UNDEFINABILITY OF ADDITION FROM ONE UNARY OPERATOR(1)

BY
ROBERT McNAUGHTON

It is the object of this paper to prove that the binary operator of addition of the natural numbers is not arithmetically definable in terms of a single unary operator. An *arithmetical* (or *elementary*) definition is one in which no variables ranging over sets of natural numbers are permitted; all variables range over just the natural numbers themselves.

It is actually easier to prove something more than this: that a single unary operator will not suffice even when any number of one-place predicates of natural numbers are added. The method of proof is by elimination of quantifiers, originally due to Presburger. A by-product of the method used is the subsidiary result that addition is not definable without quantifiers in terms of any set of unary operators, one-place predicates and two-place predicates.

The interpreted well-formed formulas herein considered have the following as symbols: $=$, identity, interpreted in the usual way; f, a unary functor, interpreted as a unary operator over the natural numbers; truth functions and quantifiers; and predicate letters, each interpreted as a definite property of natural numbers. a, b, c, d, x, y, z are variables. A term will be either a variable x or $f^i(x)$, i.e., $f(f(\cdots(x)\cdots))$, in which f occurs i times; thus $f^0(x)$ is simply the variable x. t and s, with and without subscripts and superscripts, will be arbitrary terms. The symbols $\top$ and $\bot$ are propositional constants standing, respectively, for truth and falsity. m, n, h, i, j, k are natural numbers.

The class of formulas that are allowed can be made precise by the following recursive characterization: (1) if $t_1, t_2, \cdots$ are terms and F is an n-ary predicate letter ($n \geqq 1$) then $t_1 = t_2$, $Ft_1 \cdots t_n$, $\top$ and $\bot$ are allowed formulas; (2) if Φ_1 and Φ_2 are formulas and x is a variable then $-(\Phi_1)$, $\Phi_1 \ \& \ \Phi_2$, $(\exists x)\Phi_1$ and $(x)\Phi_1$ are all formulas; and (3) nothing else is a formula.

THEOREM I. *Given the formula*

$$\begin{aligned}(\exists x)(f^p(x) = t \ \ \& \ \ & P(x) \& x \neq s_1^0 \& \cdots \& x \neq s_{n_0}^0 \\ & \& f(x) \neq s_1^1 \& \cdots \& f(x) \neq s_{n_1}^1 \\ & \quad \vdots \\ & \& f^{p-1}(x) \neq s_1^{p-1} \& \cdots \& f^{p-1}(x) \neq s_{n_{p-1}}^{p-1}),\end{aligned}$$

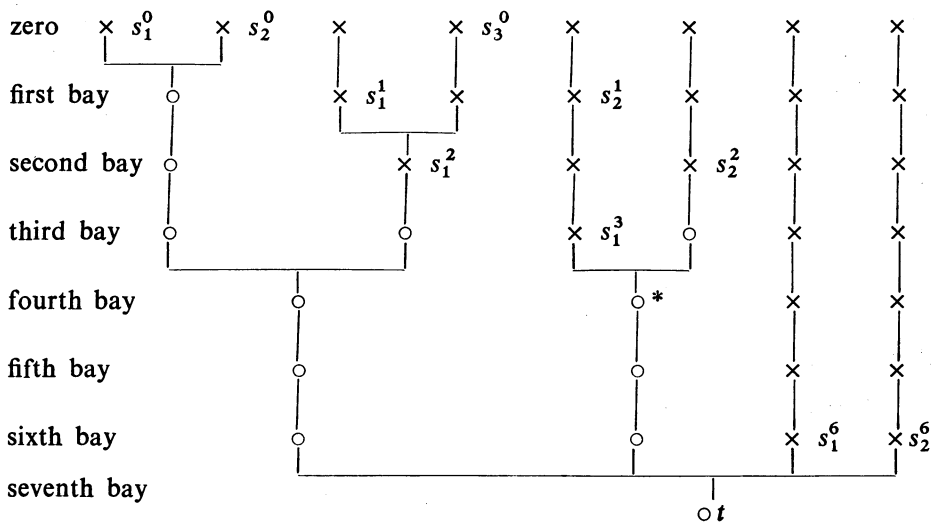
Received by the editors October 5, 1963.

(1) This paper appeared as Technical Report No. 3 of Contract DA-04-200-ORD-436 (Office of Ordnance Research) issued May 1, 1957, at the Applied Mathematics and Statistics Laboratory of Stanford University.

where t and the s's are terms not containing x, there is an equivalent formula without quantifiers but with the same free variables.

To begin the proof of this theorem, I shall describe a method which could be used to plot t and the s's on a tree assuming their numerical values were known. For $0 \leqq i \leqq p-1$, d is *eligible* for the ith bay of a tree if $f^{p-i}(d) = t$ and there exists a y such that $f^i(y) = d$ and $P(y)$. If s_j^i is not eligible for the ith bay, we do not plot it. If it is, we plot it as a cross in the ith bay. If $s_j^i = s_k^i$, then they are plotted at the same cross; otherwise, separately. If $i \neq h$, then it is not necessary to check for the equality or inequality of s_j^i and s_k^h in plotting them on the tree. Plot t as a circle as the only item in the pth (and last) bay. For each plotted s_j^i plot $f(s_j^i)$ as a circle in the $(i+1)$st bay, unless something identical to it has already been plotted. Similarly plot $f^2(s_j^i)$ in the $(i+2)$nd bay, etc. Connect by a straight line any two items e_1 and e_2 in the succeeding bay if $f(e_1) = e_2$. Change every circle to a cross if it is connected to a cross in the succeeding bay; continue this until no circle is connected by a line to a cross in a later bay. Complete the table by entering, for every cross not connected to any cross in an earlier bay, a *chain* of new crosses from that cross to the first bay. (Thus if there is a cross in bay 3 not connected to a cross in bay 2, enter one cross each in bay 1 and in bay 2 and connect these by lines.)

The tree will then look something like the following example in which $p = 7$:



Every item (of which there are finitely many) in the zero bay will be a cross and linked to t in the pth bay by a *chain*. In each chain crosses appear until the first circle following which all entries are circles. The last cross in any chain is one of the s's. All chains begin in the zero bay.

DEFINITION. A *root* of y is a z such that $f(z) = y$.

LEMMA 1. *The formula of Theorem* I *is true if and only if at least one circle in the tree has at least one more root eligible for the immediately preceding bay than there are in the tree.*

Proof. Suppose first that there is such a circle e in the ith bay. There must be an x such that $P(x), f^i(x) = e$ (and hence $f^p(x) = t$) and $f^{i-1}(x)$ is not plotted on the tree. It follows that $x, f(x), \cdots, f^{i-2}(x)$ are likewise not on the tree. To prove that, for each s_j^h, $f^h(x) \neq s_j^h$, there are three cases to consider.

Case I. $h < i$ and s_j^h is on the tree. Then since $f^h(x)$ is not on the tree, q.e.d.

Case II. $h \geqq i$ and s_j^h is on the tree. Then $f^h(x)$ must be a circle on the tree, since $e = f^i(x)$ is a circle. Since s_j^h is a cross, q.e.d.

Case III. s_j^h is not on the tree. Then, it is not eligible for the hth bay. Since $P(x)$ and $f^p(x) = t$, $f^h(x)$ is eligible; hence q.e.d.

Suppose now that the formula is true. Note that in any chain the last cross must be one of the s's. There must be an x such that $f^h(x) \neq s_j^h$, for all h and j, $P(x)$ and $f^p(x) = t$; hence, for each $i < p$, $f^i(x)$ is eligible for the ith bay. If g is the smallest number such that $f^g(x)$ is on the tree, then $f^g(x), f^{g+1}(x), \cdots, f^p(x) = t$, are in a chain on the tree. Each of these must be a circle; otherwise there would be a k such that $f^k(x)$ would be the last cross in the chain, and hence, for some j, $f^k(x) = s_j^k$, contradicting the specification of x. Thus $f^g(x)$ is a circle with a root $f^{g-1}(x)$ which is eligible for the $(g-1)$st bay but not on the tree.

LEMMA 2. *For every tree there is a formula without quantifiers which says that* t *and the* s*'s are such as to give rise to the tree.*

Let $F_i d$ mean that there exists a y such that $P(y)$ and $f^i(y) = d$. Note that F_i has a definite interpretation given f, i and P. The formula for Lemma 2 can be taken as a conjunction of all formulas described under (1) and (2) below.

(1) For each i and j a formula stating that s_j^i is eligible for the ith bay or not (i.e., either the formula

$$f^{p-i}(s_j^i) = t \ \& \ F_i(s_j^i)$$

or its negation),

(2) for each i, j, i', j' and k such that $j < n_i$, $j' < n_{i'}$, and $\max(i, i') \leqq k < p$ either the formula

$$f^{k-i}(s_j^i) = f^{k-i'}(s_{j'}^{i'})$$

or its negation.

LEMMA 3. *For any circle on a given tree, there is a formula without quantifiers which says that it has more roots eligible for the immediately preceding bay than there are in the tree.*

The proof is by example. The reader can verify that the considerations are valid in their generality. Consider the circled item marked with an asterisk in the diagram above. Let $G_4^2 z$ mean there are more than two roots of z of the form $f^3(y)$ for some y such that $P(y)$. Note that for an arbitrary z, $G_4^2 z$ does not assert that these roots are eligible for the fourth bay of the tree; it implies it only if $f^3(z) = t$. Note also that G_4^2 has a definite interpretation given f and P. The circled item with an asterisk is $f(s_1^3)$ $(= f^2(s_2^2) = f^3(s_2^1))$. Hence the condition that this circled item has more roots eligible for the preceding bay than shown on the tree can be expressed by the atomic formula $G_4^2 f(s_1^3)$.

The proof of Theorem I can now be completed. There are only finitely many, say m, trees possible; let $T_1(s_0^0, \cdots, s_{n_{p-1}}^{p-1}, t), \cdots, T_m(s_0^0, \cdots, s_{n_{p-1}}^{p-1}, t)$ be the formulas without quantifiers corresponding to these, which exist by Lemma 2. The formula without quantifiers which can replace that of Theorem I is a disjunction of m disjuncts; the ith disjunct is a conjunction of $T_i(s_0^0, \cdots, s_{n_{p-1}}^{p-1}, t)$ and a formula without quantifiers which is a disjunction of all the formulas each of which states that a circled item has more eligible roots than shown in the tree. These formulas exist by Lemma 3. That the formula so constructed is equivalent to the formula of the theorem is a consequence of Lemma 1.

THEOREM II. *To the formula like that of Theorem* I, *except that* $f^p(x) = t$ *is deleted, there is a formula equivalent to it without quantifiers but with the same free variables.*

The proof is similar to that of Theorem I except for a few changes. The tree will have only p bays since there is no entry for the pth bay. A number z is *eligible* for the jth bay if there is a number y such that $P(y)$ and $f^j(y) = z$. Lemma 1 is still true if we add the words, "or if there are more items eligible for the $(p-1)$st bay than appear on the tree." Lemmas 2 and 3 and their proofs still hold without change, but a fourth lemma must be added.

LEMMA 4. *Given any tree it is possible to state that there are more numbers eligible for the* $(p-1)$*st bay that there are in the tree by means of a formula without quantifiers.*

Proof. Consider the tree which was used as an example and diagrammed in the proof of above theorem and pretend there is no t or seventh bay. Let $H_5^6 z$ mean that z is one of at least five numbers w such that there is a y such that Py and $f^6(y) = w$. The interpretation of H_5^6 is definite given P and f. To say there are more than four numbers eligible for the sixth bay the formula $H_5^6 s_1^6$ (or $H_5^6 f^3(s_1^3)$ or etc.) will suffice.

The remainder of the proof is similar, in an obvious manner, to that part of the proof of Theorem I following Lemma 3.

THEOREM III. *A formula* $(\exists x)\Phi(x)$, *where* $\Phi(x)$ *is a conjunction of atomic formulas, or their negations, is equivalent to a formula without quantifiers and with the same free variables.*

Note that a term contains at most one variable; that an atomic formula contains at most two variables, and if it contains two variables, it must be an identity.

Case I. x appears with another variable in at least one conjunct which is an unnegated identity. Then let p be the smallest number $\geqq 0$ such that $f^p(x)$ is one of the principal terms of such an unnegated identity. Let $f^p(x) = t$ be one of these identities; t does not contain x. Divide the conjuncts of $\Phi(x)$ into three classes.

Class I. The conjunct $f^p(x) = t$, those conjuncts which contain x as the only variable, and those conjuncts containing, for some $j < p$, $f^j(x)$ in a negated identity. The clauses which contain x as the only variable can all be replaced by a single atomic formula Px, where P has that interpretation making Px equivalent to the conjunction of all the conjuncts containing x as the sole variable.

Class II. Other conjuncts containing x, which must contain x only in a term $f^j(x)$, where $j \geqq p$.

Class III. Conjuncts not containing x.

By Theorem I there is a formula ψ without quantifiers equivalent to the formula obtained from $(\exists x)\Phi(x)$ by deleting conjuncts of Classes II and III. The formula without quantifiers equivalent to $(\exists x)\Phi(x)$ is the conjunction of ψ together with the conjuncts of Class III together with the conjuncts of Class II with $f^{j-p}(t)$ substituted for each term of the form $f^j(x)$.

Case II. x does not appear with another variable in an unnegated identity but does appear in a negated identity. The proof of this case is similar to that of Case I except for using Theorem II instead of Theorem I.

Case III. x does not appear with any other variable in any conjunct. Then $(\exists x)\Phi(x)$ is logically equivalent to $((\exists x)\Phi'(x)) \cdot \chi$, where χ is the conjunction of all the conjuncts of $\Phi(x)$ which do not contain x, and $\Phi'(x)$ is the conjunction of those that do. $\Phi'(x)$ contains no variables other than x, so $(\exists x)\Phi'(x)$ is either true and can be replaced by $\top$, or false and can be replaced by $\bot$.

THEOREM IV. *Any formula is equivalent to one without quantifiers and with the same free variables.*

The proof is by Presburger's method. Replace universal quantifiers by existential quantifiers in the usual manner. Consider an innermost existential quantifier $(\exists x)$ and assume the truth function in its scope is in disjunctive normal form whose disjuncts are $\Phi_1(x), \Phi_2(x), \cdots$. $(\exists x)(\Phi_1(x) \vee \cdots)$ is logically equivalent to $(\exists x)\Phi_1(x) \vee (\exists x)\Phi_2(x) \vee \cdots$. By Theorem III each of these is replaceable by a formula without quantifiers and with the same free variables. In this manner all quantifiers can be eliminated, q.e.d.

It remains to prove that there is no formula without quantifiers containing just the variables a, b, and c which is true if and only if $a = b + c$. This fact will be proved as Theorem VIII (which it will be noted, is true even if any number of two-term relations and any number of additional unary operators are added). Formulas without quantifiers can be assumed to be in disjunctive normal form. A formula (with only a, b, c free) is *suitable* for addition if, for any m, n, p, it is true for $a = p$, $b = m$, $c = n$ only if $p = m + n$; it covers an order pair $\langle m, n\rangle$ of non-negative integers if the disjunct is true for $a = m$, $b = n$ and $c = m + n$. A *fundamental formula* is an atomic formula or its negation or a conjunction of such. A disjunctive normal formula is then a fundamental formula or a disjunction of fundamental formulas.

THEOREM V. *If a fundamental formula Φ suitable for addition covers $\langle m, n\rangle$ and $\langle m, n + h\rangle$, for $h > 0$, then it does not cover $\langle m + h, n\rangle$. (Nor does it cover $\langle m - h, n + h\rangle$.)*

Proof. Note that an atomic formula may not contain more than two variables. There are then three classes of conjuncts of Φ: C_a, those not containing a; C_c, those not containing c; and C_b, those not containing b. These are inclusive of all the conjuncts of Φ, but perhaps not exclusive. Suppose Φ covers $\langle m, n\rangle$, $\langle m, n + h\rangle$ and $\langle m + h, n\rangle$. Then the conjuncts of C_a are true for $b = m$ and $c = n$, by virtue of the coverage of $\langle m, n\rangle$; those of C_c are true for $a = m + n + h$ and $b = m$, by virtue of the coverage of $\langle m, n + h\rangle$; and those of C_b are true for $a = m + n + h$ and $c = n$, by virtue of the coverage of $\langle m + h, n\rangle$. Hence Φ is true for $b = m$, $c = n$ and $a = m + n + h$, and Φ is not suitable for addition, q.e.d.

Our main objective can be achieved if it can be shown that Theorem V implies that no finite number of fundamental formulas suitable for addition can cover all the ordered pairs of non-negative integers. To do this, we must digress. If A is a set of non-negative integers let $v_i(A), i > 0$, be the number of numbers of A less than i. The *density* of A is

$$\lim_{i \to \infty} \frac{v_i(A)}{i},$$

if this limit exists.

THEOREM VI. *If for every k the subset of those x's in A such that $x + k$ is also in A is of density 0, then A is of density 0.*

Proof. Let A_k be the set of all x's in A such that there is a y in A such that $0 < y - x \leqq k$. From the hypothesis of the theorem it follows by familiar reasoning that, for each k, A_k is of density 0. Thus, for every positive integer k and for every $\varepsilon > 0$, there is a j such that, for every $i > j$, $v_i(A_k)/i < \varepsilon$. For every x in the set

$A - A_k$, the k numbers immediately following x are not in A, and hence not in $A - A_k$; hence, for every $i > j$, $v_i(A - A_k)/i \leqq 1/(k+1)$. Thus for every $i > j$, since $v_i(A) = v_i(A_k) + v_i(A - A_k)$, $v_i(A)/i < \varepsilon + 1/(k+1)$. Since there is such a j for any positive integer k and any $\varepsilon > 0$, A is of density 0.

THEOREM VIII. *Let A be a sequence of non-negative integers that is not of density zero; then there is a positive integer k and a subset C of A not of density zero such that, for every x in C, $x + k$ is in A.*

Proof. By contraposition from Theorem VI. (Note: to say that a set is not of density zero is not to say that it has density greater than zero; for it may not have any density at all as when the limit of $v_i(A)/i$ does not exist.)

THEOREM VIII. *No finite number of fundamental formulas suitable for addition cover all the ordered pairs of natural numbers. (Hence, no formula without quantifiers expresses $a = b + c$.)*

Proof. Suppose contrary to the theorem that there are a finite number of, say m, such fundamental formulas. Then there would be m sets of ordered pairs $B_1, \cdots, B_m$ such that $B_1 \cup B_2 \cup \cdots \cup B_m$ is the set of all ordered pairs of natural numbers and such that, for each i, if $\langle m, n\rangle$ is in B_i and $\langle m, n+h\rangle$ is in B_i, then $\langle m+h, n\rangle$ is not in B_i. For any $j \geqq 0$ and for any set X of ordered pairs of natural numbers, let X^j be the set of all x's such that $\langle j, x\rangle \in X$.

Not all the B_i's are such that the density of B_i^0 is zero. Otherwise, the B's could not together cover all the pairs $\langle 0, x\rangle$. Let us suppose that B_1^0 is not of density zero. Then by Theorem VII, there exists a positive k_1 and a subset D_1 of B_1^0 such that D_1 is not of density zero and for every x in D_1, $x + k_1$ is in B_1^0. Let E_2 be the set of all pairs $\langle k_1, x\rangle$ for x in D_1. By Theorem V, $E_2 \cap B_1$ is empty, since both $\langle 0, x\rangle$ and $\langle 0, x + k_1\rangle$ are in B_1 when $\langle k_1, x\rangle$ is in E_2. $E_2^{k_1}$ is not of density zero, since D_1 is not of density 0. Now if, for each i, $B_i^{k_1} \cap E_2^{k_1}$ were of density zero, then $(B_1^{k_1} \cup \cdots \cup B_m^{k_1}) \cap E_2^{k_1}$ would be of density zero and some members of E_2 could not be covered since $E_2^{k_1}$ is not of density zero. Therefore, for some B_i, say B_2, $B_2^{k_1} \cap E_2^{k_1} = F_2$ is not of density zero. But then again by Theorem VII there is a positive integer k_2 and a subset D_2 of F_2 such that D_2 is not of density zero and, for every x in D_2, $x + k_2$ is in F_2 (and hence $\langle k_1, x + k_2\rangle$ is in E_2). Let E_3 be the set of all pairs $\langle k_1 + k_2, x\rangle$ for x in D_2. Similar to reasoning in the case of $B_1 \cap E_2$, $B_2 \cap E_3$ is empty. But now $B_1 \cap E_3$ is also empty: for if $\langle k_1 + k_2, x\rangle$ is in E_3, then x is in F_2 and hence $\langle k_1, x\rangle$ is in E_2 and, by construction of E_2, $\langle 0, x\rangle$ is in B_1; also $\langle k_1, x + k_2\rangle$ is in E_2 and $\langle 0, x + k_1 + k_2\rangle$ is in B_1. Again there must be a B_i, say B_3, such that $B_3^{k_1+k_2} \cap E_3^{k_1+k_2}$ is not of density 0. In like manner $E_4, E_5, \cdots, E_{m+1}$ can be constructed in such a way that, for each j and for each $i < j$, $B_i \cap E_j$ is empty. E_{m+1} will not be empty but, for each $i \leqq m$, $B_i \cap E_{m+1}$ will be, contradicting the assumption that $B_1 \cap \cdots \cap B_m$ is the set of all ordered pairs of natural numbers.

MAIN THEOREM. *Addition is not arithmetically definable in terms of any single unary operator even with the aid of an arbitrary set of one-placed predicates.*

This now follows from Theorems IV and VIII. An interesting though subsidiary result can be proved following the method given in Theorems V, VI, VII and VIII. If we note that the proof that addition is not definable without quantification turns solely on the feature of the language of this paper that an atomic formula may have at most two variables (cf. the proof of Theorem V), the following by-product of the present investigation is apparent.

SUBSIDIARY THEOREM. *Addition is not definable without quantifiers in terms of any number of one-place predicates, two-place predicates and unary operators.*

The above methods serve to show that both results are true for many binary operators other than addition, such as multiplication and raising to a power. I have been unable to obtain a necessary and sufficient condition on a binary operator ϕ that the results of this paper hold for it. A sufficient condition is that there exist arithmetic functions g_1, g_2 and g_3, g_1 being bi-unique (i.e., $g_1(m) = g_1(n)$ implies $m = n$) such that, for all m and n, $\phi(g_2(m), g_3(n)) = g_1(m + n)$. (As a consequence g_2 and g_3 are also bi-unique.) By reasoning in a manner similar to that in the proof of Theorem V, it follows that if a fundamental formula suitable for $a = \phi(b, c)$ covers $\langle g_2(m), g_3(n)\rangle$ and $\langle g_2(m), g_3(n + h)\rangle$, for $h > 0$, then it does not cover $\langle g_2(m + h), g_3(n)\rangle$. (Analogous definitions for "suitable for $a = \phi(b, c)$" and "cover" are assumed.) With this result, the proof of the main theorem and with it the subsidiary theorem for ϕ is apparent. Thus for the formula $a = bc$, take $g_1(m) = g_2(m) = g_3(m) = 2^m$; for the formula $a = b^c$ take $g_1(m) = g_2(m) = 2^{2^m}$ and take $g_3(m) = 2^m$. An open question is whether $a = 2^b \cdot 3^b$ is definable in terms of a single unary operator. Taking $f_2(x)$ and $f_3(x)$ as, respectively, the exponents of 2 and 3 in the prime factorization of x (or 0 if $x = 0$) and $F(x)$ meaning that $x \neq 0$ and x has no prime factor except 2 or 3, we get the following equivalent to $a = 2^b \cdot 3^c$, showing that the subsidiary theorem is false for it:

$$F(a) \;\&\; f_2(a) = b \;\&\; f_3(a) = c.$$

It is an easy matter to find three unary operators in terms of which addition may be defined. Let $f(w)$ be the sum of the exponent of 2 and the exponent of 3 in the prime factorization of w. Let $g(w)$ be the exponent of 2, and $h(w)$ the exponent of 3. Then $z = x + y$ is equivalent to

$$(\exists w)(f(w) = z \;\&\; g(w) = x \;\&\; h(w) = y).$$

In a recent paper [2], Hartig gives two unary operators in terms of which both addition and multiplication, and hence all of the notions of Peano arithmetic,

can be defined. This result, together with the one reported in this paper, establishes that two is the minimum, whether one wants to define just addition or all of Peano arithmetic.

References

1. M. Presburger, *Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt*, Comptes-Rendus du Ier, Congrès des Mathématiciens des Pays Slaves (Warsaw, 1929), pp. 92–101, 395, Skład Głowny, Warsaw, 1930.

2. K. Hartig, *Einstellige Funktionen als Grundbegriffe der elementaren Zahlentheorie*, Z. Math. Logic Grundlagen Math. **5** (1959), 209–215.

Moore School of Electrical Engineering,
University of Pennsylvania,
Philadelphia, Pennsylvania