Trace representation

The trace representation plays an important role in sequence theory, and is also used for defining and studying Boolean functions. In the theory of finite fields, the trace function on the finite field $\mathbb{F}_{p^n}$ is the function $Tr: \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ defined by $Tr(x) = x + x^p + x^{p^2} + x^{p^3} + \ldots + x^{p^{n-1}}$. Here we are considering the case when $p = 2$, that is, when our finite field is the binary field $\mathbb{F}_2^n$. So our trace is a function $Tr: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$. Define the function $Tr(\sum_{i=0}^{k} a_{i}t^{i} + b_{i})$ on $\mathbb{F}_2^n$ for $0 \leq t \leq 2^n - 2$ and integers $a, b$. Let $p(x)$ be a primitive polynomial over $\mathbb{F}_2^n$. Then $x$ can generate $\mathbb{F}_2^n$, i.e., $x^t$ where $0 \leq t \leq 2^n - 2$ are all nonzero elements of $\mathbb{F}_2^n$. From the theory of finite fields, we know that each element in $\mathbb{F}_2^n$ can be represented by a binary string of length $n$, and we also know that $\mathbb{F}_2^n$ consists of all the possible binary strings of length $n$. This means that, for each value of $x^t$, we have a corresponding binary string. By evaluating $Tr(\sum_{i=0}^{k} a_{i}t^{i} + b_{i})$ for $0 \leq t \leq 2^n - 2$, we obtain $2^n - 1$ binary values.

Now, for each $t$, let $Tr(\sum_{i=0}^{k} x^{a_{i}t^{i} + b_{i}})$ be an element in the truth table at the position corresponding to the decimal representation of the binary string corresponding to the element $x^t$. Now, if we set a value at position $0$, we will have a complete truth table. This value can be either true or false, but by convention we set it as false. The general form of the trace function we are dealing with is $Tr(\sum_{i=0}^{k} x^{a_{i}t^{i} + b_{i}})$. There is a restriction on the values of $b_1, b_2, b_3, \ldots, b_k$ depending on $a_1, a_2, a_3, \ldots, a_k$ respectively. To validate $b_i$, where $1 \leq i \leq k$ we do the following steps:

1. Compute $v = \gcd(2^n - 1, a_i)$.
2. Compute $u = (2^n - 1)/v$.
3. Find the smallest number $r$ such that $u$ divides $2^r - 1$.
4. Compute $e = (2^n - 1)/(2^r - 1)$.
5. If $x^b \in \{0, x^e, x^{2e}, \ldots, x^{(2^r-1)e}\}$, then $b_i$ is valid.

Since the trace function is linear then $Tr(\sum_{i=0}^{k} x^{a_{i}t^{i} + b_{i}}) = \sum_{i=0}^{k} Tr(x^{a_{i}t^{i} + b_{i}})$. After validating $b_i$ and $a_i$, we consider computing the trace function over the finite field $\mathbb{F}_{2^r}$ rather than $\mathbb{F}_2^n$, where $r$ is as noted above.

Let us take an example to explain how to convert a trace representation to a truth table representation. Suppose we have a Boolean function represented by $Tr(x^{3t^2})$ with a primitive polynomial $p(x) = x^3 + x + 1$ on the
finite field $F_{2^3}$. The finite field $F_{2^3}$ indicates that the Boolean function represented by $Tr(x^{3t+2})$ is a 3 variable Boolean function. Computing $Tr(x^{3t+2})$ for $0 \leq t \leq 2^3 - 2 = 6$, gives us the following table,

$$\begin{array}{|c|c|c|c|}
\hline
\alpha & x_0 & x_1 & x_2 & Tr(\alpha) \\
\hline
1 & 0 & 0 & 1 & 0 \\
x & 0 & 1 & 0 & 1 \\
x^2 & 1 & 0 & 0 & 0 \\
x^3 & 0 & 1 & 1 & 0 \\
x^4 & 1 & 1 & 0 & 1 \\
x^5 & 1 & 1 & 1 & 1 \\
x^6 & 1 & 0 & 1 & 1 \\
\hline
\end{array}$$

Table 1: Trace computation

Permuting the table to be in a lexicographical order and adding the all zero row, we get the following truth table

$$\begin{array}{|c|c|c|c|}
\hline
\alpha & x_0 & x_1 & x_2 & Tr(\alpha) \\
\hline
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 \\
x & 0 & 1 & 0 & 1 \\
x^3 & 0 & 1 & 1 & 0 \\
x^2 & 1 & 0 & 0 & 0 \\
x^6 & 1 & 0 & 1 & 1 \\
x^4 & 1 & 1 & 0 & 1 \\
x^5 & 1 & 1 & 1 & 1 \\
\hline
\end{array}$$

Table 2: Truth table representation of $Tr(x^{3t+2})$

Let us see how the trace representation can be obtained from the truth table of a Boolean function. By ordering the truth table according to the generator of the finite field $F_{2^n}$ and removing the all zeros entry we get a binary vector of length $2^n - 1$. Using the inverse of the Galois discrete Fourier transform on this binary vector, we get a vector $V$, with entries in finite field $F_{2^n}$. This vector has properties that lead us to deduce the trace function. Let $c_i$ be the coset leader of the cyclotomic coset $i$ of $F_{2^n}$, where $1 \leq c_i \leq 2^n - 2$. If the entry at position $c_i$ in the vector $V$ is nonzero
then all the entries at the positions corresponding to the elements of coset $i$ should be nonzero. If $x^j$ is an entry in the vector $V$ at position $c_i$, then the corresponding trace formula is $Tr(x^{c_i+j})$. Thus for each coset leader, we have a corresponding trace formula. So we see that the number of trace formulas depends on the number of nonzero elements of the vector $V$. The sum of these trace formulas is the trace function corresponding to the TT of the Boolean function. To do this transformation we multiply our vector by the Inverse Galois Discrete Fourier Transform (IGDFT) matrix which is an $2^n-1 \times 2^n-1$ matrix,

$$
\begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \alpha^1 & \alpha^2 & \cdots & \alpha^{2^n-1} \\
1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2^{n-1}} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha^{2^{n-1}} & \alpha^{2^{n-2}} & \cdots & \alpha^{2^n-1}
\end{bmatrix}
$$

where $\alpha = x^{2^n-2}$ and $x$ is a generator of $F_{2^n}$ according to some primitive polynomial $p(x)$ in $F_{2^n}$.

**The following example demonstrates how to convert a truth table Boolean function to a trace Boolean function.** Consider the Boolean function represented by Table 2. By permuting Table 2 back to the table on Table 1 and removing the all zeros entry, we get the following binary vector $[0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1]$. Now we want the trace function of this binary vector. Computing the inverse discrete Fourier transform on this vector gives us a vector with entries in $F_2^3$. To compute this transform we multiply our vector by the following matrix:

$$
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\
1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\
1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\
1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\
1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^4 & \alpha^2 \\
1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha & \alpha^2
\end{bmatrix}
$$

where $\alpha = x^6$ and $x^3 = x+1$ according to our primitive polynomial $p(x) = x^3 + x + 1$. This transformation gives us the following vector $[0 \ 0 \ 0 \ x^2 \ 0 \ x \ x^4]$. Now, we have nonzero elements at positions 3, 5 and 6. These positions
are the elements of a cyclotomic coset in $F_2^3$. We see that 3 is the coset leader, so $a_1 = c_1 = 3$. We also see that $x^2$ is the element at index $c_2$, so $b_1 = 2$. Therefore, our trace formula is $Tr(x^{3t+2})$. Since 3, 5 and 6 are the only nonzero positions then there is only one trace formula. Suppose that we get the following vector $[0 \ x^4 \ x \ x^2 \ x^2 \ x \ x^4]$ in some transformation. The nonzero elements give us the following cyclotomic cosets in $F_2^3$. We see that we have two cyclotomic cosets, $\{1, 2, 4\}$ and $\{3, 5, 6\}$. They give us two trace formulas, $Tr(x^{t+4})$ and $Tr(x^{3t+2})$. The sum of them, $Tr(x^{t+4}) + Tr(x^{3t+2})$, gives us the corresponding trace function.