}^{s} x_i/(a_j - b_i) = f(a_j) - \sum_{i=s+1}^{r} 1/(a_j - b_i), \quad (1 \leq j \leq s). \qquad (**)$$

This system of s equations in s unknowns has a strictly nonzero solution by the same argument as in Case 3, say $(x_1, \ldots, x_s) = (d_1, \ldots, d_s)$. Let $P = 0$

$$\text{and let } h_{b_i}(x) = \begin{cases} d_i/(x - b_i), & \text{if } 1 \le i \le s; \\ 1/(x - b_i), & \text{if } s+1 \le i \le r. \end{cases}$$

Again $f(x) = \sum_{i=1}^{r} h_{b_i}(x)$, $|P| = -1^{c_0}$, and $|h_{b_i}| = 1 \le c_i$, for $1 \le i \le r$.

Case 5: $|B| < |A|$, $c_0 = 0$. Let $A = \{a_1, \ldots, a_s\}$.

Let the matrix D be defined as follows: for each i, $(1 \le i \le r)$, D contains the c_i columns,

$$(1/(a_1 - b_i), 1/(a_2 - b_i), \ldots, 1/(a_s - b_i))^T,$$

$$(1/(a_1 - b_i)^2, 1/(a_2 - b_i)^2, \ldots, 1/(a_s - b_i)^2)^T,$$

$$\ldots$$

$$(1/(a_1 - b_i)^{c_i}, 1/(a_2 - b_i)^{c_i}, \ldots, 1/(a_s - b_i)^{c_i})^T.$$

Since $\sum_{i=1}^{r} c_i = \max(|A|, |B|) = s$, this is an s by s matrix.

Let $\bar{x} = (x_1, \ldots, x_s)$ and consider the system

$$D\bar{x} = (f(a_1), f(a_2), \ldots, f(a_s))^T. \qquad (***)$$

The matrix D is again an alternant, and by [6, p. 360],

$$\det(D) = \pm \prod_{i<j} (a_i - a_j) \prod_{i<j} (b_i - b_j) / \prod_{i,j=1}^{s,r} (a_i - b_j)^{c_j}.$$

This determinant D exists and is nonzero and the rest of the argument is in Case 3.

Case 6: $|B| < |A|$, $c_0 > 0$. Let $A = a_1, \ldots, a_s$.

Let the matrix D be formed in the following way:

there are c_0 columns,

$(1, 1, \ldots, 1)^T$,

$(a_1, a_2, \ldots, a_s)^T$,

$(a_1^2, a_2^2, \ldots, a_s^2)^T$

$\ldots$

$(a_1^{c_0}, a_2^{c_0}, \ldots, a_s^{c_0})^T$;

followed, for each c_i, $(1 \le i \le r)$, by c_i columns,

$(1/(a_1 - b_i), 1/(a_2 - b_i), \ldots, 1/(a_s - b_i))^T$,

$(1/(a_1 - b_i)^2, 1/(a_2 - b_i)^2, \ldots, 1/(a_s - b_i)^2)^T$,

$\ldots$

$(1/(a_1 - b_i)^{c_i}, 1/(a_2 - b_i)^{c_i}, \ldots, 1/(a_s - b_i)^{c_i})^T$.

This matrix D is again an alternant, and by [6, pp. 322, 360].

$$\det(d) = \prod_{i<j} (a_i - a_j) \prod_{i<j} (b_i - b_j) / \prod_{i,j=1}^{s,r} (a_i - b_j).$$

Thus det(D) exists and is nonzero and so the system of equations

$$D\bar{x} = (f(a_1), f(a_2), \ldots, f(a_s))^T \qquad (****)$$

has a strictly nonzero solution, say, $(x_1, \ldots, x_s) = (d_1, \ldots, d_s)$.

Let $P(x) = d_1 + d_2 x + \ldots + d_{c_0} x^{c_0 - 1}$, and

$$h_{b_1}(x) = d_{c_0+1}/(x - b_1) + d_{c_0+2}/(x - b_1)^2 + \ldots + d_{c_0+c_1}/(x - b_1)^{c_1},$$

$\ldots$

$$h_{b_r}(x) = d_{c_0+\ldots+c_{r-1}+1}/(x - b_r) + \ldots + d_{c_0+\ldots+c_r}/(x - b_r)^{c_r}.$$

Since the d_i are the components of the solution of (****), for each $a_j \in A$, $P(a_j) + \sum_{i=1}^{r} h_{b_i}(a_j) = f(a_j)$, and for each $b_j \in B$, $h_{b_j}(b_j)$ is undefined. $|P| = c_0 - 1 < c_0$ and $|h_{b_i}| = c_i$. This concludes the proof of the theorem.

Note that in Cases 5 and 6 it is not necessary that $\bar{x}$ only nonzero components, but only that sufficiently many components be nonzero that each h_{b_i} exist. In other words, it is sufficient that for each i, $(1 \leq i \leq r)$ there exist a j_i such that $d_{j_i} \neq 0$, where $\sum_{t=0}^{i-1} c_t < j_i \leq \sum_{t=0}^{i} c_t$.

For some fixed set of constants c_i, $(0 \leq i \leq r)$, one could define that representation to be optimal which had the fewest nonzero terms in $P + \Sigma h_{b_i}$, but there does not appear to be an easy way to construct such an optimal representation.

References

1. A. S. Wojcik, "On the Design of Three-valued Asynchronous Modules", Proceedings, Seventh International Symposium on Multiple-valued Logic, Charlotte, NC, May 1977, pp. 55-63.

2. E. J. McCluskey, "Logic Design of Multi-valued I^2L Logic Circuits" Proceedings, Eighth International Symposium on Multiple-valued Logic, Chicago, IL, May 1978, pp. 23-31.

3. A. D. Singh and J. R. Armstrong, "A Simultaneous Radix 4, I^2L Multiplier Mechanized Via Repeated Additions", Proceedings, Eighth International Symposium on Multiple-valued Logic, Chicago, IL, May, 1978, pp. 114-121.

4. T. C. Wesselkamper, "Divided Difference Methods for Galois Switching Functions", IEEETC C-27 (3) (March 1978), pp. 232-8.

5. Konrad Knopp, Theory of Functions, Part Two (trans. F. Bagemihl) (New York: Dover, 1947) pp. 34-57.

6. Thomas Muir, A Treatise on the Theory of Determinants (rev. William H. Metzler), (New York: Dover, 1960).