Additive and Linear Structures of Cryptographic Functions

Xuejia Lai

R^3 Security Engineering AG, Aathal, Switzerland
lai@r3.ch

Abstract. In the design and analysis of cryptographic algorithms, exploiting the structures of such algorithms is an important aspect. In this paper, additive and linear structures of functions from $GF^n(q)$ to $GF^m(q)$ will be considered. A function f is said to have an additive structure if there is a non-zero vector $\boldsymbol{a}$, such that $f(\boldsymbol{x}+\boldsymbol{a})-f(\boldsymbol{x})$ remains invariant for all $\boldsymbol{x}$. Such a vector $\boldsymbol{a}$ is called an additive translator of the function f. A function f is said to have a linear structure if f has an additive translator $\boldsymbol{a}$ and if $f(\boldsymbol{x}+c\boldsymbol{a})-f(\boldsymbol{x})=c(f(\boldsymbol{a})-f(\boldsymbol{0}))$ for all c in $GF(q)$. We call this $\boldsymbol{a}$ a linear translator of f. We show how to use such additive and linear structures to simplify the expression of the function f. It is shown that function f has r linearly independent linear translators if and only if there is a non-singular linear transformation such that the composition of this linear transformation with the original function gives a function that is the sum of a linear function of r variables and some function of the other $n-r$ variables. In particular, when q is a prime, then any additive translator is a linear translator, which implies that f becomes a sum of an r-variable linear function and an $n-r$-variable function if and only if f has r linearly independent additive translators. Moreover, for an invertible function f, there is a one-to-one relationship between the linear translators of f and the linear translators of its inverse function.

1. Introduction

Linear structures of block ciphers have been investigated for their cryptanalytic significance. According to Evertse [2], "a block cipher has a linear structure if there are subsets of P, K and C of plaintext bits, key bits and ciphertext bits of this block cipher, respectively, such that for *each* plaintext and *each* key, a simultaneous change of all plaintext bits in P and all key bits in K has the *same* effect on the exclusive-or sum of the bits in C of the corresponding ciphertext." One well-known example [3] of such linear structures is the DES function for which the complementation of all plaintext bits and key bits results in the complementation of all ciphertext bits. It has been pointed out in [1, 2, 3, 6] that block ciphers with linear structures are vulnerable to attacks much faster than exhaustive key search. In [4], Meier and Staffelbach considered the nonlinearity of Boolean functions in terms of their Hamming distance to functions having a linear structure and constructed Boolean functions that have maximum distance to functions with a linear structure.

In this paper we consider the additive and linear structures of functions from an n dimensional vector space F^n to an m dimensional vector space F^m, where $F = GF^n(q)$ is a finite field. In Section 1, such structures will be studied in terms of *additive* and *linear translators*, where it is shown that the set of all additive translators of a function forms an additive subgroup of the domain vector space and that the set of all linear translators of a function forms a linear subspace. The main result is in Section 3 where it is shown that the linear subspace of linear translators of an n-variable function has dimension r if and only if that there is a non-singular linear transformation on the variables of the function such that the composition of this linear transformation with the original function gives a function that is the sum of a linear function in r variables and some function of $n-r$ variables which has no linear structure. In particular, if F is a prime field, i.e., a field of p elements where p is a prime, an n-variable function has r linearly independent additive translators if and only if there is a nonsingular matrix A such that $f(\boldsymbol{x}A)$ is the sum of a linear function of r components of $\boldsymbol{x}$ and some function of the other $n-r$ components of $\boldsymbol{x}$. In Section 4 it is shown that the dimension of the subspace of linear translators remains the same for every function obtained by the composition of a non-singular linear transformation and the original function. It is then shown that for a nonlinear function the sum of its nonlinear degree and the dimension of the subspace of its linear translators is upper bounded by the number n of variables. Finally, we show in Section 5 that there is a one-to-one relationship between the linear structure of an invertible function and the linear structure of its inverse function. An additional remark is made in Section 6 which interprets the additive structures in terms of differentials used in differential cryptanalysis.

2. Additive and linear structures of functions over finite fields

Throughout this paper, elements of F^n will be denoted as $\boldsymbol{x}$ or $(x_1, x_2, \ldots, x_n)$, where $x_i \in F$ and where $x_1, x_2, \ldots, x_n$ are the coordinates of $\boldsymbol{x}$ under the canonical basis of F^n :

$$e_1 = (1, 0, \ldots, 0), \quad e_2 = (0, 1, 0, \ldots, 0), \cdots, \quad e_n = (0, \ldots, 0, 1), \tag{1}$$

that is, $\boldsymbol{x} = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n$. A function $f : F^n \mapsto F^m$ will be denoted as $f(\boldsymbol{x})$ or as $f(x_1, x_2, \ldots, x_n)$ and will be called an n-variable function.

Definition. A function $f : F^n \mapsto F^m$ is said to have an *additive structure* if there is a non-zero vector $\boldsymbol{a}$ in F^n, such that $f(\boldsymbol{x} + \boldsymbol{a}) - f(\boldsymbol{x})$ is invariant for all $\boldsymbol{x}$ in F^n. Such a vector $\boldsymbol{a}$ will be called an *additive translator* of the function f. A function f is said to have a *linear structure* if there is a non-zero vector $\boldsymbol{a}$ in F^n, such that

$$f(\boldsymbol{x} + c\boldsymbol{a}) - f(\boldsymbol{x}) = c(f(\boldsymbol{a}) - f(\boldsymbol{0})) \tag{2}$$

for all c in F, such a vector $\boldsymbol{a}$ will be called a *linear translator* of the function f. By setting $c = 1$, we see that any linear translator is always an additive translator. (By way of convention, we consider the all-zero vector $\mathbf{0}$ to be a linear translator for any function.)

By choosing $\boldsymbol{x}=\mathbf{0}$, we see that $\boldsymbol{a} = (a_1, \ldots, a_n)$ is an additive translator of function f if and only if

$$f(x_1+a_1, x_2+a_2, \ldots, x_n+a_n) = f(x_1, x_2, \ldots, x_n) + f(a_1, a_2, \ldots, a_n) - f(0, 0, ..., 0)$$

or in vector notation,

$$f(\boldsymbol{x} + \boldsymbol{a}) = f(\boldsymbol{x}) + f(\boldsymbol{a}) - f(\mathbf{0}), \tag{3}$$

for all $\boldsymbol{x}=(x_1, \ldots, x_n)$ in F^n. Similarly, we obtain from (2) that

$$f(c\boldsymbol{a}) = cf(\boldsymbol{a}) - (c-1)f(\mathbf{0}) \tag{4}$$

holds for all c in F if $\boldsymbol{a}$ is a linear translator of f.

Theorem 1. *For a function $f : F^n \mapsto F^m$, the set of all additive translators of f forms an additive subgroup of F^n, and the set of all linear translators of f forms a linear subspace of F^n.*

Proof. Let $\boldsymbol{a}$, $\boldsymbol{b}$ be two additive translators of function f. Set $\boldsymbol{x} = \boldsymbol{b}$ in (3), we have

$$f(\boldsymbol{a} + \boldsymbol{b}) = f(\boldsymbol{a}) + f(\boldsymbol{b}) - f(\mathbf{0}). \tag{5}$$

Thus, for all $\boldsymbol{x}$ in F^n,

$$\begin{aligned} f(\boldsymbol{x} + \boldsymbol{a} + \boldsymbol{b}) &= f(\boldsymbol{x} + \boldsymbol{a}) + f(\boldsymbol{b}) - f(\mathbf{0}) \\ &= f(\boldsymbol{x}) + f(\boldsymbol{a}) + f(\boldsymbol{b}) - f(\mathbf{0}) - f(\mathbf{0}) \\ &= f(\boldsymbol{x}) + f(\boldsymbol{a} + \boldsymbol{b}) - f(\mathbf{0}), \end{aligned}$$

so that $\boldsymbol{a} + \boldsymbol{b}$ is also an additive translator of f. Thus, the set of additive translators is an additive subgroup.

Since a linear translator is always an additive translator, it remains to show that if $\boldsymbol{a}$ is a linear translator of function f then for any c_0 in F, $\boldsymbol{b} = c_0\boldsymbol{a}$ is also a linear translator. For any c in F, because $\boldsymbol{a}$ is a linear translator,

$$\begin{aligned} f(\boldsymbol{x} + c\boldsymbol{b}) - f(\boldsymbol{x}) &= f(\boldsymbol{x} + cc_0\boldsymbol{a}) - f(\boldsymbol{x}) = c[c_0(f(\boldsymbol{a}) - f(\mathbf{0}))] \\ &= c[f(c_0\boldsymbol{a}) - f(\mathbf{0})] = c(f(\boldsymbol{b}) - f(\mathbf{0})) \end{aligned}$$

where the third equality is obtained from (4). Thus, $\boldsymbol{b} = c_0\boldsymbol{a}$ is indeed a linear translator of F, so that the set of linear translators is a linear subspace. □

Now we show that over a prime field additive translator and linear translator are the same concept. This explains the reason that 'additive' structure was often referred to as 'linear' structure in the earlier literature because the most often considered operation in cryptography is the bitwise-XOR, i.e., over $GF(2)$. In particular, the set of additive translators forms a linear subspace for functions over prime fields. Later we will show by example that this is not the case over a general finite field.

Theorem 2. *If $F = GF(p)$, a finite field of p elements where p is a prime, then an additive translator is also a linear translator.*

Proof. Let $\boldsymbol{a}$ be an additive translator of f. By choosing $\boldsymbol{b} = \boldsymbol{a}$, $\boldsymbol{b} = 2\boldsymbol{a}, \ldots,$ $\boldsymbol{b} = (p-1)\boldsymbol{a}$, it follows from Theorem 1 that for each element c of the prime field F, $c\boldsymbol{a}$ is also an additive translator of f. By using (5) repeatedly, we obtain

$$\begin{aligned} f(c\boldsymbol{a}) &= f((c-1)\boldsymbol{a} + \boldsymbol{a}) \\ &= f((c-1)\boldsymbol{a}) + f(\boldsymbol{a}) - f(\boldsymbol{0}) \\ &= f((c-2)\boldsymbol{a}) + 2f(\boldsymbol{a}) - 2f(\boldsymbol{0}) \\ &= f(\boldsymbol{a}) + (c-1)f(\boldsymbol{a}) - (c-1)f(\boldsymbol{0}) \\ &= cf(\boldsymbol{a}) - (c-1)f(\boldsymbol{0}). \end{aligned}$$

In (2) setting $\boldsymbol{x}$=$\boldsymbol{0}$ and using the above equality, we have

$$f(\boldsymbol{x} + c\boldsymbol{a}) - f(\boldsymbol{x}) = f(c\boldsymbol{a}) - f(\boldsymbol{0}) = cf(\boldsymbol{a}) - cf(\boldsymbol{0})$$

which shows that $\boldsymbol{a}$ is a linear translator of f. □

3. Using linear structures to simplify functions

Now we show how to use linear structures to simplify the expression of a function. Let L_f denote the set of all linear translators of function f.

Theorem 3. *Let f be a function from F^n to F^m. Then there exists an $n \times n$ invertible matrix A over F such that*

$$g(x_1, \ldots, x_n) = f((x_1, \ldots, x_n)A) = x_1\boldsymbol{v}_1 + \cdots + x_r\boldsymbol{v}_r + g^*(x_{r+1}, \ldots, x_n) \quad (6)$$

where $\boldsymbol{v}_i \in F^m$, for $1 \le i \le r$ and g^* is some non-constant function of $n-r$ variables which has no linear structure if and only if the set of linear translators of f forms an r-dimensional subspace of F^n.

Proof. First, suppose that L_f is an r-dimensional subspace. Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r$ be r linearly independent linear translators that form a basis for L_f. $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r$ can be extended to a basis of the vector space F^n : $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r, \boldsymbol{a}_{r+1}, \ldots, \boldsymbol{a}_n$. Let A be the linear transformation from the canonical basis (1) $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ to the basis $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$. Then A is non-singular and $\boldsymbol{a}_i = \boldsymbol{e}_i A$. We have

$$g(x_1, ..., x_n) = f((x_1, ..., x_n)A) = f((x_1\boldsymbol{e}_1 + \cdots + x_n\boldsymbol{e}_n)A) = f(x_1\boldsymbol{a}_1 + \cdots + x_n\boldsymbol{a}_n).$$

Because L_f is a subspace of F^n, $x_1\boldsymbol{a}_1$ is also a linear translator so we may use (3) and (4) to obtain

$$\begin{aligned} f(x_1\boldsymbol{a}_1 + \cdots + x_n\boldsymbol{a}_n) &= f(x_2\boldsymbol{a}_2 + \cdots + x_n\boldsymbol{a}_n) + f(x_1\boldsymbol{a}_1) - f(\boldsymbol{0}) \\ &= x_1 f(\boldsymbol{a}_1) - (x_1 - 1)f(\boldsymbol{0}) - f(\boldsymbol{0}) + f(x_2\boldsymbol{a}_2 + \cdots + x_n\boldsymbol{a}_n) \\ &= x_1(f(\boldsymbol{a}_1) - f(\boldsymbol{0})) + f(x_2\boldsymbol{a}_2 + \cdots + x_n\boldsymbol{a}_n). \end{aligned}$$

Proceeding similarly for the linear translators $\boldsymbol{a}_2, \ldots, \boldsymbol{a}_r$ gives

$$g(x_1, ..., x_n) = x_1\boldsymbol{v}_1 + \cdots + x_r\boldsymbol{v}_r + g^*(x_{r+1}, \ldots, x_n),$$

where $\boldsymbol{v}_i = f(\boldsymbol{a}_i) - f(\boldsymbol{0})$, for $i = 1, ..., r$, and where

$$g^*(x_{r+1}, \ldots, x_n) = f(x_{r+1}\boldsymbol{a}_{r+1} + \cdots + x_n\boldsymbol{a}_n)$$

is a function of $n-r$ variables. Moreover, if $(b_{r+1}, \ldots, b_n) \neq (0, \ldots, 0)$ is a linear translator of function g^*, then $\boldsymbol{b} = (0, \ldots, 0, b_{r+1}, \ldots, b_n)$ is a linear translator of the function g, and $\boldsymbol{b}$ is linearly independent of $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r$ so that $\boldsymbol{b}A$ is linearly independent of $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r$. But then $\boldsymbol{b}A$ will be a linear translator of f because

$$f(\boldsymbol{x}A + c\boldsymbol{b}A) = g(\boldsymbol{x} + c\boldsymbol{b}) = g(\boldsymbol{x}) + c(g(\boldsymbol{b}) - g(\boldsymbol{0})) = f(\boldsymbol{x}A) + c(f(\boldsymbol{b}A) - f(\boldsymbol{0}))$$

for all $\boldsymbol{x}A$ in F^n. This contradicts the assumption that $\dim L_f = r$. Therefore, function g^* has no linear structure.

Conversely, suppose that A is a non-singular transformation such that

$$g(x_1, \ldots, x_n) = f((x_1, \ldots, x_n)A) = x_1\boldsymbol{v}_1 + \cdots + x_r\boldsymbol{v}_r + g^*(x_{r+1}, \ldots, x_n)$$

where g^* has no linear structure. First we show that $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r$ are linear translators of g. For $1 \leq i \leq r$ and for all c in F^n,

$$\begin{aligned} g(\boldsymbol{x} + c\boldsymbol{e}_i) &= g(x_1, \ldots, x_{i-1}, x_i + c, x_{i+1}, \ldots, x_n) \\ &= x_1\boldsymbol{v}_1 + \cdots + (x_i + c)\boldsymbol{v}_i + \cdots + x_r\boldsymbol{v}_r + g^*(x_{r+1}, \ldots, x_n) \\ &= x_1\boldsymbol{v}_1 + \cdots + x_r\boldsymbol{v}_r + g^*(x_{r+1}, \cdots, x_n) + c\boldsymbol{v}_i \\ &= g(\boldsymbol{x}) + c\boldsymbol{v}_i, \end{aligned} \tag{7}$$

By setting $\boldsymbol{x} = 0$ in the above equation, we obtain that $g(c\boldsymbol{e}_i) = g(\boldsymbol{0}) + c\boldsymbol{v}_i$. For $c = 1$, we have $\boldsymbol{v}_i = g(\boldsymbol{e}_i) - g(\boldsymbol{0})$. Thus,

$$g(\boldsymbol{x} + c\boldsymbol{e}_i) - g(\boldsymbol{x}) = c\boldsymbol{v}_i = c(g(\boldsymbol{e}_i) - g(\boldsymbol{0})), \tag{8}$$

which implies that $\boldsymbol{e}_i$ is a linear translator of g.

Now we show that every linear translator of function g is a linear combination of $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r$. Let $\boldsymbol{b} = (b_1, ..., b_n)$ be a linear translator of g, then for all c in F,

$$g(\boldsymbol{x} + c\boldsymbol{b}) = g(\boldsymbol{x}) + c(g(\boldsymbol{b}) - g(\boldsymbol{0})). \tag{9}$$

The left side of the above equation is

$$(x_1 + cb_1)\boldsymbol{v}_1 + \cdots + (x_r + cb_r)\boldsymbol{v}_r + g^*(x_{r+1} + cb_{r+1}, \ldots, x_n + cb_n)$$

and the right side is

$$x_1\boldsymbol{v}_1 + \cdots + x_r\boldsymbol{v}_r + g^*(x_{r+1}, ..., x_n) + c[b_1\boldsymbol{v}_1 + \cdots + b_r\boldsymbol{v}_r + g^*(b_{r+1}, ..., b_n) - g^*(0, ..., 0)].$$

Thus, (9) is equivalent to

$$g^*(x_{r+1} + cb_{r+1}, ..., x_n + cb_n) = g^*(x_{r+1}, ..., x_n) + c[g^*(b_{r+1}, ..., b_n) - g^*(0, ..., 0)],$$

that is, $\boldsymbol{b} = (b_1, ..., b_n)$ is a linear translator of function g if and only if $(b_{r+1}, ..., b_n)$ is a linear translator of function g^*. From the assumption that g^* has no linear structure we obtain $b_{r+1} = \cdots = b_n = 0$. Therefore, every linear translator of function g is a linear combination of $e_1, \ldots, e_r$. This completes the proof of the theorem. □

By applying Theorem 1 and 2, Theorem 3 implies:

Corollary 4. *Let F be a finite field of p elements where p is a prime. Then a function $f : F^n \mapsto F^m$ has r linearly independent additive translators if and only if there exists an $n \times n$ invertible matrix A over F such that*

$$g(x_1, \ldots, x_n) = f((x_1, \ldots, x_n)A) = x_1\boldsymbol{v}_1 + \cdots + x_r\boldsymbol{v}_r + g^*(x_{r+1}, \ldots, x_n) \quad (10)$$

where $\boldsymbol{v}_i \in F^m$, for $1 \leq i \leq r$ and g^* is some non-constant function of n-r variables without additive structure.

Example 1. Consider the case that $n = 3, m = 1$ and $F = GF(2)$. For the following function of 3 variables,

$$f(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3 + x_2 + x_3,$$

the vector (111) in F_2^3 is a linear translator of f:

$$f(x_1 + 1, x_2 + 1, x_3 + 1) = f(x_1, x_2, x_3) + 1.$$

Let $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$, then $\det A \neq 0$, and

$$f((x_1, x_2, x_3)A) = f(x_1 + x_2 + x_3, x_1 + x_3, x_1 + x_2) = x_1 + x_2x_3.$$

Remark. We have proved in Theorem 2 that if F is a prime field, then the set of additive translators of a function forms a linear subspace. It was shown in [5, Proposition 3] that, for a quadratic function f, the set of additive translators is a linear subspace of F^n for any finite field F. In general, however, this result is not true. The following example due to Nyberg shows that there exist functions for which the set of additive translators is not a linear subspace.

Example 2. Consider the following function from $(GF(2^2))^3$ to $GF(2^2)$:

$$f[X, Y, Z] = f[(x_1, x_2), (y_1, y_2), (z_1, z_2)] = (x_1x_2y_1 + y_2, z_1z_2)$$

where x_i, y_i, z_i are in $GF(2)$. f has only one nonzero additive translator

$$[(0, 0), (0, 1), (0, 0)].$$

Thus, the set of additive translators cannot be a subspace because any non-zero subspace contains at least four elements. □

Remark. The result of Theorem 3 implies that it is not always possible to transform a function with r linearly independent *additive* translators into the form as the sum of a linear function of r variables and some function of $(n-r)$ variables even if the set of additive translators is a subspace, as shown by the following example. [This example further implies that Proposition 4 in [5] is not true.]

Example 3. Consider again the function

$$f(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3 + x_2 + x_3,$$

which is of the same form as in Example 1 but is over the field $F = GF(2^2)$. It is easy to verify that the vectors $\alpha(111), \alpha \in F$ are the only additive translators of f and that they form a linear subspace. However, for $\alpha \in GF(2^2)$ such that $\alpha^2 \neq \alpha$,

$$f(\alpha(1,1,1)) = f(\alpha,\alpha,\alpha) = \alpha^2 \neq \alpha = \alpha f(1,1,1),$$

so that α is not a linear translator of f. Theorem 3 then implies that the function f cannot be transformed into the form

$$g(x_1, x_2, x_3) = x_1a_1 + g^*(x_2, x_3).$$

4. Linear Structures and nonlinearity

Theorem 3 implies that for any function g obtained from a function f by a non-singular linear transformation on the variables of f, $\dim(L_g) = \dim(L_f)$. That is, $\dim(L_f)$ is invariant under linear transformations on the variables of f. Thus, $\dim(L_f)$ provides a useful measure of the "partial" linearity of function f. Another such invariance is the nonlinear degree (or nonlinear order) of f. For a function from F^n to F^m, its component functions (from F^n to F) can be written in the form of multivariable polynomials. We define the degree of monomial $x_1^{i_1} \cdots x_n^{i_n}$ to be $\sum_1^n i_j$ and the degree of a polynomial as the maximum of the degrees of the monomials occurring in the polynomial. The (total) degree of f is then defined as the maximum of the degrees of its component polynomials. The following Lemma shows that the nonlinear degree (or nonlinear order) of f is also invariant under nonsingular linear transformations on its variables.

Lemma 5. *Let*

$$g(x_1, \ldots, x_n) = f((x_1, \ldots, x_n)A)$$

where A is a nonsingular $n \times n$ matrix over F, then $\deg(f) = \deg(g)$.

Proof. We show first that $\deg(g) \leq \deg(f)$, the equality then follows from the invertibility of A. Let $x_1^{i_1} \cdots x_n^{i_n}$ be a monomial of f with degree $\sum_1^n i_j$. Under the transformation A $= \{a_{ij}\}$, the monomial becomes

$$(a_{11}x_1 + a_{21}x_2 + \cdots + a_{n1}x_n)^{i_1} \cdots (a_{1n}x_1 + a_{2n}x_2 + \cdots + a_{nn}x_n)^{i_n}.$$

Using the fact that $\deg(f_1 + f_2) \leq \max(\deg(f_1), \deg(f_2))$ and $\deg(f_1 f_2) \leq \deg(f_1) + \deg(f_2)$, we obtain

$$\begin{aligned}\deg\ & [(a_{11}x_1 + \cdots + a_{n1}x_n)^{i_1} \cdots (a_{1n}x_1 + \cdots + a_{nn}x_n)^{i_n}] \\ & \leq \deg[(a_{11}x_1 + \cdots + a_{n1}x_n)^{i_1}] + \cdots + \deg[(a_{1n}x_1 + \cdots + a_{nn}x_n)^{i_n}] \\ & \leq i_1 \deg(a_{11}x_1 + \cdots + a_{n1}x_n) + \cdots + i_n \deg(a_{1n}x_1 + \cdots + a_{nn}x_n) \\ & = \sum_1^n i_j = \deg(x_1^{i_1} \cdots x_n^{i_n}),\end{aligned}$$

that is, the degree of each monomial will not increase under the transformation A. Thus, the degree of each component polynomial of f will not increase under the transformation A, which implies that $\deg(g) \leq \deg(f)$. On the other hand, $f(x_1, \ldots, x_n) = g((x_1, \ldots, x_n)A^{-1})$ because A is invertible, so the above argument implies that $\deg(f) \leq \deg(g)$. Therefore, $\deg(f) = \deg(g)$. □

Now applying Theorem 3 to a nonlinear function f with $r = \dim(L_f)$, we know that f can be transformed into the form:

$$g(x_1, \ldots, x_n) = x_1 v_1 + \cdots + x_r v_r + g^*(x_{r+1}, \ldots, x_n).$$

Therefore,

$$\deg(f) = \deg(g) = \deg(g^*) \leq n - r \ = n - \dim(L_f).$$

Thus, we obtain the following result.

Theorem 6. *For a nonlinear function $f : F^n \mapsto F^m$,*

$$\deg(f) + \dim(L_f) \leq n.$$

In particular, a nonlinear function of full degree has no linear structure. Note that for a linear function f, $\deg(f) = 1$ and $\dim(L_f) = n$.

Example 4. Consider again the Boolean function in Example 1. Because that the function f has non-linear degree 2, the above result implies that

$$1 \leq \dim(L_f) \leq 3 - \deg(f) = 1.$$

Thus, $(1, 1, 1)$ is the only non-zero linear translator of the function f.

5. Linear structures of invertible functions

In cryptography, invertible functions are of special interest. For example, a block cipher with a given key is an invertible function. Another example is that the S-boxes in the DES consist of invertible functions from F_2^4 to F_2^4. The next result shows the relationship between the linear structures of an invertible function and that of the inverse function.

Theorem 7. *Let $f : F^n \mapsto F^n$ be an invertible function, where F is an arbitrary finite field. Then $\boldsymbol{a}$ is a linear (additive) translator of f if and only if $\boldsymbol{d} = f(\boldsymbol{a}) - f(\boldsymbol{0})$ is a linear (additive) translator of f^{-1}. Moreover, the function f and its inverse f^{-1} have the same number of linearly independent linear translators.*

Proof. For the first part of Theorem, we show first the case for linear translators. Denote $\boldsymbol{y} = f(\boldsymbol{x})$, then $\boldsymbol{x} = f^{-1}(\boldsymbol{y})$, and denote $\boldsymbol{x}_0 = f^{-1}(\boldsymbol{0})$. For a linear translator $\boldsymbol{a}$ of function f, we have $\boldsymbol{a}+\boldsymbol{x}_0 = f^{-1}(f(\boldsymbol{a})-f(\boldsymbol{0})) = f^{-1}(\boldsymbol{d})$ because

$$f(\boldsymbol{a}+\boldsymbol{x}_0) = f(\boldsymbol{a}) + f(\boldsymbol{x}_0) - f(\boldsymbol{0}) = f(\boldsymbol{a}) - f(\boldsymbol{0}) = \boldsymbol{d}.$$

Thus, for any c in F, $\boldsymbol{a}$ is a linear translator of f

$$\begin{aligned}
\Longleftrightarrow\quad & f(\boldsymbol{x}) + c(f(\boldsymbol{a}) - f(\boldsymbol{0})) = f(\boldsymbol{x} + c\boldsymbol{a}) \qquad \forall \boldsymbol{x} \in F^n \\
\Longleftrightarrow\quad & \boldsymbol{y} + c\boldsymbol{d} = f(\boldsymbol{x} + c\boldsymbol{a}) \qquad \forall \boldsymbol{x} \in F^n \\
\Longleftrightarrow\quad & f^{-1}(\boldsymbol{y} + c\boldsymbol{d}) = \boldsymbol{x} + c\boldsymbol{a} = f^{-1}(\boldsymbol{y}) + c[\boldsymbol{a} + \boldsymbol{x}_0 - \boldsymbol{x}_0] \\
& \qquad = f^{-1}(\boldsymbol{y}) + c[f^{-1}(\boldsymbol{d}) - f^{-1}(\boldsymbol{0})] \quad \forall \boldsymbol{y} \in F^n \\
\Longleftrightarrow\quad & \boldsymbol{d} = f(\boldsymbol{a}) - f(\boldsymbol{0}) \text{ is a linear translator of } f^{-1}.
\end{aligned}$$

Let $c = 1$ in the above proof, we obtain the proof for the case of additive translators.

To show the second part of the Theorem, let $\boldsymbol{a}$ and $\boldsymbol{b}$ be linear translators of f. Equation (4) and (5) implies that for any c_1, c_2 in F,

$$\begin{aligned}
f(c_1\boldsymbol{a} + c_2\boldsymbol{b}) &= c_1 f(\boldsymbol{a}) - (c_1 - 1)f(\boldsymbol{0}) + c_2 f(\boldsymbol{b}) - (c_2 - 1)f(\boldsymbol{0}) - f(\boldsymbol{0}) \\
&= c_1(f(\boldsymbol{a}) - f(\boldsymbol{0})) + c_2(f(\boldsymbol{b}) - f(\boldsymbol{0})) + f(\boldsymbol{0}).
\end{aligned}$$

Thus,

$$f(c_1\boldsymbol{a} + c_2\boldsymbol{b}) = f(\boldsymbol{0}) \quad \text{if and only if} \quad c_1(f(\boldsymbol{a}) - f(\boldsymbol{0})) + c_2(f(\boldsymbol{b}) - f(\boldsymbol{0})) = \boldsymbol{0}.$$

Because f is invertible, we see that

$$c_1\boldsymbol{a} + c_2\boldsymbol{b} = \boldsymbol{0} \quad \text{if and only if} \quad c_1(f(\boldsymbol{a}) - f(\boldsymbol{0})) + c_2(f(\boldsymbol{b}) - f(\boldsymbol{0})) = \boldsymbol{0}.$$

Thus, we have shown that $\boldsymbol{a}$ and $\boldsymbol{b}$ are linearly independent linear translators of function f if and only if $f(\boldsymbol{a}) - f(\boldsymbol{0})$ and $f(\boldsymbol{b}) - f(\boldsymbol{0})$ are linearly independent linear translators of the inverse function f^{-1}. Therefore, L_f and $L_{f^{-1}}$ have the same dimension. □

Similar to Theorem 3, we consider the "normal" form of an invertible function having linear structures. A function $f : F^n \mapsto F^n$ will be expressed as

$$\boldsymbol{y} = f(\boldsymbol{x}) \quad \Longleftrightarrow \quad \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} f_1(x_1, x_2, \ldots, x_n) \\ f_2(x_1, x_2, \ldots, x_n) \\ \vdots \\ f_n(x_1, x_2, \ldots, x_n) \end{bmatrix},$$

that is, f maps row vector $(x_1, \ldots, x_n)$ to column vector $(y_1, \ldots, y_n)$.

Theorem 8. *Let $f : F^n \mapsto F^n$ be an invertible function, then f has r linearly independent linear translators if and only if there exist $n \times n$ invertible matrices A and M over F such that*

$$g(\boldsymbol{x}) = Mf(\boldsymbol{x}A) = \begin{bmatrix} x_1 + g_1^*(x_{r+1}, \ldots, x_n) \\ \vdots \\ x_r + g_r^*(x_{r+1}, \ldots, x_n) \\ g_{r+1}^*(x_{r+1}, \ldots, x_n) \\ \vdots \\ g_n^*(x_{r+1}, \ldots, x_n) \end{bmatrix}. \tag{11}$$

Proof. Let $\boldsymbol{a}_i, i = 1, ..., r$ be r linearly independent linear translators of f. By Theorem 7, $f(\boldsymbol{a}_i) - f(\boldsymbol{0})$, $i = 1, ..., r$, are r linear translators of f^{-1}, and they are linearly independent because f is invertible. Let A be an invertible matrix such that $\boldsymbol{e}_i A = \boldsymbol{a}_i$, by Theorem 3 function $f(\boldsymbol{x}A)$ will have the form shown in (6):

$$f((x_1, \ldots, x_n)A) = x_1\boldsymbol{v}_1 + \cdots + x_r\boldsymbol{v}_r + g'(x_{r+1}, \ldots, x_n) \tag{12}$$

where $\boldsymbol{v}_i = f(\boldsymbol{a}_i) - f(\boldsymbol{0})$. Now let M be an invertible matrix such that $M(f(\boldsymbol{a}_i) - f(\boldsymbol{0}))^T = \boldsymbol{e}_i^T$, then the function $g(\boldsymbol{x}) = Mf(\boldsymbol{x}A)$ will have the form in (11).

Conversely, suppose (11) holds, then Theorem 3 implies that the vectors $\boldsymbol{a}_i = \boldsymbol{e}_i A$, $i = 1, ..., r$, are r linearly independent linear translators of function f. □

In cryptographic practice, the methods of *confusion* and *diffusion*, introduced by Shannon [7], are fundamental. A function will be said to achieve *complete diffusion* if each of its output variable depends on every input variable. The following result is a direct consequence of Theorem 8. It shows a relationship between the complete diffusion and the nonlinearity with respect to linear structures for an invertible function.

Corollary 9. *Let f: $F^n \mapsto F^n$, $n \geq 3$, be an invertible function such that, for any $n \times n$ invertible matrices A and M, the function $g(\boldsymbol{x}) = Mf(\boldsymbol{x}A)$ achieves complete diffusion, then the function f has no linear structure.*

A remark on additive translators and differential cryptanalysis

The basic concept used in differential cryptanalysis [8] is that of 'differentials' and their probabilities [8, 9]. A differential of a function f can be defined as a couple $(\boldsymbol{a},\boldsymbol{b})$ such that, if a pair of inputs of f has difference $\Delta\boldsymbol{x} = \boldsymbol{x}_1 - \boldsymbol{x} = \boldsymbol{a}$, then $\boldsymbol{b}$ is a possible value of the difference of the pair of outputs of f: $\Delta\boldsymbol{y} = f(\boldsymbol{x}_1) - f(\boldsymbol{x}) = f(\boldsymbol{x} + \boldsymbol{a}) - f(\boldsymbol{x})$. It then follows from (3) that $\boldsymbol{a}$ *is an additive translator of f if and only if $(\boldsymbol{a}, f(\boldsymbol{a}) - f(\boldsymbol{0}))$ is a differential of f with probability one.*

6. Summary

In this paper we have considered additive and linear structures of functions over a finite field in terms of their additive and linear translators. The main result was that an n-variable function has r linearly independent linear translators if and only if there is a non-singular linear transformation on the variables of the function such that the resulting function is the sum of a linear function of r variables and a function of the other $n - r$ variables.

Acknowledgement

The author would like to thank J.L. Massey for his encouraging criticism on this work when the author was at the ETH Zürich. The author would also like to thank K. Nyberg for her valuable suggestions (especially for using the term additive translators) which greatly improved this work.

References

1. D. Chaum, J.H. Evertse, Cryptanalysis of DES with a reduced number of rounds, *Advances in Cryptology - CRYPTO'85, Proceedings,* pp. 192–211, Springer-Verlag, 1986.
2. J.H. Evertse, Linear structures in block ciphers, *Advances in Cryptology - EUROCRYPT'87, Proceedings,* pp. 249–266, Springer-Verlag, 1988.
3. M. Hellman, R. Merkle, R. Schroeppel, L. Washington, W. Diffie, S. Pohlig, P. Schweitzer, Results of an initial attempt to cryptanalyze the NBS Data Encryption Standard, Information System Lab. report SEL 76-042, Stanford University, 1976.
4. W. Meier, O. Staffelbach, Nonlinearity criteria for cryptographic functions, *Advances in Cryptology - EUROCRYPT'89, Proceedings,* pp. 549–562, Springer-Verlag, 1990.
5. K. Nyberg, On the construction of highly nonlinear permutations *Advances in Cryptology - EUROCRYPT'92, Proceedings,* pp. 92–98, Springer-Verlag, 1993.
6. J.A. Reeds, J.L. Manferdeli, DES has no per round linear factors, *Advances in Cryptology - CRYPTO'84, Proceedings,* pp. 377–389, Springer-Verlag, 1985.
7. C. E. Shannon, "Communication Theory of Secrecy Systems", Bell. System Technical Journal, Vol. 28, pp. 656-715, Oct. 1949.
8. E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard,* Springer-Verlag, 1993.
9. X. Lai, J. L. Massey and S. Murphy, "Markov Ciphers and Differential Cryptanalysis", *Advances in Cryptology – EUROCRYPT'91, Proceedings,* LNCS 547, pp. 17-38, Springer-Verlag, Berlin, 1991.