NON-LINEAR RECURSIVE SEQUENCES

ELBERT A. WALKER

The purpose of this paper is to investigate non-linear recursive sequences of maximum length with elements from $GF(2)$. In particular, the question of whether or not a recursive sequence of maximum length can be equal to its dual is settled. This question, as far as the author knows, was originally asked by Rosser. Part I contains the necessary background for Part II, and in the main is a condensation of some unpublished work (1955) of W. A. Blankinship and R. P. Dilworth.

PART I

1. Let $GF(2)$ be the field with two elements, let n be a positive integer, let $\mathfrak{S}$ be the Cartesian product of n copies of $GF(2)$, and let f be a mapping from $\mathfrak{S}$ into $GF(2)$. A sequence $a_1, a_2, a_3, \ldots$ of elements in $GF(2)$ is said to be *recursively generated* by f if

$$a_{n+i} = f(a_i, a_{i+1}, \ldots, a_{n+i-1}) \qquad \text{for i} = 1, 2, 3, \ldots$$

f is called a *recursion* or a *rule of generation*. The sequence $a_1, a_2, a_3, \ldots$ is called a *recursive sequence* of span $\leqslant n$. It is of span n if in addition it is not of span $\leqslant n - 1$. The elements of $\mathfrak{S}$ will be called *patterns*, or *n-bit words*, and the elements of $GF(2)$ will sometimes be called *bits*, and denoted by 0, 1. The mapping f induces a mapping F of $\mathfrak{S}$ into $\mathfrak{S}$ in the following way. If $S = (a_1, a_2, \ldots, a_n)$ is in $\mathfrak{S}$, let $F(S) = (a_2, a_3, \ldots, a_n, f(a_1, \ldots, a_n))$. Hence with the mapping f of $\mathfrak{S}$ into $GF(2)$, we associate the mapping F of $\mathfrak{S}$ into $\mathfrak{S}$, and F uniquely determines f. Distinct mappings f_1 and f_2 of $\mathfrak{S}$ into $GF(2)$ induce distinct mappings F_1 and F_2 of $\mathfrak{S}$ into $\mathfrak{S}$. If F is one-to-one, then f is said to be a *non-singular* recursion. Otherwise f is called *singular*. All recursions considered here will be assumed to be non-singular unless otherwise stated.

2. Let f be a recursion, let F be the mapping of $\mathfrak{S}$ into $\mathfrak{S}$ determined by f and let S_1 be in $\mathfrak{S}$. Let $S_i = F(S_{i-1})$, $i = 2, 3, 4, \ldots$. Since $\mathfrak{S}$ is finite, there exists a smallest positive integer m such that $S_{m+1} = S_1$. Thus f generates a cycle of elements in $\mathfrak{S}$, namely $(S_1, S_2, \ldots, S_m)$. If T_1 is some element in $\mathfrak{S}$ not in the cycle $(S_1, S_2, \ldots S_m)$, f generates another cycle $(T_1, T_2, \ldots T_{m'})$ and these two cycles are disjoint. Continuing in this manner, $\mathfrak{S}$ is decomposed into disjoint cycles by f. Of course the cycle $(S_1, S_2, \ldots, S_m)$ is con-

Received October 17, 1958.

https://doi.org/10.4153/CJM-1959-037-x Published online by Cambridge University Press

sidered the same as $(S_2, S_3, \ldots, S_m, S_1)$. This collection of cycles determined by f is denoted by C, and it is easy to see that f is uniquely determined by C. The system C of cycles is called the cyclic structure of f. Since F is one-to-one, it is onto, and so is a permutation of $\mathfrak{S}$. If this permutation is decomposed into the product of disjoint cycles, this collection of cycles is identical with C. Thus the cyclic structure of the permutation F is identical with the cyclic structure of f. The sum of the lengths of the cycles in C is 2^n, where n is the span of f. If C consists of just one cycle, that cycle is said to be a *maximal* cycle.

3. Any mapping f of $\mathfrak{S}$ into $GF(2)$, singular or non-singular, can be represented uniquely as a polynomial in $x_1, x_2, \ldots, x_n$ with coefficients in $GF(2)$. If f is linear in x_1,

$$f(a_1, a_2, \ldots, a_n) = f(a_1 + 1, a_2, \ldots, a_n) + 1.$$

Hence f linear in x_1 implies f is non-singular. Assume f is non-singular. Then $f(1, 0, 0, 0, \ldots, 0) = 1 + f(0, 0, \ldots, 0)$ so that the term x_1 appears in the polynomial representing f. $f(1, 1, 1, \ldots, 1) = 1 + f(0, 1, 1, \ldots, 1)$ so that if the polynomial representing f has any non-linear terms with x_1 as a factor, it has an even number of them. If it has at least two, let

$$x_1 x_{i_1} \ldots x_{i_r} \qquad \text{and} \qquad x_1 x_{j_1} x_{j_2} \ldots x_{j_s}$$

be distinct and let the first have smallest possible degree. The sets $\{i_1, i_2, \ldots, i_r\}$ and $\{j_1, j_2, \ldots, j_s\}$ are distinct. There is a j_k not in $\{i_1, i_2, \ldots, i_r\}$. Let $S = (a_1, a_2, \ldots, a_n)$ be the element of $\mathfrak{S}$ whose first co-ordinate is 1, whose $i_1, i_2, \ldots, i_r$ co-ordinates are 1, and the rest of whose co-orinates are 0. Let $S' = (a_1 + 1, a_2, a_3, \ldots, a_n)$. Then $F(S) = F(S')$, and F is singular. Hence f is linear in x_1. Thus f is non-singluar if, and only if, f is dependent on x_1 and linear in x_1, and $f(x_1, x_2, \ldots, x_n) = x_1 + f_1(x_2, x_3, \ldots, x_n)$, where f_1 is a polynomial in $x_2, x_3, \ldots, x_n$.

4. Let $S = (a_1, a_2, \ldots, a_n)$ be a pattern in $\mathfrak{S}$, and let $\bar{S} = (a_1 + 1, a_2, \ldots, a_n)$. Let f_S be the mapping from $\mathfrak{S}$ into $GF(2)$ that is 1 only at S and $\bar{S}$. Explicitly,

$$f_S(x_1, \ldots, x_n) = \prod_{i=2}^{n} (1 + a_i + x_i).$$

Note that $f_S = f_{\bar{S}}$. Let C be the system of cycles of f. Suppose S and $\bar{S}$ are on distinct cycles in C. Let $(S_1, S_2, \ldots, S_k)$ be the cycle containing S, and let $(T_1, T_2, \ldots, T_m)$ be the cycle containing $\bar{S}$. For convenience, let $S_1 = S$ and $T_1 = \bar{S}$. Then the system C' of cycles of $f + f_S$ consists of the cycle $(S_1, T_2, T_3, \ldots, T_m, T_1, S_2, S_3, \ldots, S_k)$ and the remaining cycles of C unchanged. Suppose S and $\bar{S}$ are on the same cycle $(S_1, S_2, \ldots, S_k)$ in C. Let $S_1 = S$ and $S_r = \bar{S}$. Then the system C' of cycles of $f + f_S$ consists of the cycles $(S_1, S_{r+1}, \ldots, S_k)$, $(S_r, S_2, \ldots, S_{r-1})$, and the remaining cycles of C unchanged.

https://doi.org/10.4153/CJM-1959-037-x Published online by Cambridge University Press

5. Let f be a recursion that generates a cycle $C_1 = (S_1, S_2, \ldots, S_k)$. Suppose this cycle C_1 has the property that if it contains the pattern $(a_1, a_2, \ldots, a_n)$ then it contains $(a_1 + 1, a_2, a_3, \ldots, a_n)$. Let $(b_1, b_2, \ldots, b_n)$ be any pattern. C_1 contains a pattern ending in b_1, $(a_1, a_2, \ldots, a_{n-1}, b_1)$. If this pattern is not followed in C_1 by $(a_2, a_3, \ldots, a_{n-1}, b_1, b_2)$, then the pattern $(a_1 + 1, a_2, \ldots, a_{n-1}, b_1)$, which is in C_1, is followed by $(a_2, a_3, \ldots, a_{n-1}, b_1, b_2)$. Continuing in this manner, one gets the pattern $(b_1, b_2, \ldots, b_n)$ in C_1. Hence the system of cycles of f consists simply of the one cycle C_1. If a recursion f generates more than one cycle, then every cycle it generates has the property that it contains a pattern S such that it does not contain $\bar{S}$. Therefore $f + f_S$ generates one less cycle than does f. In general, if f generates k cycles, then there exist $k - 1$ patterns $S_1, \ldots, S_{k-1}$ such that

$$f + \sum_{i=1}^{k-1} f_{S_i}$$

generates just one cycle.

Part II

An unsolved problem concerning non-linear recursive sequences is that of finding a large class of recursions which generate maximal cycles. It is known **(1)** that the number of such recursions of span n is

$$2^{2^{n-1}-n}.$$

We begin this section by deriving some elementary properties a recursion must have if it generates a maximal cycle. Later we define and investigate the reverse, the dual ,and the reverse-dual of a recursion.

1. Let f be a recursion of span n that generates a maximal cycle. Then

$$f(x_1, x_2, \ldots, x_n) = 1 + x_1 + \phi(x_2, x_3, \ldots, x_n),$$

where $\phi\ (x_2, x_3, \ldots, x_n)$ is a polynomial with no constant term.

Proof. Since f generates a maximal cycle, every n-bit word must occur in that cycle. Thus the n-bit word $(0, 0, \ldots, 0)$ is not a rut, that is $f(0, 0, \ldots, 0) = 1$.

2. Let f be a recursion of span $n > 1$ that generates a maximal cycle. Then the polynomial $f(x_1, \ldots, x_n)$ that represents f does not contain all the linear terms $x_2, \ldots, x_n$.

Proof. The n-bit word $(0, 0, \ldots, 0)$ is followed by a 1. If $f(x_1, \ldots, x_n)$ has the term x_n, then the $n + 1$-bit word $(0, 0, \ldots, 0, 1)$ is followed by 0, and if it also has the term x_{n-1}, this pattern is followed by 0, etc. If $f(x_1, \ldots, x_n)$ has all the linear terms $x_2, \ldots, x_n$, we get the sequence $0, 0, \ldots, 0, 1, 0, 0, \ldots, 0$ since $f(x_1, \ldots, x_n)$ contains the linear term x_1. But if $n > 1$, this

https://doi.org/10.4153/CJM-1959-037-x Published online by Cambridge University Press

implies that f does not generate a maximal cycle. Therefore $f(x_1, \ldots, x_n)$ does not contain all those terms.

3. Let f be a recursion of span n that generates a maximal cycle. Then the polynomial that represents f has an even number of terms.

Proof. The n-bit word $(1\ ,1, \ldots, 1)$ is followed by a 0. Hence $f(1, 1, \ldots, 1) = 0$ and so $f(x_1, \ldots, x_n)$ has an even number of terms.

4. Definitions. One cycle is the *reverse* of another if either cycle can be obtained from the other by taking the bits in reserve order. One cycle is the *dual* of another if either can be found from the other by replacing all 0's by 1's and all 1's by 0's. One cycle is the *reverse-dual* of another if it is the reverse of the dual (the same as the dual of the reverse) of the other. The recursion corresponding to the reverses of the cycles generated by f is called the *reverse* of f, and is denoted by Rf. The recursion corresponding to the duals of the cycles generated by f is called the *dual* of f, and is denoted by Df. The recursion corresponding to the reverse-dual of the cycles of f is called the *reverse-dual* of f, and is denoted by RDf.

5. It is fairly clear that the cyclic structure of f, Rf, Df, and RDf are the same as far as the number of cycles in each and the lengths of cycles in each are concerned. In particular, if f generates a maximal cycle, then so do Df, Rf, and RDf.

6. Since every recursion f can be represented by a polynomial, it is of some interest to determine the polynomials representing Rf, Df, and RDf in terms of the one representing f. A moment's reflection shows that if

$$f(x_1, x_2, \ldots, x_n) = x_1 + f_1(x_2, \ldots, x_n)$$

then

$$Rf(x_1, \ldots, x_n) = x_1 + f_1(x_n, \ldots, x_2),$$

and

$$Df(x_1, \ldots, x_n) = x_1 + f_1(1 + x_2, 1 + x_3, \ldots, 1 + x_n).$$

From these follow then that

$$RDf(x_1, \ldots, x_n) = x_1 + f_1(x_n + 1, \ldots, x_2 + 1).$$

7. Since $f(x_1, \ldots, x_n) = x_1 + f_1(x_2, \ldots, x_n)$ implies that

$$Rf(x_1, \ldots, x_n) = x_1 + f_1(x_n, \ldots, x_2),$$

we see that f and Rf agree on those patterns which are symmetric in the last $(n - 1)$ bits.

8. Suppose a cycle $(S_0, S_1, \ldots, S_{k-1})$ is the same as its reverse. Suppose

https://doi.org/10.4153/CJM-1959-037-x Published online by Cambridge University Press

this cycle contains a pattern which is its own reverse, and for convenience let it be S_0. Let S_i' be the reverse of the pattern S_i. Then $S_0 = S_0'$, $S_1 = S_{k-1}'$, $\ldots, S_j = S_{k-j}', \ldots$. There is at most one j such that $j = k - j$, namely $j = \frac{1}{2}k$. Therefore, if a cycle is the same as its reverse, then it contains at most two patterns which are their own reverses. If k is odd, there is at most one such pattern, and as a matter of fact, exactly one such pattern. It is possible for a cycle of even length to be its own reverse and contain no pattern which is its own reverse. For example, the cycle ((01), (10)) is such a cycle. Now, using these facts we can prove the following theorem.

THEOREM. *If $f = Rf$, then f generates at least $2^{[\frac{1}{2}n+\frac{1}{2}]-1}$ cycles. If $n \geqslant 3$, then f does not generate a maximal cycle.*

Proof. There are $2^{[\frac{1}{2}n+\frac{1}{2}]}$ n-bit words which are their own reverses. Since $f = Rf$, a cycle which contains one of these n-bit words is its own reverse. But a cycle that is its own reverse can contain at most two n-bit words that are their own reverses. Hence there must be at least $2^{[\frac{1}{2}n+\frac{1}{2}]-1}$ cycles generated by f. If $n \geqslant 3$, $2^{[\frac{1}{2}n+\frac{1}{2}]-1} \geqslant 2$, so that f does not generate a maximal cycle.

9. We are now going to settle the question as to whether or not a cycle of maximal length can be equal to its dual. It has just been shown that if $n \geqslant 3$, a maximal cycle of span n is not equal to its reverse. The corresponding statement is true for the dual of a maximal cycle, but the proof of it is a little more complicated. We begin with a lemma, of which no proof seems readily available in the literature.

LEMMA. *If $f(x_1, \ldots, x_n) = x_1$, then the number of cycles generated by f is even, for $n > 2$.*

Proof. If $a_1a_2 \ldots a_n$ is any pattern, then the sequence obtained beginning with this pattern is $a_1a_2 \ldots a_na_1a_2 \ldots a_n \ldots$. Therefore to compute the number of cycles generated by f is the same problem as computing the number of strings of beads of length n that can be constructed using two kinds of beads, where two strings are considered the same if one is a rotation of the other. It is easily verified that this number is

$$G(n) = \sum_{d\mid n} \frac{F(d)}{d},$$

where $F(1) = 2$ and

$$F(k) = 2^k - \sum_{\substack{r\mid k\\ r<k}} F(r).$$

$F(d)$ is, in fact, the number of patterns that are equal to themselves at slides of multiples of d only. Hence such a pattern and its slides contain exactly d distinct patterns, from which it follows that $d^{-1}F(d)$ is the number of strings of beads n long of this nature. Summing over all divisors d of n yields the

https://doi.org/10.4153/CJM-1959-037-x Published online by Cambridge University Press

total number of strings of beads. This number $G(n)$ we wish to show is even. Observing that

$$\sum_{d|n} F(d) = 2^n$$

and applying the Möbius inversion formula yields

$$F(n) = \sum_{d|n} \mu(n/d)2^d.$$

Therefore we get

$$G(n) = \sum_{d|n} \frac{F(d)}{d} = \sum_{d|n} \sum_{r|d} \frac{\mu(d/r)2^r}{d}.$$

If n is odd we see immediately that $F(d)$ and hence $d^{-1}F(d)$ is even for all $d|n$. Thus we need consider only the case where

$$d = 2^a p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$$

where $a > 0$, and $p_1, p_2, \ldots, p_s$ are distinct odd primes.* Now

$$F(d) = \sum_{r|d} \mu(r)2^{d/r}$$

and each non-vanishing term in the sum has a factor

$$2^{2^{a-1}p_1^{a_1-1}p_2^{a_2-1}\ldots p_s^{a_s-1}}.$$

Hence

$$F(d) = m2^{2^{a-1}p_1^{a_1-1}\ldots p_s^{a_s-1}}$$

where m is an integer. Since $d|F(d)$,

$$p_1^{a_1}p_2^{a_2}\ldots p_s^{a_s}|m.$$

Put

$$m = up_1^{a_1}p_2^{a_2}\ldots p_s^{a_s},$$

where u is an integer. Then

$$\frac{F(d)}{d} = u2^{\{2^{a-1}p_1^{a_1-1}p_2^{a_2-1}\ldots p_s^{a_s-1}-a\}}.$$

A necessary condition that $d^{-1}F(d)$ be odd is $a_1 = a_2 = \ldots = a_s = 1$ and $a = 1$ or 2; that is, if $d = 2p_1p_2\ldots p_s$ or $d = 4p_1p_2\ldots p_s$. We show in each of these cases that $d^{-1}F(d)$ is odd. Let $d = 2p_1p_2\ldots p_s$. Then

$$F(d) = 2^d \pm 2^{d_1} \pm 2^{d_2} \pm \ldots \pm 2$$

where $d, d_1, d_2, \ldots,$ are all the divisors of d. Hence $F(d)$ is twice an odd number and since $d|F(d)$, $d^{-1}F(d)$ is odd. If $d = 4p_1p_2\ldots p_s$ then since

$$F(d) = \sum_{r|d} \mu(r)2^{d/r}$$

*The author wishes to thank the referee for furnishing a correct proof for this case.

https://doi.org/10.4153/CJM-1959-037-x Published online by Cambridge University Press

and $\mu(r) = 0$ if 4 divides r,

$$F(d) = 2^d \pm 2^{d_1} \pm 2^{d_2} \pm \ldots \pm 2^2$$

where $d, d_1, d_2, \ldots, 2$, are all the *even* divisors of d. Hence $F(d)$ is four times an odd number and since $d|F(d)$, $d^{-1}F(d)$ is odd. Now let

$$n = 2^a p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}.$$

Since $n > 2$, either $s > 0$,or $a > 1$. If $s = 0$, $n = 2^a$, a > 1 and

$$G(n) = \sum_{d|n} \frac{F(d)}{d} = \frac{F(1)}{1} + \frac{F(2)}{2} + \frac{F(4)}{4} + \sum_{r=3}^{a} \frac{F(2^r)}{2^r}$$
$$= 2 + 1 + 3 + \sum \text{ (even numbers)}.$$

Hence $G(n)$ is even. If $s > 0$, $a = 0$, then each term of

$$\sum_{d|n} \frac{F(d)}{d}$$

is even. If $s > 0$, $a = 1$, then the divisors d, for which $d^{-1}F(d)$ is odd, are the numbers $d = 2q_1q_2 \ldots q_r$, where $q_1, q_2, \ldots, q_r$ is a subset of $p_1, p_2, \ldots, p_s$. The number of such divisors is 2^s so that $G(n)$ is even. Finally, if $s > 0, a > 1$, the divisors d, for which $d^{-1}F(d)$ is odd, are of the forms $d = 2q_1q_2 \ldots q_r$ or $d = 4q_1q_2 \ldots q_r$ where $q_1, q_2, \ldots, q_r$ is a subset of $p_1, p_2, \ldots, p_s$. The number of such divisors is 2^{s+1}. Hence, again G(n) is even.

10. Let f and g be recursions of span n. If f and g disagree on the n-bit word S, then from 4, Part I, we see that $f + f_S$ and g agree on S and $\bar{S}$ and on all patterns on which f and g agree. Thus the recursion f may be changed into the recursion g by adding a suitable set of f_S's to f. From 5, Part I, we see that adding h_S to any recursion h changes the parity of the number of cycles generated by h. If $S = (a_1, a_2, \ldots, a_n)$ then

$$h_S(x_1, \ldots, x_n) = \prod_{i=2}^{n} (1 + a_i + x_i),$$

and adding h_S to h adds the term $x_2x_3 \ldots x_n$, among other terms, to the polynomial representing h. If one adds an odd number of h_S's to h one adds the term $x_2x_3 \ldots x_n$, among other terms, to the polynomial representing h. Now let f be the recursion such that $f(x_1, \ldots, x_n) = x_1$ and let g be any recursion of the same span that generates an odd number of cycles. If $n > 2$, f generates an even number of cycles, so to change f into g requires the adding of an odd number of f_S's to f, and hence the adding of the term $x_2x_3 \ldots x_n$, among other terms to the polynomial representing f, which is x_1. Hence the polynomial representing g has the term $x_2x_3 \ldots x_n$. Conversely, if g is any recursion of span n such that the polynomial representing it has the term $x_2x_3 \ldots x_n$, then one must add an odd number of f_S's to f to get g, and this implies that g generates an odd number of cycles. These remarks we sum up in the following theorem.

https://doi.org/10.4153/CJM-1959-037-x Published online by Cambridge University Press

THEOREM. *A recursion of span $n > 2$ generates an odd number of cycles if, and only if, the polynomial representing it has the term $x_2x_3 \ldots x_n$.*

COROLLARY. *If a recursion of span $n > 2$ generates a maximal cycle, then the polynomial representing it has the term $x_2x_3 \ldots x_n$.*

11. We are now in a position to prove that if $n > 2$ and f generates a maximal cycle, then $f \neq Df$. In fact, we will prove a more general result.

THEOREM. *If $n > 2$ and a recursion f generates an odd number of cycles, then $f \neq Df$.*

Proof. From 6, Part II, it is easy to see that if the polynomial representing f contains a term

$$x_{i_1}x_{i_2} \ldots x_{i_r},$$

then this term is a term of the polynomial representing Df if, and only if,

$$x_{i_1}x_{i_2} \ldots x_{i_r}$$

is a factor of an odd number of terms of the polynomial representing f. Since f generates an odd number of cycles, the polynomial representing it contains the term $x_2x_3 \ldots x_n$. If that polynomial contains a term besides 1, x_1, and $x_2x_3 \ldots x_n$, then it contains a term which is a factor of only itself and $x_2x_3 \ldots x_n$. That term then is a factor of an even number of terms, and therefore is not a term of the polynomial representing Df. If

$$f(x_1, \ldots, x_n) = 1 + x_1 + x_2x_3 \ldots x_n \text{ or } x_1 + x_2x_3 \ldots x_n$$

then

$$Df(x_1, \ldots, x_n) = 1 + x_1 + (1 + x_2)(1 + x_3) \ldots (1 + x_n)$$
$$\text{or } x_1 + (1 + x_2)(1 + x_3) \ldots (1 + x_n),$$

and is obviously not the same as $f(x_1, \ldots, x_n)$. Hence in any case, $f \neq Df$.

COROLLARY. *If $n > 2$ and f is a recursion generating a maximal cycle, then $f \neq Df$.*

12. THEOREM. *If n is even and if f is a recursion of span $n > 2$ which generates an odd number of cycles, then $Rf \neq Df$, and hence $f \neq RDf$.*

Proof. From 6, Part II, it follows that the polynomials representing the recursions f and Rf have the same structure with regard to the number of terms which are the product of a given number of variables. There are $n - 1$ possible terms which are the product of $n - 2$ variables, namely $x_3x_4 \ldots x_n$, $x_2x_4 \ldots x_n, \ldots, x_2x_3 \ldots x_{n-1}$. Since the polynomial representing f contains the term $x_2x_3 \ldots x_n$, we see from the proof of the theorem in 11, Part II, that the polynomial representing Df contains precisely those terms which are the product of $n - 2$ variables that the polynomial representing f does

https://doi.org/10.4153/CJM-1959-037-x Published online by Cambridge University Press

not contain. Thus for Rf to be equal to Df it is necessary that $n - 1$ be even. If n is even then $n - 1$ is odd so that $Rf \neq Df$ and $f \neq RDf$.

COROLLARY. *If $n > 2$ is even and f generates a maximal cycle then $Rf \neq Df$ and $RDf \neq f$.*

For n odd it can happen that $Rf = Df$. It happens in the case $n = 5$, as shown by the polynomial

$$f(x_1, x_2, x_3, x_4, x_5) = 1 + x_1 + x_4 + x_5 + x_4x_5 + x_2x_3x_5 + x_2x_3x_4 + x_2x_3x_4x_5.$$

REFERENCE

1. N. de Bruijn, *A combinatorial problem*, Koninklijke Nederlandse Akademie van Wetenschappen, Proceedings, *49* (Part 2) (1946), 758–64.

New Mexico State University

https://doi.org/10.4153/CJM-1959-037-x Published online by Cambridge University Press