1 Bent Functions

Bent functions were originally defined in a paper by Rothaus in the Journal of Combinatorial Theory in 1976 [17]. These functions are useful for cryptographic applications because they are *perfectly nonlinear* which makes them resistant to differential attacks. The original defintion of the *bent function* is presented.

First, the discrete Fourier transform should be understood.

The Fourier transform of a function has many applications in signals analysis. The idea is to express a given signal as a function of frequency to reveal the dominant frequencies in the signal. Today, digital signals have taken over analog. This fact has made the discrete Fourier transform much more applicaple to modern communication systems. The DFTs of n-variable pseudo Boolean functions are studied here.

The following discussion on DFTs will follow [**?**]. The domain of all n-variable pseudo Boolean functions is $\mathbb{F}_2^n$. The goal is to find a Fourier transform on $\mathbb{F}_2^n$ and for that we need the characters of $\mathbb{F}_2^n$.

Definition 1.1. [**?**] A *character* χ of a finite abelian group G is a group homomorphism from G into the multiplicative group $\{e^{frac2\pi\imath k|G|} : k \in \mathbb{Z}\}$ of complex number of norm 1.

For the purposes of this paper, it should be clear that $(-1)^{\lambda\cdot x}$ for $\lambda, x \in \mathbb{F}_2^n$ is a *group character* of $\mathbb{F}_2^n$ for each $\lambda \in \mathbb{F}_2^n$. Define the *dual group* $\hat{\mathbb{F}_2^n}$ to be the set of all character of G. The group operation in $\hat{\mathbb{F}_2^n}$ is pointwise multiplication of functions. This means that

$$\hat{\mathbb{F}_2^n} = \{\chi \in \mathbb{F}_2^n : \chi \text{ is a character of } \mathbb{F}_2^n\},$$

with $\chi\psi(x) = \chi(x)\psi(x)$, for all $x \in \mathbb{F}_2^n$.

By identifying each λ with $(-1)^{\lambda\cdot x}$, it is easily seen that $\mathbb{F}_2^n$ is a subgroup of $\hat{\mathbb{F}_2^n}$. Indeed,

$$(-1)^{(\lambda_1+\lambda_2)\cdot x} = (-1)^{\lambda_1\cdot x}(-1)^{\lambda_2\cdot x}.$$

The isomorphism $\mathbb{F}_2^n \cong \hat{\mathbb{F}_2^n}$ is shown by constructing a one-to-one and onto mapping $\Upsilon : \mathbb{F}_2^n \to \hat{\mathbb{F}_2^n}$ where $\Upsilon(\lambda) = (-1)^{\lambda\cdot x}$.

Proof. Let $\Upsilon(\lambda_1) = \Upsilon(\lambda_2)$. Then

$$\begin{aligned}(-1)^{\lambda_1\cdot x} &= (-1)^{\lambda_2\cdot x} \\ &= (-1)^{(\lambda_1+\lambda_1+\lambda_2)\cdot x} \\ &= (-1)^{\lambda_1\cdot x}(-1)^{(\lambda_1+\lambda_2)\cdot x}.\end{aligned}$$

Thus, $(\lambda_1 + \lambda_2)\cdot x = 0$ for all $x \in \mathbb{F}_2^n$, which implies $\lambda_1 + \lambda_2 = 0 \Rightarrow \lambda_1 = \lambda_2$. Therefore, Υ is one-to-one.

Add part of Υ being onto...
Finally, $\mathbb{F}_2^n \cong \hat{\mathbb{F}_2^n}$. □

If $f(x) \in \mathcal{BF}_n$, so $(-1)^{f(x)}$ is well defined, then by the theory of discrete Fourier transforms

$$(-1)^{f(x)} = \frac{1}{2^{n/2}} \sum_{\lambda \in \mathbb{F}_2^n} c(\lambda)(-1)^{\lambda \cdot x} \tag{1}$$

Where the $c(\lambda)$, the *Fourier coefficients* of $(-1)^{f(x)}$ are given by

$$c(\lambda) = \frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)}(-1)^{\lambda \cdot x}.$$

As observed by Rothaus, $2^{n/2}c(\lambda)$ is the number of zeros minus the number of ones of the function $f(x) + \lambda \cdot x$. It is clear that when there are more zeros than ones $c(\lambda) > 0$ and when there are more ones than zeros $c(\lambda) < 0$. Counting the number of zeros in $f(x)$ is also easily seen. Consider the zero Fourier coefficient $c(0)$:

$$\begin{aligned} c(0) &= \frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} \\ &= \frac{1}{2^{n/2}} \text{ number of zeros of } f(x) - \text{ number of ones of } f(x). \end{aligned}$$

Since $2^n =$ number of zeros of $f(x)+$ number of ones of $f(x)$,

$$\begin{aligned} \text{number of zeros of } f(x) &= \frac{2^{n/2}c(0) + 2^n}{2} \\ &= 2^{n/2-1}c(0) + 2^{n-1}. \end{aligned}$$

Definition 1.2. If all of the Fourier coefficients of $(-1)^{f(x)}$ are ± 1 then $f(x)$ is a *bent function.*

There are two immediate observations for any bent function $f(x)$ on $\mathbb{F}_2^n$. First, n must be even because $2^{n/2}c(\lambda)$ is an integer. Second, the Hamming weight of $f(x)$ equals $2^{n-1} \pm 2^{n/2-1}c(0)$. There also is a bound on the degree of the polynomial of $f(x)$ proved by Rothaus. The theorem and proof are presented here.

Theorem 1.1. *If $f(x)$ is a bent function on $\mathbb{F}_2^n$, then n is even, $n = 2k$; the degree of $f(x)$ is at most k, except in the case $k = 1$.*

Proof. □

That n is even has already been observed.

Let $n = 2k$ with $k > 1$, and let $r > k$. Consider the polynomial $f(x_1, x_2, \ldots, x_r, 0, 0, \ldots, 0) = g(x_1, x_2, \ldots, x_r)$. Then by equation 1,

$$(-1)^{g(x)} = \frac{1}{2^{r/2}} \sum_{\lambda_1, \lambda_2, \ldots, \lambda_r = 0,1} b(\lambda_1, \ldots, \lambda_r)(-1)^{\lambda_1 x_1 + \cdots + \lambda_r x_r}$$

and

$$(-1)^{f(x)} = \frac{1}{2^{n/2}} \sum_{\lambda_1,\lambda_2,\ldots,\lambda_n=0,1} c(\lambda_1,\ldots,\lambda_n)(-1)^{\lambda_1 x_1+\cdots+\lambda_r x_r}.$$

Because $f(x) = g(x)$ and the uniqueness of the Fourier expansion, b and c are related such that

$$b(\lambda_1,\ldots,\lambda_r) = \frac{1}{2^{(n-r)/2}} \sum_{\lambda_{r+1},\ldots,\lambda_n=0,1} c(\lambda_1,\ldots,\lambda_r,\lambda_{r+1},\ldots,\lambda_n).$$

Each $b(\lambda_1,\ldots,\lambda_r)$ is a sum of $c(\lambda_1,\ldots,\lambda_n)$'s.

The number of zeros of $g(x_1,\ldots,x_r) = f(x_1,\cdots,x_r,0,\cdots,0)$ equals $2^{r-1} + 2^{r/2-1}b(0) = 2^{r-1} + 2^{r-n/2-1} = 2^{r-1} + 2^{r-k-1}$.

A simple bent function construction is accomplished by the Boolean functions in the *Maiorana-McFarland class*. This is the the set $\mathcal{M}$ which contains all Boolean function on $\mathbb{F}_2^n = \{(x,y) : x,y \in \mathbb{F}_2^n\}$, of the form:

$$f(x,y) = x \cdot \pi(y) \oplus g(y)$$

where π is any permutation on $\mathbb{F}_2^{n/2}$ and g any Boolean function on $\mathbb{F}_2^{n/2}$.

All function in the Maiorana-McFarland class of Boolean functions are bent.

2 Bent Sequences

Sequences generated using bent functions have nice cryptographic properties because of their perfect nonlinearity. These sequences can be generated multiple ways. Two easy examples are a filtering function on a shift register producing an m-sequence or a shift register which uses n different shift registers as input into a bent function. These two techniques are discussed by Carlet [2]. Both of constructions use input vectors from $gftwo^n$ in a psuedorandom order to generate the sequence. Before scrambling the input in this way, the sequences generated by lexicographic ordering of input vectors is considered.

Using the lexicographic ordering, the finite sequence generated will be the column of the outputs for the Boolean function read from the truth table of the Boolean fucntion. For example, the *finite Boolean sequence* using a lexicographic on the Boolean function f in **??** is

$$(0,1,1,0,1,0,1,0,0,0,1,0,0,0,1,1).$$

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, 1966.

[2] C. Carlet, *Boolean functions for cryptography and error correcting codes*, Boolean Methods and Models (Y. Crama and P. L. Hammer, eds.), Cambridge University Press, 2006.

[3] T. W. Cusik and P. Stănică, *Cryptographic boolean functions and applications*, Elsevier, 2009.

[4] J. Đ. Golić, *Recent advances in stream cipher cryptanalysis*, Publications De L'Institut Mathématique **64** (1998), 183–204.

[5] S. W. Golomb, *Shift register sequences*, Aegean Park Press, 1982.

[6] M. Goresky and A. Klapper, *Algebraic shift register sequences*, Cambridge University Press, 2012.

[7] A. Klapper and M. Goresky, *Cryptoanalysis based on 2-adic rational approximation*, CRYPTO, 1995, pp. 262–273.

[8] ———, *Feedback shift registers, 2-adic span, and combiners with memory*, Journal of Cryptology **10** (1997), 111–147.

[9] ———, *Arithmetic correlations and walsh transforms*, IEEE Transactions on Information Theory **58** (2012), no. 1, 479–492.

[10] A. Klapper and J. Xu, *Algebraic feedback shift registers*, Theor. Comput. Sci. **226** (1999), no. 1-2, 61–92.

[11] ———, *Register synthesis for algebraic feedback shift registers based on non-primes*, Des. Codes Cryptography **31** (2004), no. 3, 227–250.

[12] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Springer-Verlag, 1977.

[13] J. R. Munkres, *Topology: A first course*, Prentice Hall, 1975.

[14] T. Neumann, *Bent functions*, Ph.D. thesis, University of Kaiserslautern, May 2006.

[15] N. Nisan and M. Szegedy, *On the degree of boolean functions as real polynomials*, Computational Complexity **4** (1994), 301–313.

[16] R. A. Reuppel, *Analysis and design of stream ciphers*, Springer-Verlag, 1986.

[17] O. S. Rothaus, *On b̈entf̈unctions*, Journal of Combinatorial Theory **20** (1976), no. 3, 300–305.

[18] W. J. Townsend and M. A. Thornton, *Walsh spectrum computations using cayley graphs*, IEEE Midwest Symposium on Circuits and Systems, August 2001, pp. 110–113.

[19] W. Trappe and L. C. Washington, *Introduction to cryptography with coding theory*, 2nd ed., Pearson Education, 2006.