ON A CONJECTURE OF GOLOMB

WILLIAM H. MILLS AND NEAL ZIERLER
ON A CONJECTURE OF GOLOMB

W. H. MILLS AND NEAL ZIERLER

On the basis of empirical evidence for \( n = 2, 3, 4, \) and 5, Golomb has conjectured that the degree of every irreducible factor of

\[
F(x) = x^{2^n+1} + x^{2^n-1} + 1
\]

over \( GF(2) \) divides \( 6(n - 1) \). We prove the stronger result that the degree of every irreducible factor of \( F(x) \) divides either \( 2(n - 1) \) or \( 3(n - 1) \), but not \( n - 1 \).

It follows from this that \( F(x) = F_1(x)F_2(x) \), where the degrees of the irreducible factors of \( F_1(x) \) divide \( 2(n - 1) \), and the degrees of the irreducible factors of \( F_2(x) \) divide \( 3(n - 1) \). The polynomials \( F_1(x) \) and \( F_2(x) \) have a number of interesting properties that we discovered for small values of \( n \) by computer runs, and that later we were able to prove for arbitrary values of \( n \). It is noteworthy that not only were these properties suggested by computer runs, but the central ideas of their proof were also suggested by these runs. The key lemma in our study of \( F_1(x) \) and \( F_2(x) \) was actually discovered for \( n = 2, 4, \) and 6 by machine. It was then not difficult to prove it for arbitrary \( n \).

1. A proof of Golomb’s conjecture. In this paper all polynomials are over \( GF(2) \).

Let \( n \) be an integer, \( n \geq 2 \), and set \( r = 2^{n-1} \). The polynomial we are interested in is

\[
F(x) = x^{2^r+1} + x^{r-1} + 1.
\]

Set

\[
K = GF(r), \quad L = GF(r^2), \quad M = GF(r^3).
\]

**Theorem 1.** Let \( \alpha \) be a root of \( F(x) \). Then \( \alpha \in K \) and either \( \alpha \in L \) or \( \alpha^{2^2+r+1} = 1 \).

**Proof.** Suppose \( \alpha \) is in \( K \). Then \( \alpha^{-1} = 1 \) and

\[
0 = F(\alpha) = \alpha^{2^{r+1}},
\]

which is impossible. Hence \( \alpha \) is not in \( K \). Next we observe that

\[
F(x^r) + x^{r^2-r}F(x) = (x^{r^2-1} + 1)(x^{r^2+r+1} + 1).
\]
The identity (1) is readily verified by expanding both sides. Since $r$ is a power of 2, we have $F(x) | F(x^r)$ so that
\[ F(x) | (x^{r^2-1} + 1)(x^{r^2+r+1} + 1). \]
Therefore, either $\alpha^{r^2-1} = 1$, in which case $\alpha \in L$, or $\alpha^{r^2+r+1} = 1$.

Since $r^2 + r + 1$ is a factor of $r^3 - 1$ it follows from Theorem 1 that any root $\alpha$ of $F(x)$ lies in either $L$ or $M$, but not in $K$. This implies that the degree of every irreducible factor of $F(x)$ divides either $2(n - 1)$ or $3(n - 1)$, but not $n - 1$. Thus, Theorem 1 implies the truth of Golomb's conjecture.

2. The polynomial $G(x)$. We can obtain more information about the roots of $F(x)$ by studying the closely related polynomial
\[ G(x) = (x^r + x^{r-1} + 1)(x^{r+1} + x + 1). \]

We begin by observing that the following identity holds:
\[ (x^{2r+1} + 1)F(x^{2r}) + \alpha > 2r(r - 1) \tau (\alpha_0 = G(\#2r+1)). \]

The identity (2) is readily verified by expanding both sides.

**Lemma 1.** If $\alpha$ is a root of $F(x)$, then $\alpha^{2r+1}$ is root of $G(x)$.

**Proof.** Since $r$ is a power of 2, we have $F(x) | F(x^r)$. Hence (2) gives us $F(x) | G(x^{2r+1})$. Therefore $F(\alpha) = 0$ implies that $G(\alpha^{2r+1}) = 0$, which proves the lemma.

Set $G_1(x) = x^r + x^{r-1} + 1$ and $G_2(x) = x^{r+1} + x + 1$, so that $G(x) = G_1(x)G_2(x)$. Let $H(x)$ be the polynomial whose roots are the inverses of the roots of $G_1(x)$. Thus $H(x) = x^r + x + 1$. It is known\(^1\) that the roots of $H(x)$ lie in the field $L$, but not in $K$, and the roots of $G_2(x)$ lie in $M$. This is easily seen by looking at the effect of the automorphism $\sigma$ given by $\sigma \omega = \omega^r$ for all $\omega$ in the splitting field of $G(x)$. Thus if $\beta$ is a root of $H(x)$, then $\sigma \beta = \beta + 1$, so that $\sigma^2 \beta = \beta$, $\alpha \beta \neq \beta$. This implies that $\beta$ lies in $L$ but not in $K$. On the other hand, if $\beta$ is a root of $G_2(x)$, then $\sigma \beta = 1 + \beta^{-1}$, $\sigma^2 \beta = (1 + \beta)^{-1}$, and $\sigma^3 \beta = \beta$, which implies that $\beta$ lies in $M$. It follows that the roots of $G_1(x)$ lie in $L$ but not in $K$, and that $G_1(x)$ and $G_2(x)$ have no common roots.

Since the trinomial $x^a + x^b + 1$ has multiple roots if and only if $a$ and $b$ are both even, we see that $G_1(x)$ and $G_2(x)$ do not have multiple roots. Hence $G(x)$ does not have multiple roots. Moreover $F(x)$ does not have multiple roots.

---

\(^1\) These results have been credited to J. Riordan. See [1, p. 93].
LEMMA 2. Let $\alpha$ be a root of $F(x)$ and let $\beta = \alpha^{2r+1}$. If $\beta$ is a root of $G_1(x)$, then $\alpha$ lies in $L$. If $\beta$ is a root of $G_2(x)$, then $\alpha^{2^r+1} = 1$ and $\alpha$ lies in $M$.

Proof. We have

$$0 = F(\alpha) = \beta + \alpha^{r-1} + 1,$$

so that

$$1 + \beta = \alpha^{r-1}.$$

Suppose first $\beta$ is a root of $G_1(x)$. Then

$$1 = \beta^{r-1}(\beta + 1) = \alpha^{(2r+1)(r-1)+r-1} = \alpha^{(2^r+2)(r-1)}.$$

Hence

$$1 = \alpha^{(r^2+1)(r-1)} = \alpha^{r^2-1},$$

so that $\alpha \in GF(r^2) = L$.

On the other hand, suppose that $\beta$ is a root of $G_2(x)$. Then

$$\alpha^{r-1} = 1 + \beta = \beta^{r+1} = \alpha^{(2r+1)(r+1)}.$$ 

Therefore

$$\alpha^{2^r+2r+2} = 1,$$

or

$$\alpha^{r^2+r+1} = 1.$$ 

Since $r^2 + r + 1$ divides $r^3 - 1$, we have

$$\alpha \in GF(r^2) = M,$$

and the proof is complete.

We note that Lemmas 1 and 2 imply Golomb’s conjecture. This gives us a second, but longer, proof of his conjecture—one whose main idea was suggested by computer results.

3. The polynomials $F_1(x)$ and $F_2(x)$. By Theorem 1 we can write

$$F(x) = F_1(x)F_2(x),$$

where every root of $F_1(x)$ lies in $L$ but not in $K$, and every root of $F_2(x)$ lies in $M$ but not in $K$. Since $L \cap M = K$ the factors $F_1(x)$ and $F_2(x)$ are uniquely determined. If $\alpha$ is a root of $F_1(x)$, then $\alpha^{2^r+1}$ is a root of $G_1(x)$. If $\alpha$ is a root of $F_2(x)$, then $\alpha^{2^r+1}$ is a root of $G_2(x)$. 

The degree of every irreducible factor of $F(x)$ divides $2(n - 1)$, but not $n - 1$. The degree of every irreducible factor of $F_3(x)$ divides $3(n - 1)$ but not $n - 1$.

For $2 \leq n \leq 18$, our computer results showed that

\[
\text{degree of } F_i(x) = \begin{cases} 
    r & \text{if } n \text{ is even}, \\
    r - (-2)^{3(n+1)} & \text{if } n \text{ is odd}.
\end{cases}
\]

In this section we will prove that (3) holds for all $n \geq 2$. We use the following characterization of the roots of $F_i(x)$:

**Lemma 3.** An element $\alpha$ of $L$ is a root of $F_i(x)$ if and only if $\alpha^{2r+1}$ is a root of $G_i(x)$.

**Proof.** It has already been shown that if $\alpha$ is a root of $F_i(x)$, then $\alpha^{2r+1}$ is a root of $G_i(x)$. Now let $\alpha$ be an element of $L$, set $\beta = \alpha^{2r+1}$, and suppose that $\beta$ is a root of $G_i(x)$. Since $\alpha^{2r-1} = 1$ we have $(\alpha\beta)^{r-1} = 1$. Therefore

\[
\beta^{r-1}F(\alpha) = \beta^{r-1}(\beta + \alpha^{r-1} + 1) = \beta^r + 1 + \beta^{r-1} = 0,
\]

so that $\alpha$ is a root of $F(x)$. Since $\alpha \in L$, it follows that $\alpha$ is a root of $F_i(x)$.

Similarly it may be shown that an element $\alpha$ of $M$ such that

\[
\alpha^{2r+1} = 1
\]

is a root of $F_i(x)$ if and only if $\alpha^{2r+1}$ is a root of $G_2(x)$.

**Lemma 4.** Let $\beta$ be a nonzero element of $L$, and let $R(\beta)$ denote the number of elements $\alpha$ in $L$ such that $\alpha^{2r+1} = \beta$. Then

\[
R(\beta) = \begin{cases} 
    1 & \text{if } n \text{ is even}, \\
    3 & \text{if } n \text{ is odd and } \beta \text{ is a cube in } L, \\
    0 & \text{otherwise}.
\end{cases}
\]

**Proof.** Any common divisor of $2r + 1$ and $r^2 - 1$ must divide

\[
(2r - 1)(2r + 1) - 4(r^2 - 1) = 3.
\]

Since $r = 2^{n-1}$, it follows that the greatest common divisor of $2r + 1$ and $r^2 - 1$ is 1 if $n$ is even and is 3 if $n$ is odd.

Since $r^2 - 1$ is the order of the multiplicative group of $L$, and since this group is cyclic, the result (4) follows at once.

**Theorem 2.** Suppose $n$ is even. Then the degree of $F_i(x)$ is $r$
and the degree of $F_2(x)$ is $r + 1$.

**Proof.** It follows from Lemmas 3 and 4 that $F_t(x)$ and $G_t(x)$ have the same degree. Therefore, the degree of $F_t(x)$ is $r$. Since $F(x) = F_t(x)F_2(x)$ and the degree of $F(x)$ is $2r + 1$, the degree of $F_2(x)$ is $r + 1$.

For $n$ odd the situation is clearly more complicated.

**Theorem 3.** Suppose $n$ is odd. Then the degree of $F_t(x)$ is $r - (-2)^{\frac{n}{3}(n+1)}$ and the degree of $F_2(x)$ is

$$((-2)^{\frac{n}{3}(n-1)} - 1)^2.$$  

**Proof.** Let $f_t$ denote the degree of $F_t(x)$. By Lemmas 3 and 4, $f_t$ is three times the number of roots $\beta$ of $G_t(x)$ that are cubes in $L$. Replacing $\beta$ by $\beta^{-1}$ we see that $f_t$ is three times the number of roots of $H(x)$ that are cubes in $L$, where $H(x) = x^r + x + 1$ as before.

Let $\sigma$ again be the automorphism such that $\sigma \omega = \omega^r$ for all $\omega$ in $L$. Let $\beta$ be a root of $H(x)$. Then $\sigma \beta = \beta + 1$. Set $\lambda = \beta(\beta + 1)$. Then

$$\lambda = \beta \sigma \beta = \beta^{1+r},$$

which is an element of $K$. Moreover $\beta$ is a cube in $L$ if and only if $\lambda$ is a cube in $K$. Since $x^2 + x = \lambda$ has only two roots, we see that $\lambda$ is not of the form $\tau(\tau + 1)$ with $\tau$ in $K$. Conversely, let $\lambda$ be an element of $K$ that is not of the form $\tau(\tau + 1)$ with $\tau$ in $K$. Let $\beta$ be one of the two roots of

$$(5) \quad x^2 + x = \lambda.$$

Since $\sigma \lambda = \lambda$, it follows that $\sigma \beta$ is also a root of (5). Now the roots of (5) are $\beta$ and $\beta + 1$. Furthermore $\beta$ is not in $K$ so that $\sigma \beta \neq \beta$. Therefore

$$\beta + 1 = \sigma \beta = \beta^r,$$

and $\beta$ is a root of $H(x)$. Thus, every cube $\lambda$ in $K$, not of the form $\tau(\tau + 1)$ with $\tau$ in $K$, corresponds to exactly two roots of $H(x)$ that are cubes in $L$. Hence $f_t = 6N$, where $N$ is the number of cubes of $K$ that are not of the form $\tau(\tau + 1)$ with $\tau$ in $K$. Since the number of nonzero cubes in $K$ is $(r - 1)/3$ we have

$$N + N_0 = (r - 1)/3$$

where $N_0$ is the number of nonzero cubes in $K$ that are of the form $\tau(\tau + 1)$ with $\tau$ in $K$. We will calculate $N_0$ by means of cubic cyclo-
Cyclotomic numbers. Let $g$ be a generator of the multiplicative group of $\mathbb{Z}/N\mathbb{Z}$, where $N$ is a positive integer. The cubic cyclotomic number $(i,j)$ is defined to be the number of solutions $t,u$ of

$$1 + g^{i+3t} = g^{j+3u}, \quad 0 \leq t, u < (r - 1)/3.$$ 

Setting $\tau = g^{i+3t}$ and

$$1 + \tau = g^{j+3u}, \quad 0 \leq i, j < 3,$$

we see that the number of $\tau$ in $K$ such that $\tau(\tau + 1)$ is a nonzero cube in $K$ is

$$(0, 0) + (1, 2) + (2, 1).$$

However, each nonzero $\lambda$ in $K$ of the form $\tau(\tau + 1)$ corresponds to two values of $\tau$. Hence

$$2N_0 = (0, 0) + (1, 2) + (2, 1).$$

It is known, [2, pp. 148-149] or [3, pp. 32-35], that

$$(1, 2) = (2, 1) = (0, 0) + 1$$

and

$$9(0, 0) = r - 8 + (-2)^{(n+1)/3}.$$ 

Putting these relations together we obtain

$$f_1 = 6N = 2r - 2 - 6N_0 = 2r - 8 - 9(0, 0)$$

$$= r - (-2)^{(n+1)/3}.$$ 

Finally, the degree of $F_3(x)$ is

$$2r + 1 - f_1 = r + 1 + (-2)^{(n+1)/3} = ((-2)^{(n-1)/3} - 1)^2,$$

and the proof is complete.

References


Received June 8, 1968.

INSTITUTE FOR DEFENSE ANALYSES
PRINCETON, NEW JERSEY
Jon F. Carlson, Automorphisms of groups of similitudes over $F_3$ ............ 485
W. Wistar (William) Comfort, Neil Hindman and Stelios A. Negrepontis, $F'$-spaces and their product with $P$-spaces .................................................. 489
Archie Gail Gibson, Triples of operator-valued functions related to the unit circle .......................................................... 503
David Saul Gillman, Free curves in $E^3$ ..................................... 533
E. A. Heard and James Howard Wells, An interpolation problem for subalgebras of $H^\infty$ .................................................. 543
Albert Emerson Hurd, A uniqueness theorem for weak solutions of symmetric quasilinear hyperbolic systems .......................................... 555
E. W. Johnson and J. P. Lediaev, Representable distributive Noether lattices .......................................................... 561
David G. Kendall, Incidence matrices, interval graphs and seriation in archeology .......................................................... 565
Robert Leroy Kruse, On the join of subnormal elements in a lattice ........ 571
D. B. Lahiri, Some restricted partition functions; Congruences modulo 3 .... 575
Norman D. Lane and Kamla Devi Singh, Strong cyclic, parabolic and conical differentiability .................................................. 583
William Franklin Lucas, Games with unique solutions that are nonconvex .................................................. 599
Eugene A. Maier, Representation of real numbers by generalized geometric series .......................................................... 603
Daniel Paul Maki, A note on recursively defined orthogonal polynomials ...... 611
Mark Mandelker, $F'$-spaces and $z$-embedded subspaces .................... 615
James R. McLaughlin and Justin Jesse Price, Comparison of Haar series with gaps with trigonometric series .................................................. 623
Ernest A. Michael and A. H. Stone, Quotients of the space of irrationals .... 629
William H. Mills and Neal Zierler, On a conjecture of Golomb ............... 635
J. N. Pandey, An extension of Haimo’s form of Hankel convolutions ....... 641
Terence John Reed, On the boundary correspondence of quasiconformal mappings of domains bounded by quasicircles .................................................. 653
Haskell Paul Rosenthal, A characterization of the linear sets satisfying Herz’s criterion .......................................................... 663
George Thomas Sallee, The maximal set of constant width in a lattice ........ 669
I. H. Sheth, On normaloid operators ........................................ 675
James D. Stasheff, Torsion in $BBSO$ ........................................ 677
Billy Joe Thorne, $A - P$ congruences on Baer semigroups .................... 681
Robert Breckenridge Warfield, Jr., Purity and algebraic compactness for modules .......................................................... 699
Joseph Zaks, On minimal complexes ........................................ 721