A Theorem for Computing Primitive Elements in the Field of Complex Integers of a Characteristic Mersenne Prime

R. L. MILLER, I. S. REED, AND T. K. TRUONG

Abstract—A method developed previously [6] for computing primitive elements in \( GF(q^2) \), where \( q \) is a Mersenne prime, is shown not to generalize to other Galois fields. The method will be successful in finding primitive elements of \( GF(q^n) \) if and only if \( q \) is a Mersenne prime and \( n = 2 \).

Implementation Issues

The algorithm's computation time to obtain one value of the cumulative distribution depends linearly on the Index \( N \), in contrast to a \( N^2 \) dependence of one published previously by Carter [3]. On the TI-59 calculator, 2 min are required for \( N = 32 \). When \( E = \gamma^2 = 1 \), (3) is indeterminate and so is the algorithm. Otherwise, the method is stable and accurate. For large \( N \), an implementation of the algorithm will encounter dynamic range problems. For such large \( N \), the linearity of the relations (5) and (6) permits an obvious method of scaling.

References


A Theorem for Computing Primitive Elements in the Field of Complex Integers of a Characteristic Mersenne Prime

R. L. MILLER, I. S. REED, AND T. K. TRUONG

Abstract—A method developed previously [6] for computing primitive elements in \( GF(q^2) \), where \( q \) is a Mersenne prime, is shown not to generalize to other Galois fields. The method will be successful in finding primitive elements of \( GF(q^n) \) if and only if \( q \) is a Mersenne prime and \( n = 2 \).

Introduction

Pollard [1] proposed the use of the fast Fourier transform (FFT) over finite fields or rings to compute circular convolutions. In [3], the authors extended the integer transforms of Rader [2] by defining a complex number-theoretic transform over the Galois field \( GF(q) \), where \( q = 2^p - 1 \) is a Mersenne prime for \( p = 2, 3, 5, 7, 13, 17, 19, 31, \ldots \). Recently, the authors in [4] developed a mixed-radix transform of \( 2^k \cdot p \) points over \( GF(q^2) \), where \( 3 < k < p + 1 \). Such an algorithm for \( GF(q^2) \) appears comparable in speed to that given by Winograd [5]. The algorithm stated in [4] for finding a primitive element of \( GF(q^2) \) was incorrect. In order to make this correction, the authors [6]-[8] presented a new method for finding primitive elements of \( GF(q^2) \). In this paper, a theorem is developed to show that this new method can be used to find primitive elements of a finite field \( GF(q^n) \) if and only if \( q \) is a Mersenne prime and \( n = 2 \).

A Theorem for Finding Primitive Elements in \( GF(q^n) \) where \( q \) is a Mersenne Prime

Before developing the theorem, the following observations and lemma are needed.

Let \( p(z) \) be an irreducible polynomial over \( GF(q) \), where \( q \) is a prime power, and let \( GF(q^n) \) be its splitting field over \( GF(q) \). Let \( a \) be the automorphism \( \sigma(a) = a^q \) of \( GF(q^n) \) that leaves every element of \( GF(q) \) fixed. Then the Galois group of \( p(z) \), denoted by \( GGF(q^n), GGF(q) \), is the cyclic group of \( n \) elements with generator \( \sigma \). That is,

\[
GGF(q^n), GGF(q) = \{ a^q, a^q^2, \ldots, a^q^{n-1} \}.
\]

The norm \( N(x) \) of \( x \in GF(q^n) \) is given by

\[
N(x) = x^{q^n} = x^{q^{(q-1)/(q-1)}} = x^{(q^n-1)/(q-1)}.
\]

Lemma: Denote the nonzero elements of \( GF(q^n) \) by \( GF*(q^n) \). These form a cyclic group of \( q^n - 1 \) elements. If \( a \in GF(q^n) \), then there exists \( x \in GF(q^n) \) such that \( N(x) = a \).

Proof: Since \( N(0) = 0 \), we may assume \( a \neq 0 \). Thus, \( a \) is a primitive \( d \)th root of unity for some \( d | q - 1 \). Let \( \gamma \) be a generator of \( GF*(q^n) \). Since both \( \gamma \) and \( \gamma^{(q^n-1)/d} \) are primitive \( d \)th roots of 1, it follows that there exists a positive integer \( k \) such that \( (k, d) = 1 \) and \( a = \gamma^{(q^n-1)/(q-1) \cdot (q-1)} \cdot k \). Thus,

\[
a = \gamma^{(q^n-1)/d} \cdot k^{(q^n-1)/(q-1)} = N(\gamma^{(q-1)/d} \cdot k).
\]

Theorem: Let \( x \in GF*(q^n) \). Then \( N(x) = GF*(q^n) \Rightarrow x = GF*(q^n) \) if and only if \( n = 2 \) and \( q = 2P - 1 \), a Mersenne prime.

Proof: Let \( \gamma \) be a primitive element of \( GF(q^n) \). By the lemma we may assume that there exists \( x \in GF*(q^n) \) such that \( \langle N(x) = GF*(q^n) \rangle = \langle N(\gamma) = GF*(q^n) \rangle \), where \( x = \gamma^{m_{\gamma}} \), \( m_{\gamma} = q^n - 1 \) and \( k, q^n - 1 = 1 \). Clearly, \( N(x) = \gamma^{m_{\gamma} m_{\gamma} (q^n-1)/(q-1)} \) is a generator of \( GF*(q^n) \) if and only if \( m_{\gamma} \). But also, \( x = \gamma^{m_{\gamma} m_{\gamma}} \) where \( m_{\gamma} \) generates \( GF*(q^n) \) if and only if \( m_{\gamma} \). Thus, to prove the theorem one needs to find values of \( q \) and \( n \) such that if \( m_{\gamma} \), \( q = 2P - 1 \), then \( m_{\gamma} \) is a solution to the Diophantine equation \( 2^k - 1 = \alpha^m - 1 \) of prime factors.

By the last corollary in [9], Dickson showed that \( x^n - 1 \) always has a prime factor not dividing \( x^m - 1 \) for all \( m < n \), unless \( n = 2 \) and \( x = 2^{x-1} \), or \( n = 6 \) and \( x = 2 \). Thus, \( q^n - 1 \) and \( q - 1 \) have the same set of prime factors if and only if \( n = 2 \) and \( q = 2P - 1 \). It is not difficult to show that there are no solutions to the Diophantine equation \( 2^k - 1 = \alpha^m \) for \( m > 1 \). (Indeed, if \( m \) is even, then reducing modulo 4 yields a contradiction; if \( m \) is odd, then \( 2^k = (a^m - 1)/(a^m - 1) \)
...+1), a contradiction, since $a$ is also odd.) Thus, since $q$ is the cardinality of the ground field (and must, therefore, be a prime power), it follows that $q = 2^p - 1$ is a Mersenne prime. This completes the proof of the theorem.

Consider now an example of the above theorem for finding a primitive element of $GF(q^2)$.

Example: If $q = 2^p - 1$ is a Mersenne prime, then the polynomial $x^2 + 1$ is irreducible over $GF(q)$. Hence, $GF(q^2) = \{a + b\hat{\imath}, a, b \in GF(q)\}, \hat{\imath}^2 = -1$. For any $x = a + \hat{\imath}b \in GF(q^2)$, $N(x) = (a + \hat{\imath}b)(a - \hat{\imath}b) = a^2 + b^2 = c$. If $(\hat{\imath}) = GF^*(q)$, then by the theorem, $(a + \hat{\imath}b) = GF^*(q^2)$. This is the same result described in [6]. The primitive element $c$ of $GF(q)$ can be obtained by using the theorem in [1]. Using the same procedure for finding the solutions of $[3, eq. (12)]$, one can find the solutions of $a^2 + b^2 = c \mod q$ for $a$ and $b$.

REFERENCES


Invariance of Distribution of Coherence Estimate to Second-Channel Statistics

A. H. NUTTALL

Abstract—When one of the two channels used in a coherence estimator contains only zero-mean stationary Gaussian noise, the probability distribution of the magnitude-squared-coherence estimate is utterly independent of the distribution in the other channel when the random variables in the two channels are statistically independent of each other. Thus, proper threshold settings for specified false alarm probabilities in a coherence-detector can be realized under complete ignorance of the statistics of the non-Gaussian channel.

INTRODUCTION

Detection of the presence of a common signal in two channels is sometimes accomplished by computing the magnitude-squared-coherence (MSC) and comparing the estimate with a threshold to decide whether a signal is present or absent [1].

One advantageous feature of such an approach is that the false alarm probability is independent of the noise level in the two channels, although it does depend on the number of pieces $N$ used in the coherence estimate. With unknown noise levels, this enables selection of threshold levels for prescribed false alarm probability.

The probability distribution of the MSC estimate was derived in [2] for the true coherence values anywhere in the range [0, 1], and for Gaussian processes in the two channels. In particular, for a true coherence value of zero, this corresponds to independent zero-mean Gaussian processes in the two channels. Recently, it has been shown [3] that if one of the two channels contains only Gaussian noise and the other contains a pure tone, then the distribution of the MSC estimate is identical to the Gauss-Gauss channels case. We will now generalize this conclusion to the following: if one channel contains only zero-mean stationary Gaussian noise, then for any number of pieces $N$, the probability distribution of the MSC estimate is utterly independent of:

1) the distribution of the samples in the other channel if this latter channel process is random and statistically independent of the Gaussian channel; or
2) the particular sample values in the other channel if this latter channel process is deterministic.

Thus, for a true coherence of zero, the MSC estimator is very robust with respect to the behavior of the non-Gaussian channel.

TECHNICAL CONSIDERATIONS

For the sake of brevity, we assume the reader to be familiar with the background and notation of [2]. At one particular frequency of interest, let the complex Fourier coefficients be represented by the random variables (RV)'s

\begin{align}
\{u_n + iv_n\}^N_{n=1} \quad &\text{in channel 1,} \\
\{u_n + iv_n\}^N_{n=1} \quad &\text{in channel 2,}
\end{align}

where $\{u_n\}^N_{n=1}$ and $\{v_n\}^N_{n=1}$ are real zero-mean unit-variance\(^1\) independent Gaussian random variables (ZM UV IG RV’s). We will specify nothing about the behavior of the RV’s in (2), except to say that, if random, they are statistically independent of the RV’s in (1). Thus, we are concentrating solely on the zero-coherence case.

The MSC estimate available from $N$ pieces of data is given by [2]

\begin{align}
s = \frac{1}{N} \sum_{n=1}^{N} \left| u_n + iv_n \right|^2, \quad N \geq 2.
\end{align}

We will evaluate the statistics of $\hat{s}$, holding $\{u_n + iv_n\}^N_{n=1}$ fixed; that is, we evaluate the conditional probability distribution of $\hat{s}$. We show that this conditional distribution is completely independent of the particular values of $\{u_n + iv_n\}^N_{n=1}$. Thus, even before we get around to performing the average of the conditional distribution with respect to the probability distribution of $\{u_n + iv_n\}^N_{n=1}$, the dependence on RV’s (2) has disappeared. Thus, whether we average (channel 2 random) or not (channel 2 deterministic), the same probability distribution results for $\hat{s}$, and it is identical to that given in [2] and [3].

Let

\begin{align}
u_n + iv_n = m_n e^{i \theta_n} \quad \text{for } 1 \leq n \leq N
\end{align}

\(^1\)This could be relaxed to any common variance value; the absolute scale cancels out in the MSC estimate in (3).