Pacific Journal of Mathematics

ON A CONJECTURE OF GOLOMB

WILLIAM H. MILLS AND NEAL ZIERLER

Vol. 28, No. 3 May 1969

PACIFIC JOURNAL OF MATHEMATICS
Vol. 28, No. 3, 1969

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

$$F(x) = x^{2^n+1} + x^{2^{n-1}-1} + 1$$

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, $n \geqq 2$, and set $r = 2^{n-1}$. The polynomial we are interested in is

$$F(x) = x^{2r+1} + x^{r-1} + 1 .$$

Set

$$K = GF(r),\ L = GF(r^2),\ M = GF(r^3) .$$

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

Proof. Suppose α is in K. Then $\alpha^{r-1} = 1$ and

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

which is impossible. Hence α is not in K. Next we observe that

$$F(x^r) + x^{r^2-r}F(x) = (x^{r^2-1} + 1)(x^{r^2+r+1} + 1) . \tag{1}$$

The identity (1) is readily verified by expanding both sides. Since r is a power of 2, we have $F(x) \mid F(x^r)$ so that

$$F(x) \mid (x^{r^2-1} + 1)(x^{r^2+r+1} + 1) .$$

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 α 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:

$$(x^{2r+1} + 1)F(x^{2r}) + x^{2r(r-1)}F(x) = G(x^{2r+1}) . \tag{2}$$

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

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

Proof. Since r is a power of 2, we have $F(x) \mid F(x^{2r})$. Hence (2) gives us $F(x) \mid G(x^{2r+1})$. 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 σ given by $\sigma\omega = \omega^r$ for all ω in the splitting field of $G(x)$. Thus if β is a root of $H(x)$, then $\sigma\beta = \beta + 1$, so that $\sigma^2\beta = \beta$, $\alpha\beta \neq \beta$. This implies that β lies in L but not in K. On the other hand, if β 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 β 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 α be a root of $F(x)$ and let $\beta = \alpha^{2r+1}$. If β is a root of $G_1(x)$, then α lies in L. If β is a root of $G_2(x)$, then $\alpha^{r^2+r+1} = 1$ and α lies in M.*

Proof. We have

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

so that

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

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

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

Hence

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

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

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

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

Therefore

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

or

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

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

$$\alpha \in GF(r^3) = M ,$$

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 α is a root of $F_1(x)$, then α^{2r+1} is a root of $G_1(x)$. If α is a root of $F_2(x)$, then α^{2r+1} is a root of $G_2(x)$.

The degree of every irreducible factor of $F_1(x)$ divides $2(n-1)$, but not $n-1$. The degree of every irreducible factor of $F_2(x)$ divides $3(n-1)$ but not $n-1$.

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

$$\text{(3)} \qquad \text{degree of } F_1(x) = \begin{cases} r & \text{if } n \text{ is even}, \\ r - (-2)^{\frac{1}{2}(n+1)} & \text{if } n \text{ is odd}. \end{cases}$$

In this section we will prove that (3) holds for all $n \geqq 2$. We use the following characterization of the roots of $F_1(x)$:

LEMMA 3. *An element α of L is a root of $F_1(x)$ if and only if α^{2r+1} is a root of $G_1(x)$.*

Proof. It has already been shown that if α is a root of $F_1(x)$, then α^{2r+1} is a root of $G_1(x)$. Now let α be an element of L, set $\beta = \alpha^{2r+1}$, and suppose that β is a root of $G_1(x)$. Since $\alpha^{r^2-1} = 1$ we have $(\alpha\beta)^{r-1} = 1$. Therefore

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

so that α is a root of $F(x)$. Since $\alpha \in L$, it follows that α is a root of $F_1(x)$.

Similarly it may be shown that an element α of M such that

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

is a root of $F_2(x)$ if and only if α^{2r+1} is a root of $G_2(x)$.

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

$$\text{(4)} \qquad R(\beta) = \begin{cases} 1 & \text{if } n \text{ is even}, \\ 3 & \text{if } n \text{ is odd and } \beta \text{ is a cube in } L, \\ 0 & \text{otherwise}. \end{cases}$$

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 $F_1(x)$ is r*

and the degree of $F_2(x)$ *is* $r + 1$.

Proof. It follows from Lemmas 3 and 4 that $F_1(x)$ and $G_1(x)$ have the same degree. Therefore, the degree of $F_1(x)$ is r. Since $F(x) = F_1(x)F_2(x)$ 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* $F_1(x)$ *is* $r - (-2)^{\frac{1}{2}(n+1)}$ *and the degree of* $F_2(x)$ *is*

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

Proof. Let f_1 denote the degree of $F_1(x)$. By Lemmas 3 and 4, f_1 is three times the number of roots β of $G_1(x)$ that are cubes in L. Replacing β by β^{-1} we see that f_1 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 σ again be the automorphism such that $\sigma\omega = \omega^r$ for all ω in L. Let β 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 β is a cube in L if and only if λ is a cube in K. Since $x^2 + x = \lambda$ has only two roots, we see that λ is not of the form $\tau(\tau + 1)$ with τ in K. Conversely, let λ be an element of K that is not of the form $\tau(\tau + 1)$ with τ in K. Let β be one of the two roots of

$$x^2 + x = \lambda . \tag{5}$$

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

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

and β is a root of $H(x)$. Thus, every cube λ in K, not of the form $\tau(\tau + 1)$ with τ in K, corresponds to exactly two roots of $H(x)$ that are cubes in L. Hence $f_1 = 6N$, where N is the number of cubes of K that are not of the form $\tau(\tau + 1)$ with τ 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 τ in K. We will calculate N_0 by means of cubic cyclo-

tomic numbers. Let g be a generator of the multiplicative group of K. The cubic cyclotomic number (i, j) is defined to be the number of solutions t, u of

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

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

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

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

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

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

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

Putting these relations together we obtain

$$\begin{aligned} f_1 = 6N &= 2r - 2 - 6N_0 = 2r - 8 - 9(0, 0) \\ &= r - (-2)^{\frac{1}{2}(n+1)} . \end{aligned}$$

Finally, the degree of $F_2(x)$ is

$$2r + 1 - f_1 = r + 1 + (-2)^{\frac{1}{2}(n+1)} = ((-2)^{\frac{1}{2}(n-1)} - 1)^2 ,$$

and the proof is complete.

References

1. Solomon W. Golomb, *Shift register sequences*, Holden-Day, Inc., 1967.
2. Marshall Hall, Jr., *Combinatorial theory*, Blaisdell Publishing Co., 1967.
3. Thomas Storer, *Cyclotomy and difference sets*, Markham Publishing Co., 1967.

Received June 8, 1968.

Institute for Defense Analyses
Princeton, New Jersey

PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. It should not contain references to the bibliography. Manuscripts, in duplicate if possible, may be sent to any one of the four editors. Please classify according to the scheme of Math. Rev. **36**, 1539-1546. All other communications to the editors should be addressed to the managing editor, Richard Arens, University of California, Los Angeles, California, 90024.

50 reprints are provided free for each article; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published monthly. Effective with Volume 16 the price per volume (3 numbers) is $8.00; single issues, $3.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues $1.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 7-17, Fujimi 2-chome, Chiyoda-ku, Tokyo, Japan.

Pacific Journal of Mathematics
Vol. 28, No. 3 May, 1969