A Note on Structure of $F_2^n$ with respect to Trace of its Elements

R. K. Sharma, Wagish Shukla, S. Ramasamy

Abstract-- A structure of $F_2^n$ is depicted. A relation (Equivalence relation) on the positions of $g(1:n-1)=(\text{Tr}(\beta), \text{Tr}(\beta^2), \text{Tr}(\beta^3), \ldots, \text{Tr}(\beta^{n-1}))$ is defined and a formula is derived to find the number of classes of length $i$ for a given $i$ with $1 \leq i \leq n-1$ where $m$ is the largest positive integer such that $2^m \leq n$ and it is used to find the cardinal number of the set of binary trace sequences of the type $g(1:n-1)$ of length $n-1$. Two new results on traces of the elements of a polynomial basis of $F_2^n$ over $F_2$ are proved.

I. Introduction

Irreducible polynomial: A polynomial $p(x)$ in $F[x]$ is said to be irreducible over the field $F$ if $p(x)$ has positive degree and $p(x) = f(x)g(x)$ with $f(x)$, $g(x)$ $\in F[x]$ implies that either $f(x)$ or $g(x)$ is a constant polynomial.

Trace: Let $K=F_2$ and $F=F_2^n$. For $\beta$ in $F$, the trace $\text{Tr}_{F/K}(\beta)$ of $\beta$ is defined as $\text{Tr}_{F/K}(\beta) = \beta + \beta^q + \beta^{q^2} + \cdots + \beta^{q^{n-1}}$. The trace of a monic irreducible polynomial $f(x)$ is the coefficient of $x^n$ in $f$. If $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ then the trace of $f(x)$ is $c_0$.

Polynomial basis: If $\alpha$ is a root of an irreducible polynomial then $\{1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{n-1}\}$ is called a polynomial basis of $F_2^n$ over $F_2$ with respect to $\alpha$.

Primitive element: Generator of the cyclic group $F_q^*$ is called a primitive element of $F_q$.

II. Structure of $F_2^n$ with respect to traces of its Elements

The following array gives a structure of the non-zero elements of $F_2^n$ in terms of their traces over $F_2^n$. For any fixed primitive element $\alpha$ of $F_2^n$, consider the following array.

$$
\begin{array}{cccccccccccc}
\alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\
\alpha^{15} & \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \\
\end{array}
$$

Fig. 1: Distribution of elements of $F_2^n$.

Every $i^{th}$ row has $2^{i-1}$ elements for $1 \leq i \leq n$. New columns introduced in every $i^{th}$ row have $n-i+1$ elements (including $n-i$ elements below them) for $1 \leq i \leq n$. The above array contains all the $2^n-1$ non-zero elements of $F_2^n$ with all elements in each column having the same trace.

This concept can be extended to any finite field of odd characteristic as well. The following theorem shows that trace-one and trace-zero elements are equally distributed in $F_2^n$.

A. Theorem

Number of trace 1 elements is equal to number of trace 0 elements in $F_2^n$ over $F_2^n$.

Proof:

Let $N_0$ and $N_1$ denote the number of trace 0 and 1 elements respectively.

Every element of $F_2^n$ satisfies either

$$
\begin{align*}
x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}} &= 0 \quad (1) \\
x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}} &= 1 \quad (2)
\end{align*}
$$

but not both. (1) has at most $2^{n-1}$ roots in $F_2^n$ and so $N_0 \leq 2^{n-1}$.

Similarly, $N_1 \leq 2^{n-1}$.

Since $\text{Tr}: F_2^n \rightarrow F_2$ is an onto function, both 0 and 1 have pre-images in $F_2^n$ and so

$$
N_0 + N_1 = 2^n \quad \text{................. (3)}
$$

Therefore, $N_0 = 2^{n-1}$ and $N_1 = 2^{n-1}$.

B. Theorem [2]

If $\alpha$ and $\beta$ are non-zero elements of $F_q$ then $N_\alpha(n, q) = N_\beta(n, q)$ where $N_\alpha(n, q)$ denotes the number of monic irreducible polynomials over $F_q$ of degree $n$, having trace $\alpha$.

Notation: Let $\vec{a}(1: j) = (a_1, a_2, a_3, \ldots, a_j)$ denote any binary sequence of length $j$ beginning with position 1 and ending with position $j$. For any element $\beta$ in $F_2^n$, let $\beta', \beta^2', \ldots, \beta^{n-1}'$ and $\text{Tr}(\beta), \text{Tr}(\beta^2), \ldots, \text{Tr}(\beta^{n-1})$ respectively denote the sequence and binary trace sequence of $\beta$ of length $n-1$.

Equivalence class: Let $i, j \in N$. ‘$i$’ is said to be related to ‘$j$’ (or $\beta$ is related to $\beta'$) if $j = 2^k \times i$ for some integer $k$. 

R.K.Sharma, Wagish Shukla, and S.Ramasamy are with the Department of Mathematics, IIT Delhi, New Delhi-110016, India.
This is an equivalence relation. (Elements in) $i^{th}$ and $j^{th}$ positions of a binary sequence are in the same class iff $j = 2^k \times i$ for some integer $k$ and hence the elements in the same class have the same trace.

**Length of a class** Let $\{1:n\} = (a_1, a_2, a_3, \ldots a_n)$ be any binary trace sequence of length $n$. Then $l$ is called length of a class beginning with position $2i - 1$ for $i \geq 1$ if $l$ is the largest positive integer such that $(2i-1)2^{l-1} \leq n$.

Since the positions in the same class always have the same trace value, each class can be considered as a single position for the purpose of calculation of total number of binary trace sequences.

**Notation** For any set $X$, let $|X|$ denote its cardinal number. Let $X(m)$ denote the set of classes of length $i$ in $\{1:n\}$ if $n = 2^m$. Let $X(m')$ denote the set of classes of length $i$ in $\{1:n\}$ if $n = 2^m + 1$. Let $|X(m)|$ and $|X(m')|$ denote the total number of classes in $\{1,n-1\}$ and $\{2^m + 1, 1\}$ respectively.

**C. Theorem**

If $n = 2^m$ for some positive integer $m$, the total number of $(n-1)$-binary trace sequences of all the elements of $F_2^n$ is $2^{n/2}$.

**Proof**

For any suffix $k$ of $a_k$ with $1 \leq k \leq n$, let $X_{k}(m)$ denote equivalence class of length $i$ containing the position $k$.

Since $|X_{m}(m)| + |X_{m+1}(m)| = 1$, total number of classes is

$$|X_{m}(m)| + |X_{m+1}(m)| + \ldots + |X_{n-3}(m)| + |X_{n-2}(m)| + |X_{n-1}(m)| + |X_{n}(m)| + |X_{n+1}(m)|$$

$$= 2^{m-2} + 2^{m-3} + 2^{m-4} + 2^{m-5} + \ldots + 2^{m-1} + 2^1 + 2^0 + 1$$

$$= 2^{m-1} - 1$$

Therefore, total number of $(n-1)$-binary trace sequences is $2^{n/2}$.

**D. Theorem**

$$|X(m)| = |X(m')|$$

**Proof**

From the proof of the above theorem(2.3), it is seen that

$$|X_{m}(m)| = |X_{m}(m')|$$

for $i = 1$ to $m-1$.

$$|X_{m}(m)| = 1$$ and $$|X_{m+1}(m)| = 0$$

$$|X_{m}(m')| = 0$$ and $$|X_{m+1}(m')| = 1$$

$$|X(m)| = |X_{m}(m)| + |X_{m+1}(m)|$$

$$|X_{m}(m')| + |X_{m+1}(m')|$$

since $|X_{m}(m)| + |X_{m+1}(m)| = |X_{m+1}(m')| + |X_{m}(m')|$

$$= |X(m')|$$

This completes the proof of the theorem.

When $2^n + 1 \leq n \leq 2^{n+1}$, let $n = n_0 + R$ where $n_0 = 2^n$.

Let $X(m), X'$ and $X''$ denote the set of all classes of length $i$ and let $X(m), X'$ and $X''$ denote the set of all classes in $[1, 2^m-1], [1, 2^m + R-1]$ and $[1, 2n-1]$ respectively.

For a real number $s \geq 0$, let $[s]$ denote the integral part of the real number $s$.

**E. Theorem**

(i) For $1 \leq i \leq m - 1$, $|X_i'| = |X_i(m)| + [(R + 1)/2] - [(R + 1)/2] + 1$ for $1 \leq R \leq 2^m$.

(ii) For $m \leq i \leq m + 1$, $|X_i'| = |X_i(m')| + [(R + 1)/2] - [(R + 1)/2] + 1$ for $1 \leq R \leq 2^m$.

**Proof**

Since for every step of $2^i$ with $1 \leq i \leq m - 1$ in $R$ beginning with $2^m + 1$, an equivalence class of length $i$ will be increased in the total of $|X_i(m)|$ for $X'$ and for every step of $2^i$ beginning with $2^m + 2^i$, an equivalence class of length $i$ will be reduced from $X_i(m)$ for $X''$, the result (i) follows. Result (ii) can be proved by similar argument with $|X_i(m')|$ in place of $|X_i(m)|$.

**III. TRACES AND COEFFICIENTS OF IRREDUCIBLE POLYNOMIALS**

**A. Some Preliminary Remarks [3]**

Let $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + 1$ be an irreducible polynomial of degree $n$ over $F_2$, and let $\alpha$ be a root of $f(x)$ in $F_2[x]/(f)$. The roots of $f(x)$ in $F_2^n$ are precisely $x = \alpha^2$ for $0 \leq i \leq n-1$ and $f(x) = \Pi(x-x_i)$ where the product runs from $i = 0$ to $n-1$.

Let $s_k = \Sigma x_i^k$ where the sum runs through $i = 0$ to $n-1$ then $s_k = \text{Tr}(\alpha^k)$ for $0 \leq k \leq n-1$.

Omran Ahmadi and Alfred Menezes[3] have proved the following result:

**B. Theorem [3]**

Let $f(x) = x^n + x^{n-m(1)} + x^{n-m(2)} + \ldots + x^{n-m(l)} + 1$ be an irreducible polynomial over $F_2$ with $m(l) > m(l-1) > m(l-2) > \ldots > m(2) > m(1) > n/2$, and let $\alpha$ be a root of $f(x)$ in $F_2^n = F_2[x]/(f)$.

Then for $0 \leq k \leq n-1$, we have $s_k = n \bmod 2$ if $k = 0$ and let $\bmod 2$ if $k \in \{m(1), m(2), \ldots, m(l)\}$.

**C. Our contributions on traces**

**1. Theorem**

Let $f(x) = x^n + x^{n-m(1)} + x^{n-m(2)} + \ldots + x^{n-m(l)} + 1$ be an irreducible polynomial over $F_2$ with $m(0) = 0 < m(1) < \ldots < m(l)$. Theorem 2.3 has been proved by

Proof: The proof is by induction on \( k \).

By Newton\(\text{o}\)s formula,
\[ s_k = s_{k-1}a_1 + s_{k-2}a_2 + \ldots + s_1a_{k-1} + ka_k \]

When \( k = 0 \),
\[ s_k = 1 + \ldots + 1(n\text{ times}) \equiv n \mod 2 \]
When \( 0 < k < m(1) \), \( s_k = 0 \) since \( a_u = 0 \) for all \( u < m(1) \).

When \( k = m(1) \),
\[ s_k = s_{k-m(1)} \equiv 1 \mod 2 \]
When \( k < m(1) \), \( s_k = 0 \).

Take \( i = t = 1 \).

If \( k \) is not divisible by \( m(t-1) \), then
\[ s_k = s_{k-m(t-1)} \equiv 1 \mod 2 \]

Now \( k \) can be either \( k = m(t) \) or \( m(t) < k < m(t+1) \).

Therefore, \( s_k \equiv 0 \mod 2 \) for all positive integers \( r < k \).

When \( k = m(t) \),
\[ s_k = s_{k-m(t)} + s_{k-m(t-1)} + \ldots + s_1a_{k-m(t-1)} + ka_k \]

This implies that \( s_k = s_{k-m(t)} \equiv 1 \mod 2 \).

If \( k < m(t) \), then
\[ s_{k-m(t)} = s_{k-m(t-1)} = \ldots = s_{k-m(1)} \]

Therefore, by induction hypothesis, \( s_{k-m(t)} \equiv 0 \) for all \( i < t \).

Therefore, \( (4) \) becomes \( s_k = s_{k-m(t)} \).

Similarly, by the same argument, when \( k < m(t+1) \), \( s_k \equiv 0 \mod 2 \).

Proof of the theorem is complete.
REFERENCES


R.K.Sharma, Wagish Shukla, and S.Ramasamy are with the Department of Mathematics, IIT Delhi, New Delhi-110016, India