Technical Report CS74008-R

Three Papers on the Completeness Properties of Abelian Semigroups and Groups

T. C. Wesselkamper

Department of Computer Science

College of Arts and Sciences

Virginia Polytechnic Institute and State University

Blacksburg, Virginia 24061

March 1974

Abstract

The three papers presented here all arise from recent research into sets of operators which are sufficient to define a horizontal microlanguage for a computer and which are (in some undefined sense) natural for human beings to use. It is this criterion of naturalness which leads us to consider dyadic operators which are commutative and associative, that is, structures which are abelian semigroups.

The first paper will be presented at the 1974 International Symposium on Multiple-valued Logics. It discusses the necessary and sufficient conditions for functional completeness due to Ivo Rosenberg and the application of those conditions in the situation in which one is permitted to use the constants of the space in a functional definition. We establish that for a single group operation to be functionally complete it is necessary that the group be nonabelian and simple. The sufficiency of this condition has been announced elsewhere (Reference 3 of that paper). The paper ends with a proof that for each natural number k the exist three abelian semigroups defined on the space of k elements whose group operations form a functionally complete set (in the weak sense that the constants may be used in definitions).

The second paper has been submitted to the Zeitschrift fur Math. Logik und Grundlagen der Math. It contains an analog of the Shannon Decomposition Theorem on a space of k elements and uses that Decomposition Theorem to give a much improved proof of the theorem on the completeness of three abelian semigroups.

The last paper has been submitted to the Mathematical Notes section of the American Mathematical Monthly. It is an extension of a theorem which

recently appeared in that section. The two notes taken together imply that it is a necessary and sufficient condition for two ring operations to be functionally complete that the ring be a finite field. Since two of the three operators used in the first two papers form a ring over the space, this shows that the results of those papers are best possible in the sense that if ring operations are used at all (a fairly natural thing to do) then in the general case at least one additional operator is required.

Some Completeness Results for Abelian Semigroups and Groups

by

T. C. Wesselkamper*

1. Some Observations about Weak Completeness.

Let $E(k) = \{0, 1, \ldots, k-1\}$, $(k \leq 3)$. If A is a set of functions with values in $E(k)$ and variables over $E(k)$, then A is called a complete set of functions if each function over $E(k)$ can be expressed as a composition of functions of A. A is called weakly complete if every function over $E(k)$ can be expressed as a composition of functions of A together with the constants of $E(k)$, that is, if the set $A \cup E(k)$ is complete. Thus, over the space $\{0, 1\}$ the set consisting of the single function 'nand' is complete while the set consisting of the single function 'implication' is weakly complete. Since each of these sets consists of a single function, these functions are called Sheffer and weakly Sheffer, respectively.

The results reported in this paper arise out of research into sufficient sets of operators to define a horizontal microlanguage on a computer with fixed word size. In this context, since the constants are always available, weak completeness is quite sufficient. The constraints that the operators be commutative and associative arises from a desire that the operators be natural (in some undefined sense).

* Author's address: Department of Computer Science, Virginia Polytechnic
Institute and State University, Blacksburg, Virginia

Ivo Rosenberg has given a set of necessary and sufficient conditions that a set of functions over E(k) be complete [1, 2]. In this paper all of the functions will be functions of one or two variables. Except for this specialization the terminology and definitions of this paper are those of Rosenberg.

Let f be a function of one variable. Let s be a permutation of E(k). Then f is selfdual with respect to s if for each $a \in E(k)$ we have:

$$f(s(a)) = s(f(a)).$$

Let f_a denote the constant function with value a.

Lemma 1: If s is a non-identical permutation of E(k) then there is a constant function of E(k) which is not selfdual with respect to s.

proof: Suppose s contains the cycle (a b ...).

Then $s(f_a(a)) = s(a) = b$, while $f_a(s(a)) = f_a(b) = a$.

It follows that a set of functions which contains the constant functions contains, for each permutation s, a function which is not selfdual with respect to s. This means that Rosenberg's second condition for completeness is always trivially satisfied for weak completeness.

2. Some Results Concerning Groups.

In this section we describe a group as Sheffer (weakly Sheffer) when its group operation is Sheffer (weakly Sheffer).

A relation $\leq$ is called a partial order of E(k) if it is reflexive, transitive, and antisymmetric.

Rosenberg's first condition requires that if a set A of functions is complete then for each partial order of E(k) with a greatest element and a least element, the set A of functions contains an element which is not monotonic with respect to the order relation.

Lemma 2: If $\leq$ is an order of $E(k)$ with a greatest element and a least element, and if $<E(k), *>$ is a group, then the group operation $(*)$ is not monotonic with respect to the order.

proof: Let T and t be the greatest element and the least element of $E(k)$, respectively. Then there exists an $a \in E(k)$ such that $a * T = t$, since $<E(k), *>$ is a group. Now $t \leq T$ and $a \leq a$. Assume that the group operation is monotonic. Then $a*t \leq a*T = t$. Since t is the least element, we must have $a*t = t$, that is, a is the identity element of the group. But then $T = a*T = t$, that is, the greatest and least elements are equal and so $k = 1$. This contradicts our original assumption about k.

A function f of two variables is quasilinear with respect to a group G if for all $a, b, c, d \in E(k)$ we have:

$$f(a+c, b+d) = f(a, b) + f(c, d) - f(0,0),$$

where + and - are atdition and multiplication in F and 0 is the identity element of G.

Rosenberg's third condition is that if $k = p^m$ (where p is prime and m a natural number), then for each group G over $E(k)$ such that the order of G is p, A contains a function which is not quasilinear with respect to G.

Lemma 3: There exists no group of prime order whose group operation is Sheffer (weakly Sheffer).

proof: If $k = p$, a prime, then all groups over $E(k)$ are isomorphic to the cyclic group of order p. Choose the group G so that the two groups are isomorphic under the identity mapping. Since the cyclic groups are abelian, we have:

$$(a + c) + (b + d) = (a + b) + (c + d) - (0 + 0),$$

that is, the group operation is quasilinear with respect to itself. Hence, no group of prime order is Sheffer. But since the constant functions are quasilinear, no group of prime order is weakly Sheffer.

Non-simple groups of composite order fare no better.

Rosenberg's fourth condition is that for each non-universal, non-trivial equivalence relation on $E(k)$, the set of functions A contains a function which does not preserve that relation.

Lemma 4: No non-simple group of composite order is Sheffer (weakly Sheffer).

proof: Let $<E(k), *>$ be a non-simple group of composite order. Since the group is non-simple it contains a proper normal subgroup, say H, of index h in $E(k)$. Let $E(k) = H + a_1H + \ldots + a_{h-1}H$ be a left coset decomposition of $E(k)$. The disjoint cosets of this decomposition induce an equivalence relation on $E(k)$ which is neither trivial nor universal. But since the mapping $x \rightarrow xH$ is a homomorphism from $E(k)$ into the factor group $E(k)/H$, the group operation preserves the equivalence relation induced by the coset decomposition. Hence a non-simple group of composite order is not Sheffer. However, since the constant functions preserve every equivalence relation, a non-simple group of composite order is not weakly Sheffer either.

Theorem 1: No abelian group over $E(k)$ is weakly Sheffer. No non-simple, non-abelian group is weakly Sheffer.

proof: Lemmas 4 and 5.

3. A Positive Result.

As has been seen, Rosenberg's conditions are particularly useful in establishing negative results. They are more difficult to use to establish positive results. In this section we use a constructive proof method.

Define the following three operations on E(k) for each $k \geq 2$:

$$Jxy = \begin{cases} 0, \text{ if } x = 0 \text{ or } y = 0, \text{ but not both;} \\ 1, \text{ otherwise.} \end{cases}$$

$$Pxy = x + y \pmod{k}.$$

$$Txy = xy \pmod{k}. \qquad (1)$$

It is easy to show that each of these operations defines an abelian semigroup over E(k).

For each $j \in E(k)$ let j^* denote $k-j \pmod{k}$. From elementary group properties it is clear that $x = j^*$ is the unique solution of the equation $x + j = 0$, that is, $x = j^*$ is the unique solution of $Pxj = 0$.

We define the functions:

$$V_jx = J0Pxj^*, \ (0 \leq j \leq k-1) \qquad (2)$$

Lemma 5:

$$V_jx = \begin{cases} 1, \text{ if } x = j; \\ 0, \text{ if } x \neq j. \end{cases}$$

proof: If $x = j$, then $V_jx = V_jj = J0Pjj^{**} = J00 = 1$. On the other hand, if $x \neq j$, then $Pxj^* \neq 0$ and $V_jx = J0Pxj^* = 0$.

We define the function:

$$Kxy = TJ1xJ1y \qquad (3)$$

Lemma 6:

$$Kxy = \begin{cases} 0, \text{ if } x = 0 \text{ or } y = 0; \\ 1, \text{ otherwise.} \end{cases}$$

proof: There are three cases:

Case 1: $x = y = 0.$

$Kxy = TJ10J10 = T00 = 0.$

Case 2: $x \neq y = 0.$

$Kxy = TJ1xJ10 = T10 = 0.$

Case 3: $x \neq 0$ and $y \neq 0.$

$Kxy = TJ1xJ1y = T11 = 1.$

Suppose that $x_1, x_2, \ldots, x_n$ are n variables over the space $E(k)$. Let $t_1, t_2, \ldots, t_n$ be elements of $E(k)$. Let Q be the state defined by:

Q: $x_1 = t_1, x_2 = t_2, \ldots, x_n = t_n.$

We define the function:

$$X_Q(x_1, \ldots, x_n) = KV_{t_1}x_1KV_{t_2}x_2K\ldots KV_{t_{n-1}}x_{n-1}V_{t_n}x_n. \tag{4}$$

Henceforth we denote $(x_1, \ldots, x_n)$ by $\overline{x}$.

Lemma 7: $X_Q\overline{x}$ is a characteristic function for Q over $E^n(k)$.

proof: If $\overline{x}$ is in the state Q, then $V_{t_i}x_i = 1$ for $1 \leq i \leq n$.

Hence $X_Q\overline{x} = K1K1K\ldots K11$, and since $K11 = 1$, $X_Q\overline{x} = 1$. if $\overline{x}$ is in a state other than Q then there exists ar least one index $i*$ such that $x_{i*} \neq t_{i*}$, that is, $V_{t_{i*}}x_{i*} = 0$. Hence $X_Q\overline{x} = 0$.

Now we want to show that if we have a function f of the n variables $x_1, \ldots, x_n$ and if in the state Q,f takes on a value different from r, then we can define, in terms of f and the semigroups of (1), a function f' which has the same value as f in all states except Q and which has the value r in the state Q. Said in another way, we can modify the definitional table for f at exactly one point.

We define:

$$f' = PTX_{Q}rTJ0X_{Q}f. \tag{5}$$

<u>Lemma 8</u>: $f'\overline{x} = \begin{cases} f\overline{x}, \text{ if } \overline{x} \text{ is not in the state } Q; \\ r, \text{ if } \overline{x} \text{ is in the state } Q. \end{cases}$

<u>proof</u>: Suppose $\overline{x}$ is in the state Q. Then $X_{Q} = 1$, and

$$\begin{aligned} f' &= PT1rTJ01f \\ &= PrT0f \\ &= Pr0 = r. \end{aligned}$$

Suppose $\overline{x}$ is not in the state Q. Then $X_{Q} = 0$, and

$$\begin{aligned} f' &= PT0rTJ00f \\ &= P0T1f \\ &= P0f = f. \end{aligned}$$

<u>Theorem 2</u>: For any natural number k there exists a set of three abelian semigroups which is weakly complete over E(k).

<u>proof</u>: The result is trivially true for $k = 1$ and well-known for $k = 2$. Let k be a fixed integer such that $k \geq 3$. Let S denote the set of abelian semigroups defined over E(k) by (1) above. The functions $V_{j}x$ defined in (2) are defined in terms of the elements of S and the constants of E(k). This implies that for each state of the variables $x_{1}, \ldots, x_{n}$, there is a characteristic function, defined as in (3), which is defined in terms of the elements of S and the constants of E(k). Given any function f of the n variables $x_{1}, \ldots, x_{n}$ and a state Q such that in the state Q, f takes on a value different from r, then it is possible, by the definition given in (4), to define a function f', in terms of f

and the elements of S and the constants of E(k) which has the same value as f in every state except Q and which has the value r in the state Q.

Suppose that g is a function of n variables over E(k). Choose h an element of S. If g = h, then the theorem is proved. If g ≠ h, then there is some number of state, say j, of the k^n possible state, in which g and h differ. Apply the construction of (4) to obtain a new function, defined in terms of S and the constants of E(k) which differs from g in j-1 places. Repetition of the process j times produces a definition of g in terms of the elements of S and the constants of E(k).

Since the semigroup h is chosen arbitrarily, there is nothing unique about the definition obtained by this construction. Neither is there anything unique about the choice of the semigroups of S. For example, if the definition of J is modified, so that it takes on the values 0 and k-1 instead of the values 0 and 1, then T and P can be replaced by max and min.

The author is grateful to the referee for the reference to [3].

References.

1. Ivo Rosenberg, "La structure des fonctions de plusieurs variables sur un ensemble fini." C.R. Acad. Sc. Paris, t. 260 (5 April 1965), pp 3817-9.

2. Ivo Rosenberg, "Über die funktionale Vollständigkeit in den mehrwertigen Logiken", Rada Matematickych a Prirodnich Ved R. 80 - S. 4 (1970), pp. 1-90. (Contains the proof of 1 .)

3. H. Werner, "Finite simple non-abelian groups are functionally complete", announcement in Notices AMS 20, 6, *73T-A228.

Weak Completeness and Abelian Semigroups

by

T. C. Wesselkamper

Author's address: Department of Computer Science, Virginia
Polytechnic Institute and State University,
Blacksburg, Virginia 24061, U.S.A.

$$f_{i+1}x = V_{a_j}x.r + JOV_{a_j}x.f_i x.$$

If $x = a_j$, then $f_{i+1}x = V_{a_j}a_j.r + JOV_{a_j}a_j.f_i a_j$ (3)

$$= 1.r + J01.f_i a_j$$

$$= r + 0.f_i a_j = r.$$

If $x \neq a_j$, then $f_{i+1}\ x = V_{a_j}x.r + JOV_{a_j}x.f_i x$

$$= 0.r + J00.f_i x$$

$$= 1.f_i x = f_i x.$$

Whence if a_j, the j^{th} value in the value sequence, is different from r then the value sequence of f_{i+1} agrees with the value sequence of f_i at each position except the j^{th} position and in the j^{th} position the value sequence of f_{i+1} contains an r.

Define a set offunctions:

$$B^* = C \cup \{J, +, .\} \cup \{V_i\}_{i \in E(k)}. \quad (4)$$

Lemma 2: The set of functions B* generates the set of one place functions over E(k).

proof: Let $f = \langle a_0 a_1 \ldots a_{k-1} \rangle$ be a one place function over E(k).

The constant function $h_o = \langle 00\ldots.0 \rangle \in C$. If $f = h_o$, then the proof is complete. If $f \neq h_0$, then the value sequences for f and h_0 differ in at most p places ($1 \leq p \leq k-1$). Let $f_o = h_o$ and let q be the smallest index for which the value sequences differ. By the construction (3),

$$f_1\ x = V_{a_q}x.r + JOV_{a_q}x.f_o x,$$

defines a new function f_1 in terms of the constants 0 and a_q, the functions $\{J, +, .\}$, and the function $V_{a_q} \in \{V_j\}$. The function f_1 has a value sequence which differs from the value sequence of f in q-1 places. Repetition of this process q-1 more times produces a function $f_q = f$. (In practice, h_o might be a poor choice for f_o.)

We define the set:

$$B = C \cup \{J, +, .\} \tag{5}$$

For each $j \in E(k)$, let $j^* = k-j \pmod k$.

Lemma 3: The set B generates the set B*.

proof: We need to show only that the set $\{V_j\}_{j \in E(k)}$. is generated by B.

Let $V_j\, x = JO(x + j^*)$. (6)

From the group properties of $<E(k), +>$, $x = j$ is the unique solution of the equation $x + j^* = 0$.

Case 1: If $x = j$, $V_jx = JO(j + j^*) = JOO = 1$.

Case 2: If $x \neq j$, $V_jx = JO(x + j^*) = 0$.

Hence for each j, V_jx can be defined in terms of the constants 0 and j^*, and the functions J and +.

Corollary 1: The set of functions B generates the set of one place functions over E(k).

Lemma 4: The set of functions B generates all n place functions over E(k).

proof: The proof is by induction. Lemma 3 forms the basis for the induction. If the statement of the Lemma is true for some $n > 1$, and if f is some n+1 place function, then by Lemma 1 there exist k functions $\{g_i\}_{i \in E(k)}$, such that each g_i is an n place function and,

$$fx_1x_2\ldots x_nx_{n+1} = \sum_{i=0}^{k-1} V_ix_{n+1}\cdot g_ix_1\ldots x_n.$$

By the induction hypothesis the g_i are generated by B. By Lemma 3 the V_i are generated by B and {+, .} < B. Hence f is generated by B and the induction is complete.

Corollary 2: The set of functions B is complete.

Theorem: For each natural number k there exists a set of three abelian semigroups which is weakly complete over E(k).

proof: Since the set B is complete, the set {J, +, .} is weakly complete.

It should be noted that the set {J, +, .} is not unique. If the definition of J is modified so that the function produces the values 0 and k-1 instead of 0 and 1, then the construction can be carried out with addition and multiplication replaced by max and min.

The author is grateful to Dr. J.C. Muzio who suggested definition (6).

References

1. Alan Rose, Computer Logic, (London: John Wiley & Sons, Ltd., 1971), p. 70.

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

An Extension of a Theorem of Brawley and Carlitz

by

T. C. Wesselkamper

Author's address: Department of Computer Science, Virginia
Polytechnic Institute and State University,
Blacksburg, Virginia 24061

If R is a commutative ring with identity, then every function f: $R \to R$ is representable as a polynomial if and only if R is a finite field [2, p. 507]. This result has been generalized by Brawley and Carlitz [1] in a theorem which states:

Theorem. Let R be a ring with 1 and let $L[x]$ and $R[x]$ denote respectively the left and right polynomials over R, that is $L[x] = \{a_0 + xa_1 + \ldots + x^n a_n: \ a_i \in R\}$, $R[x] = \{a_0 + a_1 x + \ldots + a_n x^n: \ a_i \in R\}$. Let $P_L(R)$ and $P_R(R)$ denote those functions in R^R representable by left and right polynomials, respectively. Then $P_L(R) = R^R$ if and only if $P_R(R) = R^R$ if and only if R is a finite field.

The purpose of this note is to extend the Brawley-Carlitz theorem to polynomials in k indeterminates and functions of k variables for each natural number k.

Let $R^*(k) = \{f: \ f: \ R^k \to R\}$, the functions from R^k into R, for each natural number k. Let $P[x; k]$ be the polynomials in k indeterminates, $x_1, x_2, \ldots, x_k$, over R. Let $F_{P[x;\ k]}$ be the set of functions in $R^*(k)$ which are representable as polynomials in $P[x; k]$. It is well known that $R^*(1) = F_{P[x;\ 1]}$.

We employ a lemma which is an analog of the Shannon Decomposition Theorem [3].

Suppose R is a finite field and suppose that for each $j \in R$ there exists a function $V_j x$ such that:

$$V_jx = \begin{cases} 1, \text{ if } x = j; \\ 0, \text{ otherwise.} \end{cases} \tag{1}$$

Lemma. If f: $R^n \to R$, then there exist functions g_i: $R^{n-1} \to R$, $(i \in R)$, such that:

$$fx_1x_2\ldots x_n = \sum_{i \in R} V_ix_ng_ix_1x_2\ldots x_{n-1}.$$

proof: For each $i \in R$ let $g_ix_1x_2\ldots x_{n-1} = fx_1x_2\ldots x_{n-1}i$. Choose $j \in R$ and suppose that $x_n = j$. Then $V_jx_n = 1$ and for all $i \neq j$, $V_ix_n = 0$. Using this fact, we have:

$$\begin{aligned} \sum_{i \in R} V_ix_ng_ix_ix_2\ldots x_{n-1} &= V_jx_ng_jx_1x_2\ldots x_{n-1} \\ &= g_jx_1x_2\ldots x_{n-1} \\ &= fx_ix_2\ldots x_{n-1}j. \end{aligned} \tag{2}$$

Since j was chosen arbitrarily (2) holds whenever $x_n = j \in R$, and the proof is complete.

Theorem 1. If R is a finite field, then for each natural number k, $R^*(k) = F_{P[x;\ k]}$.

proof: The proof is by induction on k. The Brawley-Carlitz theorem is the case $k = 1$ and forms the basis for the induction. Since every function f: $R \to R$ has a polynomial representation, the functions V_jx defined in (1) have a polynomial representation. Now suppose that the statement of the theorem is true for some natural number k and suppose that f: $R^{k+1} \to R$. Then by the Lemma there exist functions g_i: R^n R such that:

$$fx_ix_2\ldots x_n = \sum_{i \in R} V_ix_{n+1}g_ix_1x_2\ldots x_n. \tag{3}$$

As already noted the $V_i x$ have a polynomial representation. By the induction hypothesis the $g_i x_1 x_2 \ldots x_n$ have a polynomial representation. Hence the expression (3) is a polynomial representation of $f x_1 x_2 \ldots x_{n+1}$.

The converse theorem is trivially true, for if for each natural number k a polynomial representation exists, then it exists in particular for $k = 1$, and the theorem reduces to the Brawley-Carlitz Theorem.

Interest in such theorems arises in a natural way if one considers the following situation: Suppose one has a digital computer with word length k. Then all of the operations in that computer are functions of some finite number of variables over a space of 2^k elements if the computer utilizes twos-complement arithmetic and functions over a space of 2^k-1 elements if the machine utilizes ones-complement arithmetic. The theorems of this note ensure that in the twos-complement case the computer can be competely described in terms of polynomials over the finite field of 2^k elements, whereas in the ones-complement case if ring operations are used in the description at least one other operation is necessary. The author has shown elsewhere [4] that one additional operation is sufficient. The Brawley-Carlitz Theorem is benign since it lays to rest the possibility that the situation could be improved in the ones-complement case by using non-commutative ring operations.

References

1. J. V. Brawley and L. Carlitz, "A Characterization of the n x n Matrices over a Finite Field", this Monthly 80, number 6 (June-July, 1973), pp. 670-2.

2. L. Redei, Algebra, Vol. 1, Pergamon Press, Oxford, 1967.

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

4. T. C. Wesselkamper, "Some Completeness Results for Abelian Semigroups and Groups", 1974 International Symposium on Multiple-valued Logics, (to appear).