Connections between Nonlinearity and Restrictions, Terms and Hypergraphs of Boolean Functions

Xian-Mo Zhang
Dept of Computer Science
University of Wollongong
Wollongong, NSW 2522
AUSTRALIA
Email: xianmo@cs.uow.edu.au

Yuliang Zheng
School of Comp & Info Tech
Monash University
Frankston, Melbourne
VIC 3199, AUSTRALIA
Email: yzheng@fcit.monash.edu.au

Hideki Imai
Institute of Industrial Science
University of Tokyo
7-22-1 Roppongi, Minato-ku
Tokyo 106, JAPAN
Email: imai@iis.u-tokyo.ac.jp

Abstract — **This paper studies nonlinear characteristics of (Boolean) functions which are important in cryptography. Main contributions of this paper are: (1) we show that the restriction of a function on a coset has significant influence on cryptographic properties of the function, (2) we identify relationships between the nonlinearity of a function and the distribution of terms in the polynomial representation of the function, (3) we prove that cycles of odd length in the terms, as well as quadratic terms, in the polynomial representation of a function play an important role in determining the nonlinearity of the function. Results in this paper will contribute to the study of new cryptanalytic attacks on encryption algorithms, and more important, counter-measures against such attacks.**

I. Definitions and Notations

We consider functions from V_n to $GF(2)$ (or simply functions on V_n), V_n is the vector space of n tuples of elements from $GF(2)$.

An *affine* function f on V_n is a function that takes the form of $f(x_1,\ldots,x_n) = a_1x_1 \oplus \cdots \oplus a_nx_n \oplus c$, where $a_j, c \in GF(2)$, $j = 1, 2, \ldots, n$. Furthermore f is called a *linear* function if $c = 0$.

The *nonlinearity* of f, denoted by N_f, is the minimal Hamming distance between f and all affine functions on V_n, i.e., $N_f = \min_{i=1,2,\ldots,2^{n+1}} d(f,\varphi_i)$ where φ_1, φ_2, ..., $\varphi_{2^{n+1}}$ are all the affine functions on V_n.

The nonlinearity of functions on V_n coincides with the covering radius of the first order binary Reed-Muller code $R(1,n)$ of length 2^n [2], and it is upper bounded by $2^{n-1} - 2^{\frac{1}{2}n-1}$ [6]. If $N_f = 2^{n-1} - 2^{\frac{1}{2}n-1}$ then f is called a *bent function*. Bent functions on V_n exist only for even n.

Let f be a function on V_n and U be an s-dimensional subspace of V_n. The *restriction* of f to a coset $\Pi_j = \beta_j \oplus U$, $j = 0, 1, \ldots, 2^{n-s}-1$, denoted by f_{Π_j}, is a function on U, and it is defined by $f_{\Pi_j}(\alpha) = f(\beta_j \oplus \alpha)$ for every $\alpha \in U$.

II. Main Results

Theorem 1 *Let f be a function on V_n, W be a p-dimensional subspace of V_n, and Π be a coset of W. Then the nonlinearity of f and the nonlinearity of f_Π satisfy* $N_f - N_{f_\Pi} \le 2^{n-1} - 2^{p-1}$

Theorem 2 *Let f be a function on V_n, W be a p-dimensional subspace of V_n, and Π be a coset of W. If the restriction of f to Π, f_Π, is an affine function on Π, then the nonlinearity of f, N_f, satisfies $N_f \le 2^{n-1} - 2^{p-1}$.*

Theorem 3 *Let f be a function on V_n and J be a subset of $\{1,\ldots,n\}$ such that f does not contain any term $x_{j_1}\cdots x_{j_t}$ where $t > 1$ and $j_1,\ldots,j_t \in J$. Then the nonlinearity of f, N_f, satisfies $N_f \le 2^{n-1} - 2^{s-1}$ where $s = |J|$.*

Theorem 4 *Let f be a function on V_n and P be a subset of $\{1,\ldots,n\}$ such that for any term $x_{j_1}\cdots x_{j_t}$ with $t > 1$ in f, $\{j_1,\ldots,j_t\} \cap P \ne \emptyset$ holds where $\emptyset$ denotes the empty set. Then the nonlinearity of f, N_f, satisfies $N_f \le 2^{n-1} - 2^{n-p-1}$ where $p = |P|$.*

For any function on V_n, say f, we can define the *hypergraph [1] of f*, denoted by $\Gamma(f)$, by the following rule: Let $X = \{x_1,\ldots,x_n\}$. A subset of X, $E_j = \{x_{j_1},\ldots,x_{j_t}\}$ is referred to as an edge of $\Gamma(f)$ if and only if $x_{j_1}\cdots x_{j_t}$ is a term of f.

Theorem 5 *Let f be a bent function on V_n. Then either $\Gamma(f)$ contains a cycle of odd length or f contains $\frac{1}{2}n$ disjoint quadratic terms.*

Theorem 6 *Let f be a function on V_n, whose nonlinearity, N_f, satisfies $N_f \ge 2^{n-1} - 2^{\frac{2}{3}n-t-1}$ where t is real with $1 \le t \le \frac{1}{6}n$. Then either $\Gamma(f)$ contains a cycle of odd length or f contains at least $3t$ disjoint quadratic terms.*

Theorem 7 *Let f be function on V_n, whose nonlinearity, N_f, satisfies $N_f > 2^{n-1} - 2^{\frac{2}{3}n-1}$. Then either $\Gamma(f)$ contains a cycle of odd length or f contains a quadratic term.*

References

[1] R. L. Graham and M. Grötschel and L. Lovász, *Handbook of Combinatorics*, volume 1, Elsevier Science B. V., 1995.

[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, New York, Oxford, 1978.

[3] M. Matsui, Linear Cryptanalysis Method for DES Cipher, *Advances in Cryptology - EUROCRYPT'93*, 765, Lecture Notes in Computer Science, 386-397, Springer-Verlag, Berlin, Heidelberg, New York.

[4] O. S. Rothaus, On "Bent" Functions, *Journal of Combinatorial Theory*, Ser. A, 20, pages, 300-305, 1976.

[5] National Bureau Standards, Data Encryption Standard, Federal Information Processing Standards, Publication FIPS PUB 46, U.S. Department of Commerce, January 1977.

[6] J. Seberry and X. M. Zhang and Y. Zheng, Nonlinearity and Propagation Characteristics of Balanced Boolean Functions, *Information and Computation*, 119 (1), 1-13, 1995.

[7] C. E. Shannon, Communications Theory of Secrecy Systems, *Bell System Technical Journal*, 28: 656-715, 1949.