Here using $\beta = \frac{1}{2} - \alpha + o(1)$, we get with some computation that for
$0 < \alpha < \frac{1}{2} + o(1)$

$$G = \mathcal{G}(n, \beta) = \mathcal{G}(n) \geq \mathcal{G}(0) = \frac{1}{Y^x} \frac{1}{2} - o(1),$$

which proves Lemma 2.

Thus we have from formulae (2.2), (2.15), (2.11), (2.12) and (2.16):

$$2 \sum_{d < \varepsilon} \delta(d) \leq \frac{1}{\varepsilon} \sum_{n < \varepsilon} g(n) + O(1) \leq \frac{1}{\varepsilon} \sum_{n < \varepsilon} g'(n) + O(1)$$

$$\leq \log \varepsilon \left(1 - \frac{1}{\log x} + o(1)\right) \leq \log \varepsilon \left(1 \left(1 - \frac{1}{Y^x}\right) + o(1)\right).$$

1. **Introduction.** Let $GF(q)$ denote the finite field of order $q = p^a$ where $p$ is prime and $a \geq 1$. Let $\Gamma(p)$ denote the algebraic closure of $GF(p)$. A polynomial $Q \in GF[q; x_1, \ldots, x_n]$ is absolutely irreducible if $Q$ has no nontrivial factors over $\Gamma(p)$. Throughout this paper, the term irreducible will mean absolutely irreducible.

A polynomial with coefficients in $GF(q)$ of the form

$$L(x) = \sum_{c=0}^r c x^{q^c}$$

is called a linear polynomial. The requirement that the coefficients be in $GF(q)$ ensures that the operation of mapping composition for linear polynomials is commutative. Corresponding to the linear polynomial $L(x)$ we have the ordinary polynomial

$$l(x) = \sum_{c=0}^r c x^{q^c}.$$

We shall assume in the following that $c_0 \neq 0$; this avoids multiple factors in $L(x)$ and insures that there is a smallest integer $r$ such that $l(x)$ divides $x^r - 1$. We say that $l(x)$ has exponent $r$.

Let $Q(a_1, \ldots, a_n) = a_1 x_1 + \ldots + a_n x_n + 1$ where $[\deg a_1, \ldots, \deg a_n] = s$ if $a \in GF(q^s)$ but $a \notin GF(q^t)$, $1 < t < s$, we say that the degree of a relative to $GF(q)$ is $s$ and write $\deg a = s$. We shall assume that $\{a_1, \ldots, a_n\}$ are linearly independent over $GF(q)$; otherwise $Q(a_1, \ldots, a_n)$ can be reduced at once to a polynomial in $m$ variables by suitable first degree transformations, where $m$ is the number of elements in a maximal linearly independent subset of $a_1, \ldots, a_n$.

In this paper we describe the factorization of $Q(L(x_1), \ldots, L(x_n))$. (We note that it is possible to have $Q(L(x_1), \ldots, L(x_n))$ reduce to a polynomial in fewer than $k$ variables even though $\{a_1, \ldots, a_n\}$ are linearly
independent over $GF(q)$; see Example 5.1.) If $s \mid r$, we shall show that
$Q(L(s_1, \ldots, L(s_n))$ is absolutely irreducible. If $s \mid r$, the character of the
factorization depends on $L(x)$. For $L(x) = x^s - x$, we obtain factors of degree
one, for $L(x) = x^s - x^s - 1 + \cdots + x$ we obtain absolutely irreducible
factors of degree $q^s - 1$, and for arbitrary $L(x)$ we obtain absolutely irreducible
factors of degree $q^s - 1$, where $u$ is determined by $L(x)$. For the precise state-ment of this result, see Theorem 5.1. For convenience in Sections 3 and 4, we shall describe the factorization for $Q(x, y) = ax + by + 1$ and then indicate how the results may be extended to
more than two variables.

The results for the homogeneous case

$$Q(a_1, \ldots, a_n) = a_1x_1 + \cdots + a_nx_n$$

are similar.

The factorizations considered in this paper are motivated by the multiple variable factorizations for $L(x) = x^s - x$ obtained by Long in [2] and [3] and the single variable results for arbitrary $L(x)$ obtained by Long and Vaughan in [4] and [5]. It is interesting to note that the case
$s \mid r$ behaves like a result of Ehrenfeucht and Felczakowski [1]: The polynomial
$f(x) + g(y) + h(z)$ is absolutely irreducible over the complex number field
for any polynomials $f, g$ and $h$. However in the case of finite fields, $f(x) + g(y) + h(z)$ may indeed factor when $s \mid r$.

2. Preliminaries

Lemma 2.1. Let $x = (x_1, x_2, \ldots, x_n)$, that is let $x$ denote a vector with
components $x_1, \ldots, x_2$. Let $f(x) \in GF(q)[x]$. For any integer $j \geq 1$, $y^j + f(x)$ is absolutely irreducible if and only if $f(x)$ is not a $p^{th}$ power in any extension
field of $GF(q)$.

Remark. If $j = 0$, $y + f(x)$ is obviously an absolutely irreducible
first degree polynomial.

Proof. To show necessity, let $f(x) = [a(x)]^p$ in $GF(q, x)$. Then for $j \geq 1$, we have

$$y^j + f(x) = [y^j - 1 + a(x)]^p.$$  

The proof of sufficiency will be by induction on $j$. Let $j = 1$. If $f(x)$ is not a $p^{th}$ power, then any factorization of $y^p + f(x)$ in some extension
field of $GF(q)$ would be of the form

$$y^p + f(x) = y(y, x)\psi(y, x)$$

where $\phi$ is an absolute irreducible and $\psi$ is either irreducible or a product of
irreducibles. If the factorization is nontrivial, $\psi$ actually appears in $\phi$ and $\psi$. We consider separately the two cases $(\phi, \psi) = 1$ and $(\phi, \psi) \neq 1$.

Case I. $(\phi, \psi) = 1$. On differentiating (2.1) with respect to $y$ we have

$$\phi\psi_y + \psi\phi_y = 0.$$  

Now (2.2) implies that $\phi\psi_y = 0$. Since $(\phi, \psi) = 1$ we have $\phi\psi_y = 0$, which is impossible unless $\phi_y = 0$. Similarly $\psi_y = 0$. But $\phi_y = 0$ implies $\psi = \psi_1(y^p, x)$
with $y^p$ actually appearing. Similarly $\psi_y = 0$ implies $\psi = \psi_1(y^p, x)$ with $y^p$ actually appearing. Consequently the product $\phi\psi$ contains a term with $y^p$ and this clearly contradicts the choice of $\phi$ and $\psi$ in (2.1).

Case II. $(\phi, \psi) \neq 1$. We may assume the factorization in the form

$$y^p + f(x) = \phi(y^p, x)$$

where $\phi$ is absolutely irreducible over $GF(q)$ and $k$ is an integer $\geq 1$. (If $y^p + f(x) = \phi(y, x)\psi(y, x)$ with $(\phi, \psi) = 1$, we may apply the argument of Case I.)

If $k = 0 \pmod{p}$, then $y^p + f(x)$ is a $p^{th}$ power and this contradicts the hypotheses on $f(x)$ since this would imply $f(x)$ is a $p^{th}$ power. Thus $k \neq 0 \pmod{p}$. On differentiating (2.3) we have

$$k\phi^{k-1}\psi_y = 0.$$  

Since $k \neq 0 \pmod{p}$, and $\phi^{k-1} \neq 0$, we have $\psi_y = 0$. Hence $\psi(y, x) = \psi_1(y^p, x)$ and

$$y^p + f(x) = \phi_1(y^p, x)$$

where $y^p$ actually appears in $\phi_1$. In order that the degree of $y$ in both members of (2.5) be $p$, we must have $k = 1$. Thus $y^p + f(x)$ is absolutely irreducible over $GF(q)$.

Assume that the lemma is true for $j = r - 1$.

Case I. $(\phi, \psi) = 1$. For $j = r$, we have as before

$$y^{p^r} + f(x) = \phi_1(y^p, x)\psi_1(y^p, x).$$

Let $z = y^p$ so that (2.6) becomes

$$z^{p^n} + f(x) = \phi_1(z, x)\psi_1(z, x).$$

By the induction hypothesis, $z^{p^n} + f(x) = y^{p^n} + f(x)$ is absolutely irreducible over $GF(q)$.

Case II. $(\phi, \psi) \neq 1$. For $j = r$ we have

$$y^{p^n} + f(x) = \phi_1(y^p, x).$$

Again set $z = y^p$ and (2.8) becomes

$$z^{p^n} + f(x) = \phi_1(z, x)$$

which is absolutely irreducible by the induction hypothesis.
Lemma 2.2. Let \( \beta \) belong to \( \Gamma(p) \). Then \( x^\beta + x + \beta \) is never a \( p \)-th power.

Proof. The derivative of \( x^\beta + x + \beta \) with respect to \( x \) is 1; the derivative of a \( p \)-th power is 0. Hence \( x^\beta + x + \beta \) is not a \( p \)-th power.

Lemma 2.3. Let \( f(x) = a_0 + a_1 x + \ldots + a_n x^n \) be a polynomial of degree \( q^i \) with coefficients in GF(\( q \)). If \( f(x+c) = f(x) \) for all \( c \) such that \( G(c) = 0 \) then \( f(x) = \varphi(G(\omega)) \) where \( \varphi \) is a polynomial over GF(\( q^i \)).

Proof. Using the division algorithm we may write

\[
 f(x) = \sum_{i=0}^{n} A_i(x) G^i(x) \quad (\text{deg} A_i(x) < q^i).
\]

Since \( f(x+c) = f(x) \), (2.10) becomes

\[
 f(x) = \sum_{i=0}^{n} A_i(x+c) G^i(x+c).
\]

Since \( G(x+c) = G(x) + G(c) = G(x) \) it follows that

\[
 f(x) = \sum_{i=0}^{n} A_i(x) G^i(x). 
\]

Since the coefficients in (2.10) are uniquely determined we have

\[
 A_i(x+c) = A_i(x) 
\]

for all \( c \) such that \( G(c) = 0 \). Since \( \text{deg} A_i(x) < q^i \) and \( \text{deg} G(x) = q^i \), we immediately conclude that \( A_i(x) \) is a constant.

Lemma 2.4. Let \( f(x_1, \ldots, x_k) \) be a polynomial with coefficients in GF(\( q^i \)), and let \( G(x) \) be a linear polynomial of degree \( q^i \) with coefficients in GF(\( q \)). If \( f(x_1+c_1, \ldots, x_k+c_k) = f(x_1, \ldots, x_k) \) for all \( c_i \) such that \( G(c_i) = 0 \), \( i = 1, \ldots, k \), then

\[
 f(x_1, \ldots, x_k) = \varphi(G(x_1), \ldots, G(x_k))
\]

where \( \varphi \) is a polynomial over GF(\( q^i \)).

Proof. Use Lemma 2.3 and induction on \( k \).

Lemma 2.5. Let

\[
 f(x_1, \ldots, x_k) = \prod_{c_1, \ldots, c_k} \varphi(x_1+c_1, \ldots, x_k+c_k)
\]

where the product is over all \( c_i \), \( 1 \leq i \leq k \), such that \( G(c_i) = 0 \), \( \psi \) is a polynomial over GF(\( q^i \)), and \( G(x) \) is a linear polynomial over GF(\( q \)). Then

\[
 f(x_1, \ldots, x_k) = \varphi(G(x_1), \ldots, G(x_k))
\]

where \( \varphi \) is a polynomial over GF(\( q^i \)).

Proof. This is an immediate corollary of Lemma 2.4.

Lemma 2.6. Let \( x^\beta - 1 = l(x)m(x) \). Let \( L(x) \), \( M(x) \) be the linear polynomials corresponding to \( l(x) \), \( m(x) \) respectively. If \( Q(L(x), L(y)) = F(x, y)G(x, y) \), then

\[
 Q(x^\beta - x, y^\beta - y) = F(M(x), M(y))G(M(x), M(y)).
\]

Proof. Since \( x^\beta - x = L(M(x)) \), we have

\[
 Q(x^\beta - x, y^\beta - y) = Q[L(M(x)), L(M(y))] = F(M(x), M(y))G(M(x), M(y)).
\]

Note that Lemma 2.6 can be immediately generalized to more than two variables. The lemma is of course also true for one variable.

Lemma 2.7. Let \( G(x) \) be an arbitrary linear polynomial in GF[\( q; x \)]. Let

\[
 P(x_1, \ldots, x_k) = \prod_{c_1, \ldots, c_k} [a_1(x_1+c_1) + \ldots + a_k(x_k+c_k)+a_0]
\]

where \( a_0, \ldots, a_k \) are coefficients from GF(\( q^i \)) and the product is over all \( c_i \), \( 1 \leq i \leq k \), such that \( G(c_i) = 0 \). For a given \( k \)-tuple \( (c_1, \ldots, c_k) \) of roots of \( G(x) \), define the class \( C(c_1, \ldots, c_k) \) as follows:

\[
 C(c_1, \ldots, c_k) = \{(d_1, \ldots, d_k) \mid G(d_i) = 0, 1 \leq i \leq k, \text{ and } a_1(d_1+c_1) + \ldots + a_k(d_k+c_k)+a_0 = a_1(c_1+c_1) + \ldots + a_k(c_k+c_k)+a_0\}
\]

These classes partition the \( k \)-tuples of roots of \( G(x) \) and each class has the same cardinality.

Proof. If \( C(c_1, \ldots, c_k) \) and \( C(c_1', \ldots, c_k') \) have a \( k \)-tuple in common, it follows that

\[
 a_1(x_1+c_1) + \ldots + a_k(x_k+c_k)+a_0 = a_1(x_1+c_1) + \ldots + a_k(x_k+c_k)+a_0.
\]

Thus \( (c_1', \ldots, c_k') \in C(c_1, \ldots, c_k) \) and conversely. Hence

\[
 C(c_1, \ldots, c_k) = C(c_1', \ldots, c_k').
\]

Let \( C_k = C[0, \ldots, 0] \). Then \( C(c_1, \ldots, c_k) \in C_k \) if and only if \( a_1(c_1) + \ldots + a_k(c_k)+a_0 = 0 \). Let \( C = C[d_1, \ldots, d_k] \) denote an arbitrary class. For each \( (c_1, \ldots, c_k) \in C_k \), we have

\[
 a_1(d_1+c_1) + \ldots + a_k(d_k+c_k)+a_0 = a_1(d_1) + \ldots + a_k(d_k).
\]

Thus \( (d_1+c_1, \ldots, d_k+c_k) \in C \). Hence \( |C| \geq |C_k| \). On the other hand if \( (d_1', \ldots, d_k') \in C \), we have \( (d_1'-d_1, \ldots, d_k'-d_k) \in C_k \). Thus \( |C| \leq |C_k| \). Hence \( |C| = |C_k| \). We conclude that \( |C| = |C_k| \).

Lemma 2.8. Let \( G(x) \) be a linear polynomial over GF(\( q \)) having degree \( q^i \). Let \( h(x_1, \ldots, x_k) = a_1x_1 + \ldots + a_kx_k \in GF[q^i; x_1, \ldots, x_k] \). Then the set of
The factorisation of $Q(L(x_1), \ldots, L(x_k))$

We now show that if $s \mid r$ and if $a$ and $b$ are linearly independent over $GF(q)$, then $Q(x^s - a, y^s - y)$ is absolutely irreducible of degree $q^*$. Since $s \mid r$, at least one of $\{\deg a, \deg b\}$ does not divide $r$. Consequently we may write

$$a = ax^s + f(a), \quad b = by^s + g(b)$$

with at least one of $\{f(a), g(b)\}$ non-zero. Thus

$$a(x^s - a) + b(y^s - y) + 1 = (ax + by)^s - (ax + by) + 1 + f(a)x^s + g(b)y^s$$

$$= W^s - W + 1 + X^s + Y^s$$

where $W = ax + by$, $X = f(a)x^s - a$, and $Y = g(b)y^s - y$.

Let $T = X + Y$. Then (3.3) has the form

$$T^s + (W^s - W + 1).$$

By Lemma 2.2, $W^s - W + 1$ is not a $p$th power. Hence (3.4), and therefore (3.3), is absolutely irreducible by Lemma 2.1. We have proved:

**Theorem 3.3.** Let $Q(x, y) = ax + by + 1$ where $\deg a, \deg b = s$ relative to $GF(q)$ and $a$ and $b$ are linearly independent over $GF(q)$. If $s \mid r$, then $Q(x^s - a, y^s - y)$ is absolutely irreducible.

The proof for the homogeneous case is the same except that, with the same notation as before, we use Lemmas 2.1 and 2.2 to show that $T^s + (W^s - W)$ is absolutely irreducible.

We have:

**Theorem 3.4.** Let $Q(x, y) = ax + by$ where $\deg b = s$ relative to $GF(q)$ and $a$ and $b$ are linearly independent over $GF(q)$. If $s \mid r$, then $Q(x^s - a, y^s - y)$ is absolutely irreducible.

We note that minor modifications in the proofs permit Theorems 3.1–3.4 to be extended to more than two variables.

**Example 3.1.** This example illustrates Theorem 3.1. Let $Q(x, y) = ax + ay + 1$ where $a^2 = a + 1$ generates $GF(4)$. Let $L(x) = x^s - a$. Then $s = 2$ and $r = 2$, so that $s \mid r$. Let $W = ax + ay$. Then

$$Q(x^s - a, y^s - y) = W^s + W + 1 = \prod_{i=0}^{s-1} (W - \beta^i)$$

where $\beta^2 = \beta + 1$ generates $GF(16)$.

**Example 3.2.** This example illustrates Theorem 3.3. Let $Q(x, y) = ax + ay + 1$ where $a^2 = a + 1$ generates $GF(4)$. Let $L(x) = x^s - a$. Then $s = 2$ and $r = 3$, so that $s \mid r$. Thus

$$Q(x^s - a, y^s - y) = ax^s + ax^s y^s - ax - a^2y + 1$$

is absolutely irreducible.
4. The factorization of \(a(L(x)) + b(L(y)) + 1\) where \(L(x) = x^{q^r-1} + x^{q^r-2} + \ldots + a\). This substitution is of special interest since \(L(x)\) is the trace function of \(GF(q^r)\) over \(GF(q)\). We note that the exponent of the corresponding ordinary polynomial \(l(x)\) is either \(r\) or \(r-1\). The value \(r-1\) occurs only when \(p = 2\) and \(r = 2\); in this case \(L(x) = x^2 - a\) and the factorization is described in Section 3. Consequently, we shall exclude the case \(p = r = 2\), so that the exponent of \(l(x)\) is \(r\) throughout this section.

**Theorem 4.1.** Let \(Q(x, y) = ax + by + 1\) where \([\deg a, \deg b] = s\) relative to \(GF(q)\) and \(a\) and \(b\) are linearly independent relative to \(GF(q)\). Let

\[
L(x) = x^{q^r-1} + x^{q^r-2} + \ldots + a.
\]

Let the corresponding ordinary polynomial \(l(x) = x^{r-1} + x^{r-2} + \ldots + 1\) have exponent \(r\). If \(s \nmid r\), then \(Q(L(x), L(y))\) is absolutely irreducible.

**Proof.** Suppose that \(Q(L(x), L(y)) = F(x, y)G(x, y)\). Then by Lemma 2.6,

\[
Q(x^q - x, y^q - y) = F(x^q - x, y^q - y)G(x^q - x, y^q - y).
\]

This factorization is in contradiction to Theorem 3.3 since \(s \nmid r\).

**Remark.** The condition of linear independence over \(GF(q)\) for \(a\) and \(b\) rules out the possibility of using a change of variable to transform \(Q(L(x), L(y))\) to a polynomial in one variable when \(L(x)\) is the trace function of \(GF(q^r)\) over \(GF(q)\).

The proof of Theorem 4.1 also applies to the case where \(Q(x, y)\) is homogeneous. We have:

**Theorem 4.2.** Let \(Q(x, y) = ax + by\) where \(\deg b = s\) relative to \(GF(q)\). Let \(L(x) = x^{q^r-1} + x^{q^r-2} + \ldots + a\). Let the corresponding ordinary polynomial \(l(x) = x^{r-1} + x^{r-2} + \ldots + 1\) have exponent \(r\). If \(s \nmid r\), then \(Q(L(x), L(y))\) is absolutely irreducible.

**Theorem 4.3.** Let \(Q(x, y), L(x), l(x), s\) and \(r\) be given as in Theorem 4.1. If \(s \mid r\), then \(Q(L(x), L(y))\) is the product of \(q^2\) absolute irreducibles of degree \(q\) in \(x\) and \(y\).

**Proof.** Let \(X = x^q - x\) and \(Y = y^q - y\). Then, as in (3.1),

\[
Q(X, Y) = Q(x^q - x, y^q - y) = \prod_{\lambda} (\alpha x + \beta y + \lambda)
\]

where the product extends over all \(\lambda\) satisfying \(x^2 - \lambda + 1 = 0\).

Consider a fixed factor \(\alpha x + \beta y + \lambda\) of (4.1). Let \(c\) and \(d\) independently satisfy the equation \(x^2 - x = 0\), that is \(c\) and \(d\) belong to \(GF(q)\). Since \(a\) and \(b\) are linearly independent, the factors

\[
a(x + c) + b(y + d) + \lambda = (c, d \in GF(q))
\]

are all distinct. Furthermore they are all factors of \(Q(X, Y)\). We now form the product of the factors (4.2) and obtain the polynomial \(P(x, y)\) of degree \(q^2\) in \(x\) and \(y\):

\[
P(x, y) = \prod_{\lambda, \mu, \nu \in \lambda}(\alpha x + \beta y + \eta).
\]

By Lemma 2.5

\[
P(x, y) = P_1(x^q - x, y^q - y) = P_1(X, Y),
\]

and \(P_1(X, Y)\) is a polynomial of degree \(q\) in \(X\) and \(Y\).

We now show that \(P_1(X, Y)\) is absolutely irreducible. If not, there exists a nontrivial absolutely irreducible factor of \(P_1(X, Y)\), call it \(R(X, Y)\). Replacing \(X\) by \(x^q - x\) and \(Y\) by \(y^q - y\), it is clear that \(R(x^q - x, y^q - y)\) divides \(P_1(x^q - x, y^q - y)\); this implies that \(R\) is a product of some of the first degree factors (4.2). If we suppose that one first degree factor divides \(R\), then it follows that all \(q^2\) factors in (4.2) divide \(R\). Hence \(R(X, Y)\) is identical with \(P_1(X, Y)\).

Thus the factors of (4.1) are grouped into \(q^2\) products of the form \(P(x, y)\) in (4.3). Each \(P(x, y)\) has degree \(q^2\) in \(x\) and \(y\) and can be written as an absolute irreducible of degree \(q\) in \(X\) and \(Y\).

The same proof applies in the case where \(Q(x, y)\) is homogeneous.

We have:

**Theorem 4.4.** Let \(Q(x, y), L(x), l(x), s\) and \(r\) be given as in Theorem 4.2. If \(s \mid r\), then \(Q(L(x), L(y))\) is the product of \(q^2\) absolute irreducibles of degree \(q\) in \(x\) and \(y\).

Theorems 4.1 and 4.2 can be extended without modification to more than two variables. Theorems 4.3 and 4.4 require a slight change. We state only the theorem corresponding to Theorem 4.3; the homogeneous case is essentially the same.

**Theorem 4.5.** Let \(Q(x_1, \ldots, x_k) = \alpha_1 x_1 + \ldots + \alpha_k x_k + 1\) where \([\deg \alpha_1, \ldots, \deg \alpha_k] = s\) relative to \(GF(q)\) and \(\{x_1, \ldots, x_k\}\) are linearly independent relative to \(GF(q)\). Let

\[
L(x) = x^{q^r-1} + x^{q^r-2} + \ldots + a.
\]

Let \(l(x) = x^{r-1} + x^{r-2} + \ldots + 1\) have exponent \(r\). If \(s \mid r\), then \(Q(L(x_1), \ldots, L(x_k))\) is the product of \(q^2\) absolute irreducibles of degree \(q^2\) in \(x_1, \ldots, x_k\).

**Proof.** We first note that the condition of linear independence on \(\{x_1, \ldots, x_k\}\) insures that \(s \geq k\) and hence \(r \geq k\). For we consider \(GF(q^2)\) as a vector space of dimension \(s\) over \(GF(q)\). A maximal linearly independent set of elements in \(GF(q^2)\) has cardinality \(s\).

The proof is the same as that for Theorem 4.3 except that (4.1) becomes

\[
Q(X_1, \ldots, L(X_k)) = \prod_{\lambda, \mu, \nu \in \lambda}(\alpha_1 x_1 + \ldots + \alpha_k x_k + \lambda).
\]
where the product is over all \( \lambda \) such that \( \lambda^{2} - \lambda + 1 = 0 \). Thus (4.3) becomes

\[
P(a_{1}, \ldots, a_{k}) = \prod_{a_{1}, \ldots, a_{k} \in \text{GF}(q)} \left[ a_{1}(a_{2} + b_{2}) + \cdots + a_{k}(a_{k} + b_{k}) + \lambda \right]
\]

\[
= P_{1}(X_{1}, \ldots, X_{k})
\]

where \( X_{i} = a_{i} - \alpha_{i} \) for \( 1 \leq i \leq k \). As before, it can be shown that \( P_{1}(X_{1}, \ldots, X_{k}) \) is absolutely irreducible of degree \( q - 1 \) in its variables, and the factors of (4.4) are partitioned to form \( q - k \) such absolute irreducibles.

In the preceding theorems we have assumed that the coefficients of the variables are linearly independent relative to \( \text{GF}(q) \). We now describe what occurs if this is not the case. We illustrate with the generalization of Theorem 4.5 when \( 0 \neq r \) and we also describe the case when \( 0 = r \).

**Theorem 4.6.** Let \( Q(x_{1}, \ldots, x_{k}) = a_{1}x_{1} + \cdots + a_{k}x_{k} + 1 \) and, by renumbering if necessary, let \( \{a_{1}, \ldots, a_{m} \} \) be a maximal linearly independent subset of \( \{a_{1}, \ldots, a_{k} \} \) relative to \( \text{GF}(q) \). Let \( L(x) \) and \( l(x) \) be given as in Theorem 4.5. If \( 0 \neq r \), then \( Q(L(x_{1}), \ldots, L(x_{k})) \) is the product of \( q - m - 1 \) absolute irreducibles of degree \( q - m - 1 \) in \( x_{1}, \ldots, x_{k} \).

**Proof.** By writing the coefficients \( a_{m+1}, \ldots, a_{k} \) as linear combinations of \( \{a_{1}, \ldots, a_{m} \} \) over \( \text{GF}(q) \), we may first use field transformations of the variables \( x_{1}, \ldots, x_{k} \) to rewrite \( Q \) in the form \( Q(y_{1}, \ldots, y_{m}) = a_{1}y_{1} + \cdots + a_{m}y_{m} + 1 \). The result follows from Theorem 4.5 since \( \{a_{1}, \ldots, a_{m} \} \) are linearly independent over \( \text{GF}(q) \) and \( Q(L(y_{1}), \ldots, L(y_{m})) = Q(L(x_{1}), \ldots, L(x_{k})) \).

**Theorem 4.7.** Let the hypotheses of Theorem 4.6 be satisfied. If \( 0 = r \), then \( Q(L(x_{1}), \ldots, L(x_{k})) \) is absolutely irreducible unless all the ratios \( j/a_{j} \), \( 1 \leq j \leq k \) are in \( \text{GF}(q) \). In that case \( Q(L(x_{1}), \ldots, L(x_{k})) \) is the product of first degree factors.

**Proof.** As in the proof of Theorem 4.6, we have a polynomial \( Q(L(x_{1}), \ldots, L(x_{k})) \) which may reduce to an \( m \)-variable polynomial. Now \( m = 1 \) if and only if \( a_{j}/a_{j} \) belongs to \( \text{GF}(q) \) for \( 1 \leq j \leq k \). If \( m > 1 \), \( Q(L(x_{1}), \ldots, L(x_{k})) \) is absolutely irreducible by Theorem 4.1 or its generalization. If \( m = 1 \), first degree factorization is always possible.

**Example 4.1.** This example illustrates Theorem 4.1. Let \( Q(x, y) = ax + ay + 1 \) where \( a^2 = a + 1 \) generates \( \text{GF}(3) \). Let \( L(x) = a^{r} + ax \).

Then \( r = 2 \), \( n = 3 \), and \( 0 \neq r \).

Thus

\[
Q(a^{r} + ax + 1, a^{r} + ay + 1) = (a^{r} + ax)^{2} + a^{r} + ay + (a^{r} + ax)(a^{r} + ay + 1)
\]

is absolutely irreducible.

**Example 4.2.** This example illustrates Theorem 4.2. Let \( Q(x, y) = ax + ay + 1 \) where \( a^2 = a + 1 \) generates \( \text{GF}(4) \). Let \( L(x) = a^{r} + ax \).

Then \( r = 2 \), \( n = 4 \), and \( 0 \neq r \).

Thus

\[
Q(a^{r} + ax + 1, a^{r} + ay + 1) = (a^{r} + ax)^{2} + a^{r} + ay + (a^{r} + ax)(a^{r} + ay + 1)
\]

is absolutely irreducible.

**Example 4.3.** This example illustrates Theorem 4.3. Let \( Q(x, y) = ax + ay + 1 \) where \( a^2 = a + 1 \) generates \( \text{GF}(16) \). Let \( L(x) = a^{r} + ax \).

Then \( r = 2 \), \( n = 4 \), and \( 0 \neq r \).

Then if \( b^{r} = b + 1 \) generates \( \text{GF}(16) \), we have

\[
Q(L(x), L(y)) = (Z + W^{3} + W^{4} + (Z + W^{2} + W) + 1
\]

\[
= \left( \sum_{i=0}^{3} [Z + W^{i} + W^{i+1}] \right)^{2}
\]

Each factor in (4.6) is absolutely irreducible, and thus \( Q(L(x), L(y)) \) is the product of 4 absolute irreducibles of degree 2.

**Example 4.4.** This example illustrates Theorem 4.6. Let \( Q(x, y, z) = ax + ay + z + 1 \) where \( a^2 = a + 1 \) generates \( \text{GF}(3) \). Let \( L(x) = a^{r} + ax \).

Then \( r = 2 \), \( n = 3 \), and \( 0 \neq r \).

Now if \( Z = Z + W^{3} + W^{4} + (Z + W^{2} + W) + 1 \) where \( Z = a^{r} + ax + 1 \) and \( v = y + z \), we have

\[
Q(x, y, z) = (ax + a^{r} + ax + z + 1 = Z + W^{3} + W^{4} + (Z + W^{2} + W) + 1
\]

where each factor in the right member of (4.7) is absolutely irreducible of degree 3.

**Example 4.5.** This example illustrates Theorem 4.6. Let \( Q(x, y, z) = ax + ay + z + 1 \) where \( a^2 = a + 1 \) generates \( \text{GF}(3) \). Let \( L(x) = a^{r} + ax \).

Then \( r = 2 \), \( n = 3 \), and \( 0 \neq r \).

Now if \( Z = a^{r} + ax + 1 \) and \( v = y + z \), we have

\[
Q(x, y, z) = (ax + a^{r} + ax + z + 1 = Z + W^{3} + W^{4} + (Z + W^{2} + W) + 1
\]

The coefficients of \( q(x, y, z) \) are absolutely irreducible of degree 3.

**Theorem 4.8.** Let \( Q(x_{1}, \ldots, x_{k}) = a_{1}x_{1} + \cdots + a_{k}x_{k} + 1 \) where \( a_{i} \) are algebraically independent over \( \text{GF}(q) \), and let \( L(x_{i}) = a_{i}x_{i} + 1 \). Then \( Q(L(x_{1}), \ldots, L(x_{k})) \) is an absolutely irreducible polynomial.

**Proof.** As in the proof of Theorem 4.6, we have a polynomial \( Q(L(x_{1}), \ldots, L(x_{k})) \) which may reduce to an \( m \)-variable polynomial. Now \( m = 1 \) if and only if \( a_{j}/a_{j} \) belongs to \( \text{GF}(q) \) for all \( 1 \leq j \leq k \). If \( m > 1 \), \( Q(L(x_{1}), \ldots, L(x_{k})) \) is absolutely irreducible by Theorem 4.1 or its generalization. If \( m = 1 \), first degree factorization is always possible.

**Example 4.6.** This example illustrates Theorem 4.6. Let \( Q(x, y, z) = ax + ay + z + 1 \) where \( a^2 = a + 1 \) generates \( \text{GF}(3) \). Let \( L(x) = a^{r} + ax \).

Then \( r = 2 \), \( n = 3 \), and \( 0 \neq r \).

Now if \( Z = a^{r} + ax + 1 \) and \( v = y + z \), we have

\[
Q(x, y, z) = (ax + a^{r} + ax + z + 1 = Z + W^{3} + W^{4} + (Z + W^{2} + W) + 1
\]

where each factor in the right member of (4.7) is absolutely irreducible of degree 3.
over $I(p)$ (and indeed over GF$(q^i)$). If $s \bar{r}$ and $s \bar{r}_i$ for at least one $i$, $1 \leq i \leq t$, then $Q(L(a_1), \ldots, L(a_n))$ is the product of $q^{r-h+u}$ absolute irreducibles of degree $q^{r-h+u} 
/ u$.

Proof. If $s \bar{r}_i$, the proof of Theorem 4.1 applies. If $s \bar{r}$ and $s \bar{r}_i$, $1 \leq i \leq t$, then $Q(L(a_1), \ldots, L(a_n))$ can be written as a polynomial in one variable $x$ where $x = a_1 + a_2 + \cdots + a_n$. We therefore have first degree factors over $I(p)$. The factors actually have coefficients in GF$(q^i)$ by Corollary 3.2 of [4].

Now assume that $s \bar{r}$ and $s \bar{r}_i$ for at least one $i$, $1 \leq i \leq t$. Now

\begin{equation}
Q[L(G(a_1)), \ldots, L(G(a_n))] = Q[x_1^q - x_1, \ldots, x_n^q - x_n] 
= \prod_{i=1}^{n} (a_{1i} x_1 + \cdots + a_{ni} x_n + \lambda_i)
\end{equation}

where the product extends over all $\lambda$ satisfying $x^q - x = 1$.

For a fixed $\lambda$, consider the product

\begin{equation}
P(a_1, \ldots, a_n) = \prod_{a_{1i} \cdots a_{ni}} [a_1 (a_{1i} + c_1) + \cdots + a_n (a_{ni} + c_n) + \lambda]
\end{equation}

where $G(c_i) = 0$. Since the roots of $G(x)$ are in GF$(q^i)$, it follows that the factors of (5.3) occur in (5.2). Although $\{a_1, \ldots, a_n\}$ are linearly independent over GF$(q)$, they may not be linearly independent over $W$, the subspace generated by the roots of $G(x)$. Thus there may be repeated factors in (5.3). By Lemma 2.7 and 2.8, each distinct factor appears with the same cardinality $q^u$ where $u \geq 0$. By Lemma 2.5, we then have

\begin{equation}
P(a_1, \ldots, a_n) = [P_i(G(a_1), \ldots, G(a_n))]^{q^u}
\end{equation}

where $P_i(G(a_1), \ldots, G(a_n))$ is absolutely irreducible of degree $q^{(r-h+u)}$.

The total number of such absolute irreducibles formed from the factors of (5.2) is $q^{r-h+u}$ since (5.2) is of degree $q^{-1}$ in the variables $G(x_1), \ldots, G(x_n)$. (Note that each factor $P_i(G(a_1), \ldots, G(a_n))$ appears exactly once in the factorization of (5.2).)

Corollary 5.1. For the case $s \bar{r}$ and $s \bar{r}_i$ for at least one $i$, $1 \leq i \leq t$, of Theorem 5.1, if $\{a_1, \ldots, a_n\}$ are linearly independent over $W$, the vector space of roots of $G(x) = 0$, then $Q(L(a_1), \ldots, L(a_n))$ is the product of $q^{r-h}$ absolute irreducibles of degree $q^{r-h}$.

Proof. Under the hypothesis of linear independence over $W$, (5.1) has only the trivial solution $\{c_1, \ldots, c_n\} = (0, \ldots, 0)$. Consequently the cardinality of the vector space $V$ of solutions of (5.1) is 1, and therefore \(|W \cap V| = q^0 = 1\) (see Lemma 2.8). We conclude that $u = 0$.

Remark. In Theorems 4.1, 4.3, 4.5, and 4.6, $G(x) = x^q - x$. Thus the hypothesis of linear independence of the $a_i$ over GF$(q)$ in these theorems insures that $u = 0$.

In general, $u$ is a function of $r, q, k$, and the degree of linear dependence of $\{a_1, \ldots, a_k\}$ over $W$. Thus it does not appear convenient to give an algorithm for computing $u$. The following example shows that values of $u > 0$ can be obtained.

Example 5.1. Let $\theta$ be a root of $x^\theta + x + 1$, an irreducible of degree 9 over GF$(2)$, so that $\theta$ generates GF$(2^9)$. Let $\beta$ be a root of $x^{\theta^q} + x^{\theta} + 1$, an irreducible of degree 3 over GF$(2)$, $\beta$ generates GF$(2^3)$. Let $Q(a_1, a_2) = \theta a_1 + \theta^q a_2 + 1$. Let $L(x) = x^\theta + x^\theta + 1$ with corresponding ordinary polynomial $I(x) = x^3 + x^\theta + x + 1$. Here $k = 2$, $r = 9$, $g(x) = x^\theta - 1$, $j = 3$, and $G(x) = x^9 - x$. Since $s = [deg \theta, deg \theta^q] = 9$, we have $s \bar{r}$, but $s$ does not divide $c_1 = 6$ and $c_2 = 3$. The vector space $W$ of roots of $G(x)$ is GF$(8)$. Since $\theta a_1 + \theta^q a_2 = 0$ implies $c_1 = -\beta c_2$, each element $c_2$ of GF$(8)$ determines $a_2 = c_2 G(8)$. Hence $\beta a_1 + \theta^q a_2 = 0$ has $2^s$ solutions $\{c_1, c_2\}$ where $c_1$ and $c_2$ are roots of $G(x) = 0$. We have $u = 3$ and $Q(L(a_1), L(a_2))$ factors into $q^{r-h+u} = 2^s$ absolute irreducibles of degree $q^{r-h+u} = 1$.

We observe that the polynomial can be written

\begin{equation}
Q(L(a_1), L(a_2)) = 6x^9 + 6x^3 + 6x + 1
\end{equation}

where $X = x^\theta + x^\theta$. Since (5.5) is a polynomial in the single variable $X$ it is the product of (absolutely irreducible) first degree factors in $x^\theta$ and $x^\theta$.

Corollary 5.2. If $L(x) = x^\theta - x$ has corresponding ordinary polynomial $I(x)$ with exponent $r$ in Theorem 5.1 and $s \bar{r}$, then $Q(L(a_1), \ldots, L(a_n))$ is the product of $q^{r-h}$ absolute irreducibles of degree $q^{r-h}$.

Remark. Note that Corollary 5.2 is the same as Theorem 4.5.

Proof. Since $G(x) = x^\theta - x$, the coefficients $a_1, \ldots, a_n$ of $Q(a_1, \ldots, a_n)$ are linearly independent over $W$, the vector space of roots of $G(x)$, $G(a_i) = 0$, by the hypothesis that $\{a_1, \ldots, a_n\}$ are linearly independent over GF$(q)$. If $s = 1$, this hypothesis insures that $k = 1$ and we have $q^s$ first degree factors of $Q(L(a_1), \ldots, L(a_n))$.

If $s > 1$, then $s \bar{r}$ since the term $x^\theta$ appears in $L(a)$. Consequently Corollary 5.1 is satisfied with $j = 1$, and we have $q^{r-h}$ absolute irreducibles of degree $q^{r-h}$.

References


[2] Andrew F. Long, "A theorem on factorable irreducible polynomials in several vari-
ables over a finite field with the substitution $x^2 - x$ for $x$, Math. Nachr. 63 (1974), pp. 123–130.


4. Andrew F. Long and Theresa P. Vaughan, Factorization of $Q(k(T)(a))$ over a finite field where $Q(a)$ is irreducible and $k(T)(a)$ is linear I, Linear Algebra and Appl. 13 (1976), pp. 207–221.

5. — — Factorization of $Q(k(T)(a))$ over a finite field where $Q(a)$ is irreducible and $k(T)(a)$ is linear II, Ibid. 11 (1975), pp. 53–72.


BOOKS PUBLISHED BY THE POLISH ACADEMY OF SCIENCES INSTITUTE OF MATHEMATICS


MONOGRAFIE MATEMATYCZNE

53. R. Engelking, General topology, in print.

New series

BANACH CENTER PUBLICATIONS