PUC

Series: Monographs in Computer Science
and Computer Applications

Nº 1/73

A CHARACTERIZATION OF ALGEBRAIC FUNCTIONS WHOSE SOLUTIONS ARE N^{th} ROOTS OF UNITY

by

Carlos R. P. Hartmann
and
Larry Kerschberg

Computer Science Department - Rio Datacenter

Pontifícia Universidade Católica do Rio de Janeiro
Rua Marquês de São Vicente, 209 — ZC-20
Rio de Janeiro — Brasil

A CHARACTERIZATION OF ALGEBRAIC FUNCTIONS WHOSE SOLUTIONS ARE N^{th} ROOTS OF UNITY

C. R. P. Hartmann
Associate Professor
Syracuse University

and

L. Kerschberg
Associate Professor
Computer Science Department
PUC/RJ

Series Editor: Prof. S. M. dos Santos

March/1973

ABSTRACT

This investigation presents existence theorems for algebraic functions over Galois Fields which admit n^{th} roots of unity as solutions. For a special class of these functions, the existence test reduces to calculating the greatest common divisor of integers. These results are applied to the characterization of a class of binary cyclic codes whose minimum distance is exactly three.

1. INTRODUCTION

Algebraic functions over Galois Fields have been studied extensively in pure and applied mathematics [1 - 2]. In this investigation we characterize certain algebraic functions whose solutions are n^{th} roots of unity. In Section 2 the problem is stated in its most general form. Necessary and sufficient conditions for the existence of a solution are presented.

Section 3 presents a special case in which the greatest common divisor of integers determines the existence of a solution. In Section 4 an application to coding theory is presented; a class of one-error correcting codes whose true minimum distance is three is characterized. Lastly, a table is given for those codes of length n ($3 \leq n \leq 127$) which belong to this class.

2. PROBLEM STATEMENT

Let $GF(q = p^{\ell})$ denote the Galois Field of characteristic p, p a prime. The ring of polynomials in x over GF(q) is denoted by $GF(q)[x]$. Let (a, b) be the greatest common divisor of a and b. We wish to study the following problem:

P) For a given $f(x) \in GF(q)[x]$ and a given natural number n, find at least one $x_0 \in GF(q^m)$, where $GF(q^m)$ is the spliting field of f(x), such that

$$f(x_0) = 0 \quad \text{and} \quad x_0^n = 1 \qquad (1)$$

Theorem 1 $P)$ admits a solution if and only if $f(x)$ and $x^n - 1 \in GF(q)[x]$ are not relatively prime, ie, $(f(x), x^n - 1) \neq 1$

Proof: ($\Longrightarrow$) Trivial.

($\Longleftarrow$) If $(f(x), x^n - 1) \neq 1$ then there exists an x_0 such that $(x - x_0) \mid f(x)$ and $(x - x_0) \mid (x^n - 1)$. Thus, x_0 satisfies (1)

The above result can easily be implemented on a digital computer. Once the existence of a solution to $P)$ has been verified, the n^{th} roots of unity may be substituted in $f(x)$ to see which of them are roots of $f(x)$. The next two corollaries are refinements of Theorem 1.

Corollary 1 If $n = p^r w = uw$ then $(f(x), x^n - 1) \neq 1$ if and only if $(f(x), x^{n/u} - 1) \neq 1$.

Proof: Since $n = uw$ then $n = (n/u)\, u$. Also, p is the characteristic of $GF(q)$ which implies that $(x^{(n/u)\, u} - 1) = (x^{(n/u)} - 1)^u$. Thus $x_0^n = 1$ iff $x^{n/u} = 1$.

Since $x_0 = 1$ can be readily verified by substitution in (1), we wish to know when $P)$ has solutions different from unity.

Corollary 2 If $n = p^r w = uw$ then P) admits a solution $x_0 \neq 1$ if and only if $(f(x), \frac{x^{n/u} - 1}{x - 1}) \neq 1$.

The above results will be used to examine a special case in which the existence of a solution reduces to calculating the greatest common divisor of integers.

3. A SPECIAL CASE

In this section we particularize P) to P') as follows:

P') Let $p = 2$ and $\ell = 1$ with $n > 0$ of the form

$$n = 2^v (2^k + 2^t - 2^s - 1) \quad \text{such that } (2, 2^k + 2^t - 2^s - 1) = 1$$

and $t \geq s$.

Define $f(x) \in GF(2)[x]$ as

$$f(x) = x^{2^{k+v}} + x^{2^{t+v}} + x^{2^{s+v}} + x^{2^v}$$

Find $x_0 \in GF(2^m)$ such that $f(x_0) = 0$, $x_0^n + 1 = 0$, and $x_0 \neq 1$.

Theorem 2 P') admits a solution if and only if

$$((2^{k-s} - 1)(2^{t-s} - 1), 2^k + 2^t - 2^s - 1) \neq 1$$

In order to prove theorem 2 we need the result given by the following lemma:

Lemma 1 Let θ and $\emptyset$ be integers. If $(\theta, b) = 1$, then $(a, b) = (\theta a + \emptyset b, b)$.

Proof: Let $(a, b) = d$, thus $d|b$. Moreover, $d|g$ where $g = (\theta a + \emptyset b, b)$. Since $g|(\theta a + \emptyset b)$ and $g|b$, then $g|\theta a$. Now $(\theta, b) = 1$ and $g|b \Longrightarrow (\theta, g) = 1 \Longrightarrow g|a$. Thus $g|a$ and $g|b \Longrightarrow g|d$. Finally, $g|d$ and $d|g \Longrightarrow d = g$.

Notice that Lemma 1 is also true for polynomials over any field.

Proof of Theorem 2:

$$\text{Let } b(x) = \frac{x^{n/2^v} + 1}{x + 1} = x^{2^k + 2^t - 2^s - 2} + x^{2^k + 2^t - 2^s - 3} + \ldots + x + 1.$$

Since GF(2) is of characteristic 2,

$$f(x) = x^{2^{k+v}} + x^{2^{t+v}} + x^{2^{s+v}} + x^{2^v} = (x^{2^k} + x^{2^t} + x^{2^s} + x)^{2^v} =$$

$$(\bar{f}\ (x))^{2^v}.$$

Since b(x) is a complete polynomial with no repeated roots,

$(f(x), b(x)) = (\bar{f}(x), b(x))$. Moreover, $(x(x+1), b(x)) = 1$ so that, by Lemma 1, $(\bar{f}(x), b(x)) = \left(\frac{\bar{f}\ (x)}{x(x+1)}, b(x)\right)$. Thus, $P')$ admits a solution iff

$$\left(\frac{\bar{f}\ (x)}{x(x+1)}, b(x)\right) = (x^{2^k-2} + x^{2^k-3} + \ldots + x^{2^t-1} + x^{2^s-2} + x^{2^s-3} +$$

$$+ \ldots + x + 1, b(x)) \neq 1 \qquad (2)$$

Case 1) $t > s$ By Lemma 1,

$$(a, b) = (a + b, b) \qquad (3)$$

Using (2) and (3) we see that $P')$ admits a solution iff

$$(x^{2^k} + 2^t - 2^s - 2 + x^{2^k} + 2^t - 2^s - 3 + \ldots + x^{2^k} - 1 + x^{2^t} - 2 + x^{2^t} - 3$$

$$+ \ldots + x^{2^s} - 1 \,,\ b(x)) =$$

$$= (x^{2^k} - 1 (x^{2^t} - 2^s - 1 + x^{2^t} - 2^s - 2 + \ldots + x + 1) + x^{2^s} - 1 \ (x^{2^t} - 2^s - 1 +$$

$$+ x^{2^t - 2^s - 2} + \ldots + x + 1),\ b(x))$$

$$= (x^{2^s} - 1 \ (x^{2^k} - 2^s + 1)(x^{2^t} - 2^s - 1 + x^{2^t} - 2^s - 2 + \ldots + x + 1),\ b(x))$$

$$= (x^{2^s} - 1 \ (x^{2^k} - 2^s + 1) \left(\frac{x^{2^t} - 2^s + 1}{x + 1} \right),\ b(x))$$

$$= ((x^{2^k} - 2^s + 1) \ (x^{2^t} - 2^s + 1),\ b(x)),\ \text{since } (x^{2^s} - 1,\ b(x)) = (x + 1,\ b(x)) = 1,$$

$$= ((x^{2^{k-s}} - 1 + 1)^{2^s} \ (x^{2^{t-s}} - 1 + 1)^{2^s},\ b(x))$$

$$= ((x^{2^{k-s}} - 1 + 1)(x^{2^{t-s}} - 1 + 1),\ b(x)) \neq 1$$

We note that the solution $x_0 \neq 1$ must satisfy two equations:

$$x_0^{2^k} + 2^t - 2^s - 1 = 1 \text{ and } (x_0^{2^{k-s}} - 1 + 1)(x_0^{2^{t-s}} - 1 + 1) = 0$$

This implies that $x_0^{2^{k-s}-1} = 1$ or $x_0^{2^{t-s}-1} = 1$. Let σ be the order of x_0. Then $\sigma | 2^k + 2^t - 2^s - 1$ and $\sigma | 2^{k-s}-1$ or $\sigma | 2^{t-s}-1$.

Then $x_0 \neq 1$ is a solution to P') iff

$$(2^{t-s} - 1,\ 2^k + 2^t - 2^s - 1) \neq 1 \text{ or } (2^{k-s} - 1,\ 2^k + 2^t - 2^s - 1) \neq 1$$

More succinctly, P') has a solution iff

$$((2^{k-s} - 1)(2^{t-s} - 1),\ 2^k + 2^t - 2^s - 1) \neq 1 \qquad (4)$$

Case 2) $t = s$ and $k \geq 2$

According to (2) P') admits a solution iff

$$(x^{2^k-2} + x^{2^k-3} + \ldots + x + 1,\ \frac{x^{2^k-1} + 1}{x + 1}) = (\frac{x^{2^k-1} + 1}{x + 1}) \neq 1$$

Thus for $t = s$, P') always has a solution $x_0 \neq 1$. In fact, all the $(2^k - 1)^{th}$ roots of unity are solutions because $f(x)=(x(x^{2^k-1}+1))^{2^v}$. We note that the condition (4) given in case 1 is also valid in this case, since

$$((2^{k-s}-1)(2^0-1),\ 2^k-1)=(2^{k-s}-1)(0),\ 2^k-1)=(0,\ 2^k-1) = 2^k-1 \neq 1.$$

Q.E.D.

4. AN APPLICATION TO CODING THEORY

We define the set

$$A_n = \{a(x) \mid a(x) \equiv f(x) \pmod{x^n-1};\ f(x) \in GF(q)[x]\}$$

It is well known [3] that A_n is an algebra under the operations sum and convolution product module $x^n - 1$.

A cyclic code of length n is a subspace of A_n which is closed under multiplication by x (modulo $x^n - 1$). It can be shown [3] that a cyclic code is a principal ideal of A_n, call it V_n. Thus, V_n has a generator polynomial $g(x) \in GF(q)[x]$ such that any $v(x) \in V_n$ may be written as $v(x) = r(x)g(x) \pmod{x^n - 1}$, where $r(x) \in GF(q)[x]$. Moreover, $g(x) \mid x^n - 1$.

The number of nonzero coefficients of a code polynomial is called its Hamming weight. The minimum distance, d, of a cyclic code V_n is the minimum Hamming weight among all nonzero polynomials in V_n.

Noise can modify the code polynomial upon transmission, thereby changing the coefficients of the transmitted code polynomial. There is a direct relation between the error correcting power of a cyclic code and its minimum distance. Cyclic codes of distance $d \geq 2t + 1$ can recuperate the transmitted code polynomial if t or less errors occur upon transmission.

In general the minimum distance d of a cyclic code is not known; a lower bound known as the BCH bound [4, 5, 6] can be obtained. In this section we will investigate the minimum distance of a class of binary one-error-correcting codes of length n generated by $g(x) = m_1(x)$, where $m_1(x)$ is the minimum function for α, α a primitive n^{th} root of unity.

Let V_n be a binary cyclic code of length n and minimum distance d generated by $g(x) = m_1(x)$. The BCH bound yields $d \geq 3$ [3]. Suppose $d = 3$. Then there exists a $v(x) \in V_n$ such that the Hamming weight of v(x) is three. Since the code is cyclic we may write

$$v(x) = 1 + x^j + x^i; \quad 0 < j < n, \quad 0 < i < n, \; i \neq j.$$

Since $g(x) = m_1(x)$ and $v(x) = a(x)\, g(x) \pmod{x^n - 1}$ for some $a(x) \in GF(2)[x]$, then $v(x) \in V_n$ if and only if

$$v(\alpha) = 1 + \alpha^j + \alpha^i = 0; \quad 0 < j < n, \quad 0 < i < n, \; i \neq j. \qquad (5)$$

In other words, $d = 3$ if and only if there exist i and j satisfying (5). We simplify (5) to obtain $(1 + \alpha^j)^n = 1$. Thus, we restate the problem as: $d = 3$ if and only if we can find j, $0 < j < n$ such that

$$(1 + \alpha^j)^n = 1 \qquad (6)$$

The next theorem gives necessary and sufficient conditions for the existence of cyclic codes of minimum distance three for $n = 2^k + 2^t - 2^s - 1$. The proof utilizes previously obtained results.

Theorem 3 The binary cyclic code V_n of length $n = 2^k + 2^t - 2^s - 1$, $s \geq 0$, $t \geq s$, $k \geq t$ and $k \geq 2$, generated by $m_1(x)$ has minimum distance $d = 3$ if and only if $((2^{k-s} - 1)(2^{t-s} - 1), 2^k + 2^t - 2^s - 1) \neq 1$.

Proof: An in (6), $d = 3$ iff there exists $0 < j < 2^k + 2^t - 2^s - 1$ such that

$$(1 + \alpha^j)^{2^k + 2^t - 2^s - 1} = 1$$

or

$$(1 + \alpha^j)^{2^k + 2^t} = (1 + \alpha^j)^{2^s + 1}$$

or

$$(\alpha^j)^{2^k} + (\alpha^j)^{2^t} + (\alpha^j)^{2^s} + (\alpha^j) = 0$$

Thus $d = 3$ iff the equation $x^{2^k} + x^{2^t} + x^{2^s} + x = 0$ has a solution $x_0 = \alpha^j$ such that $x_0 \neq 1$ and $x_0^{2^k + 2^t - 2^s - 1} = 1$. In accordance with theorem 2, this solution exists iff

$$((2^{k-s} - 1)\ (2^{t-s} - 1),\ 2^k + 2^t - 2^s - 1) \neq 1$$

Q.E.D.

Table 1 below lists those binary one-error correcting cyclic codes with $n = 2^k + 2^t - 2^s - 1 \leq 127$ ($s \geq 0$, $t \geq s$, $k \geq t$, $k \geq 2$) which have $d = 3$. Notice that if $s = t$, we obtain the Hamming codes [7]. For the case $t = 2$, $s = 1$ we obtain the codes investigated in [8].

Table 1: BINARY CYCLIC CODES WITH d = 3.

k	t	s	n	Nº of Information Digits
2	1	1	3	1
3	1	1	7	4
4	1	1	15	11
5	1	1	31	26
6	1	1	63	57
7	1	1	127	120
3	2	1	9	3
5	2	1	33	23
4	3	1	21	15
4	4	2	22	9
5	3	2	35	23
5	4	1	45	33
6	3	1	69	47
6	4	2	75	55
6	4	1	77	47
6	5	3	87	59
6	5	1	93	78

5. CONCLUSIONS

This investigation characterizes a class of algebraic functions whose solutions are n^{th} roots of unity. The existence of such solutions is verified by calculating the greatest common divisor of polynomials (theorem 1) or integers (theorem 2). The results of theorem 2 are directly applicable to determining which cyclic codes of length n, $n = 2^k + 2^t - 2^s - 1$, have minimum distance three.

Future research can be directed to studying other forms for n, such as $n = 2^k + 2^t + 1$. Another area of interest would be the development of existence conditions similar to theorem 3 for cyclic codes of minimum distance other than three.

REFERENCES

1. E. Artin, Algebraic numbers and algebraic functions (Gordon and Breach, New York, 1967)

2. E. R. Berlekamp, Algebraic coding theory (McGraw-Hill, New York, 1968)

3. W. W. Peterson and E. J. Weldon, Error-correcting codes (2 nd edition, M.I.T. Press, Cambridge, 1972)

4. A. Hocquenghem, Codes correcteurs d'erreurs, Chiffers 2 (1959), 147 - 156.

5. R. C. Bose and D. K. Ray-Chaudhuri, On a class of error correcting binary group codes, Information and Control (1960) 68-79.

6. R. C. Bose and D. K. Ray-Chaudhuri, Further results on error correcting binary group codes, Information and Control (1960) 279 - 290.

7. R. W. Hamming, Error detecting and error correcting codes, Bell System Tech. Journ, (1950) 147 - 160.

8. K. K. Tzeng and C. R. P. Hartmann, On the minimum distance of certain reversible cyclic codes, IEEE Trans. Information Theory IT 16 (1970) 644 - 646.