<table>
<thead>
<tr>
<th>Name or Title</th>
<th>Initials</th>
<th>Circulate</th>
<th>Coordination</th>
<th>File</th>
<th>Information</th>
<th>Necessary Action</th>
<th>Note and Return</th>
<th>See Me</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>N. Friedman</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Remarks**

**From Name or Title**

**Organization and Location**

Approved for Release by NSA on 10-30-2013 pursuant to E.O. 13526
A METHOD FOR GENERATING IRREDUCIBLE POLYNOMIALS

A. Gleason
R. W. Marsh
NSA-314
26 May 1955

It was observed that, if the polynomial \( f(x) = \sum_{i=0}^{P} a_i x^i \) (coefficients in GF(2)) is irreducible and its root has maximum period \( 2^P - 1 \), then the polynomial \( F(x) = \sum_{i=0}^{P-1} 2^i x^{2^i-1} \) is irreducible and its root has maximum period. This was verified in all cases up to \( P = 5 \).

We shall give a proof that \( F \) is always irreducible but leave unsettled the question of whether its roots are primitive.

Let \( K \) be a finite field of cardinal \( q \) (which must be a prime power and, in the case of particular interest, is 2). Let \( K^* \) be a minimal algebraically closed field containing \( K \). For each positive integer \( n \) there is in \( K^* \) a unique field \( K^n \) of degree \( n \) over \( K \); \( K^* = \bigcup K^n \). We may regard \( K^* \) as an infinite dimensional vector space over \( K \); then each of the fields \( K^n \) is a vector subspace.

Let \( \alpha \) be the mapping \( x \mapsto x^q \) of \( K^* \) into itself.

Lemma 1. \( \theta \in K^n \iff \alpha^n \theta = \theta \)

Proof: The field \( K^n \) has \( q^n \) elements, and the \( q^n - 1 \) non-zero elements from a group under multiplication. By the theorem of Lagrange every element of this group satisfies the relation \( \theta^{q^n-1} = 1 \), whence every element of \( K^n \) satisfies \( \theta^{q^n} = \theta \). This proves one half of the lemma.

The polynomial \( x^{q^n} - x \) can have at most \( q^n \) roots in \( K^* \). Hence all of the roots are in \( K^n \). This proves the second half of the lemma.
The mapping \( \alpha \) is an automorphism of \( K^* \) since it evidently satisfies
\[
\alpha (\theta \varphi ) = \alpha (\theta ) \alpha (\varphi ) \quad \text{and} \quad \alpha (\theta + \varphi ) = \alpha (\theta ) + \alpha (\varphi )
\]
because \( q \) is a power of the characteristic. We have seen that \( \alpha \theta = \theta \) if \( \theta \in K = K' \). Hence \( \alpha \) is a linear transformation of \( K^* \) regarded as a vector space over \( K \).

Lemma 2. If \( \theta \in K^* \), the degree of \( \theta \) is the least positive integer \( n \) for which \( \alpha^n \theta = \theta \).

Proof: Obvious from lemma 1.

Theorem: Let \( f = \sum_{i=0}^{p} b_1 x^i \) be an irreducible polynomial of degree \( p \) over \( K \) whose roots are primitive in \( K^p \). Then \( F = \sum_{i=0}^{p} b_1 x^{q^i - 1} \) is an irreducible polynomial of degree \( q^p - 1 \).

Proof: Consider any root \( \theta \) of \( F \). Evidently \( \theta \neq 0 \). We have then
\[
0 = \theta F(\theta) = \sum_{i=0}^{p} b_1 \theta^{q^i} = \left( \sum_{i=0}^{p} b_1 \alpha^i \right) \theta = f(\alpha) \theta.
\]

The set of all polynomials \( P \) such that \( P(\alpha) \theta = 0 \) is an ideal \( \mathfrak{c} \) in the polynomial ring over \( K \). Since this ring is a principal ideal ring and \( \mathfrak{c} \) contains the irreducible polynomial \( f \), \( \mathfrak{c} \) is either the unit ideal or the principal ideal \( (f) \). The former possibility implies \( \theta = 0 \) which is false, so \( \mathfrak{c} = (f) \). By lemma 2, the degree of \( \theta \) is the least integer \( n \) for which \( (\alpha^n - 1)\theta = 0 \), that is, the least integer \( n \) for which \( x^n - 1 \in (f) \). Since the roots of \( f \) are primitive this integer is \( 2^p - 1 \).

The minimal polynomial for \( \theta \) is therefore an irreducible polynomial of degree \( 2^p - 1 \) which divides \( F \). Comparing degrees we see that the
quotient is in $K$, hence $F$ is irreducible. q.e.d.

It may be remarked that in case $f$ does not have primitive roots we can see that $F$ splits into irreducible factors of degree equal to the order of the roots of $f$.

Concerning the second question as to whether $F$ has primitive roots in the case $K = GF(2)$, it may be remarked that if true we could then obtain an algebraic recursion giving only irreducible polynomials by iterating the procedure. Since this is closely related to a prime generating function, it is rather unlikely to be provable by elementary methods, if true. Starting with $q = 3$, $K = GF(3)$, and the irreducible polynomial $x^2 - x - 1$ which has primitive roots we obtain the irreducible polynomial $x^3 - x^2 - 1$, whose roots have order 160, a far cry from being primitive. This also indicates that any proof would have to rely on number theoretic properties of the number 2.