2-round Substitution-Permutation and 3-round Feistel Networks have bad Algebraic Degree

Didier Alquié
DGA, CELAR
didier.alquie@laposte.net

February 5, 2010

Abstract

We study algebraic degree profile of reduced-round block cipher schemes. We show that the degree is not maximal with elementary combinatorial and algebraic arguments. We discuss on how it can be turned into distinguishers from balanced random functions.

1 Introduction

1.1 Context and related works

Generic Feistel schemes have received much attention, probably due to the particular esssential structure that each round identically copies half the entry. Although SP-schemes give the feeling that every bit of input data "goes through" a non linear boolean function, Feistel schemes give the feeling that this non linear crossing only occurs one round out of two for any given input bit.

Indeed, the security of reduced round generic Feistel schemes has been studied under well defined security models. Since the original paper by M. Luby and C. Rackoff [1], various contributions by Patarin and al. [2, 3, 4, 5] show how such schemes are "different", in fact distinguishable, from random permutations. These papers give the complexities of various distinguishers, in terms of adversary model, amount of known data or chosen queries to an oracle, and negligible error probability.

In the present paper, we stress that the Feistel structure but also SP schemes induces abnormal behaviour of algebraic degrees. More precisely, we proove that algebraic degrees on – very – reduced round is always sub optimal, making the corresponding scheme indeed different from a random permutation.

The work essentially relies on intrinsic properties of boolean functions. It is strongly related to evaluation of the algebraic expression of the whole scheme as a boolean function. Thus, unfortunately, it requires a irrelevant number of queries and, in this way, cannot pretend to turn into any efficient distinguisher. Nevertheless, it lightens algebraic features that come to confirm previously known generic weaknesses on Feistel schemes. Besides, this "algebraic-degree" approach is, up to our knowledge, an original point of view.

Finally, we are not aware of systematic studies on generic SP schemes, so that the corresponding results in the present paper may be original as well.

1.2 Outline

Paper is organized as follows. Section 2 introduces notations and definitions. In section 3, we give some easy but useful results on boolean functions with possibly multiple output bits, the proofs of which are gathered in appendix A. Section 4 studies the algebraic degree profile of a 2-round SP network, as Section 5 gives the analogue for a 3-round Feistel network. Section 6 discusses some consequences on distinguishing those reduced-round block ciphers from random functions. The results in their brute form appear to be inefficient to this purpose, possible directions are proposed for further research.

2 Notations and definitions

Let $\mathbb{F}_2^n$ be n-dimensionnal vector space over the finite field $\mathbb{F}_2$, and define the partial order $\preceq$ in $\mathbb{F}_2^n$ by $x \preceq y \Leftrightarrow \forall i = 1, \ldots, n,\ x_i \leq y_i$.
We deal with boolean functions with mulitple, say $n(> 1)$ input bits, and possibly multiple output bits. We refer to a boolean function with single (resp. multiple) output bit(s) as a *scalar* (resp. *vectorial*) boolean function. The *support* (resp. *weight*) of a scalar boolean function denotes the set $f^{-1}(1)$ (resp. the cardinality of the latter) and is denoted by Supp(f) (resp. $wt(f)$).
Every scalar boolean function $f(x_1, \ldots, x_n)$ can be uniquely represented by its *algebraic normal form* (ANF), a multivariate polynomial in the quotient polynomial ring $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n)$:

$$f(x_1, \ldots, x_n) = \sum_{(u_1,\ldots,u_n)\in\mathbb{F}_2^n} a_{u_1,\ldots,u_n} x_1^{u_1} \ldots x_n^{u_n}$$

Note that $x_1^{u_1} \ldots x_n^{u_n} = 1$ if, and only if for every $i = 1, \ldots, n$, $x_i = 1$ whenever $u_i = 1$.
The *algebraic degree* of f is the maximum degree of monomials $x_1^{u_1} \ldots x_n^{u_n}$ for which $a_{u_1,\ldots,u_n}$ is not zero. It isdenoted by $\deg(f)$.

2.1 The Mobius transform

Recall that the so called *Mobius transform* gives a correspondance between the list of the values of the function f and the list of its ANF coefficients. More precisely, it goes from one list to the other by the way:

$$\begin{aligned} \forall(u_1, \ldots, u_n) \in \mathbb{F}_2^n, \quad a_{u_1,\ldots,u_n} &= \sum_{(x_1,\ldots,x_n)\preceq(u_1,\ldots,u_n)} f(x_1, \ldots, x_n) \\ \forall(x_1, \ldots, x_n) \in \mathbb{F}_2^n, \quad f(x_1, \ldots, x_n) &= \sum_{(u_1,\ldots,u_n)\preceq(x_1,\ldots,x_n)} a_{u_1,\ldots,u_n} \end{aligned}$$

For $x = (x_1, \ldots, x_n)$ and $u = (u_1, \ldots, u_n) \in \mathbb{F}_2^n$, define the symbolic x^u to be the monomial $x_1^{u_1} \ldots x_n^{u_n}$ in the aformentionned quotient polynomial ring.
Here we borrow the notation of indicator function, and denote generically $1(A)$ for the boolean number that is 1 (resp. 0) if proposition A holds (resp. does not hold). It permits a very compact rewriting of all these properties. First, $x^u = 1 \Leftrightarrow u \preceq x$, and then $x^u = 1(u \preceq x)$. Therefore, the Mobius correspondance

can be rewritten itself in a short way:

$$\forall u \in \mathbb{F}_2^n,\ \ a_u = \sum_{x\in\mathbb{F}_2^n} f(x)1(x \preceq u)$$
$$\forall x \in \mathbb{F}_2^n,\ \ f(x) = \sum_{u\in\mathbb{F}_2^n} a_u 1(u \preceq x)$$

The reason why we want to point out this compact writing is actually an epiphenomenon: in our feeling, it makes it easier to formally write the proof of these equalities. Indicator function notation is generally easy to handle formally, even if it is not the most concrete writing in this particular case.

3 Results on balancedness of boolean functions

In this section we give a few basic results on the relationship between algebraic degree and balancedness of boolean functions. We make intense use of those results in the following sections, and therefore we have decided to summarize them in the present section, pushing their proofs away to the appendix.
We show that the balancedness of vectorial boolean functions is closely related to the balancedness of (scalar) nonzero linear forms of their output bits. We also establish a nice result about balancedness of pointwise products of the output bits. We finally formulate the properties in the specific case of n-variables bijections.
Let us start with a lemma. It is rather elementary, but the subsequent results of this section largely make use of it.

Lemma 1 *Let f be a scalar (ie with single output bit) boolean function with $n > 1$ input bits. Then:*

(i) the coefficient of the monomial $x_1 \ldots x_n$ in the ANF of f is equal to $\sum_{x\in\mathbb{F}_2^n} f(x)$.

(ii) $\deg(f) \leq n-1$ if, and only if wt(f) is even.

(iii) if f is balanced, then $\deg(f) \leq n-1$.

Proof See appendix A. □

We now come out with vectorial boolean functions, *ie* having multiple, say t, output bits instead of a single one. We still denote the number of input bits by n, and we assume that $t \leq n$. If f is such a function, we will write $f_1, \ldots, f_t$ for the components of f, that of course are themselves scalar boolean functions. Balancedness generalizes very naturally and we will say that f is balanced if all $y \in \mathbb{F}_2^t$ have the same number of preimages by f in $\mathbb{F}_2^n$, that is

$$\forall y \in \mathbb{F}_2^t, \#\{x :\ x \in \mathbb{F}_2^n, f(x) = y\} = 2^{n-t}.$$

Note that it indeed forces t to be $\leq n$. We are now ready to give the

Proposition 2 *Let $1 < t \leq n$ be two integers, and $f : \mathbb{F}_2^n \to \mathbb{F}_2^t$ be a vectorial boolean function with scalar components $f_1, \ldots, f_t$. Then the following two properties are equivalent:*

(1) f is a balanced function;

(2) every nonzero linear form of the outputs of f is balanced, ie $\forall(\lambda_1, \ldots, \lambda_t) \in \mathbb{F}_2^t - \{0, \ldots, 0\}$, $x \mapsto \lambda_1 f_1(x) \oplus \ldots \oplus \lambda_t f_t(x)$ is balanced.

Proof See appendix A. □

Corollary 3 *Assume (1) or, equivalently, (2) holds in proposition 2. Then every linear form of the outputs of f is a boolean function with algebraic degree $\leq n-1$.*

Proof From proposition 2, every linear form of the outputs of f is either null, either balanced. In the latter case, lemma 1*(iii)* applies. □

We now give a result about the pointwise product of balanced boolean functions. The pointwise product of two scalar boolean functions f and g is defined by $fg : x \mapsto f(x)g(x)$. Since $\mathrm{Supp}(fg) = \mathrm{Supp}(f) \cap \mathrm{Supp}(g)$, there is no systematic relation between balancedness of fg and the one of f and g. Moreover, in the case when f and g are balanced, fg cannot be balanced unless we are in the "degenerate" case where $f = g$. Nevertheless, we are able to proove a nice result on the algebraic degree of a product of some balanced functions, provided the number of factors in the product is not too much. Let us state it precisely.

Proposition 4 *Let $1 < t \leq n$ be two integers, and $f : \mathbb{F}_2^n \to \mathbb{F}_2^t$ be a vectorial boolean function with scalar components $f_1, \ldots, f_t$. Assume that f is balanced. Then all the pointwise products $f_{i_1} \ldots f_{i_r}$, with $1 \leq i_1 < \cdots < i_r \leq t$, $1 \leq r \leq \min(t, n-1)$ have algebraic degree $\leq n-1$.*

Proof See appendix A. □

A particular case we are interested in is the one where f is bijective mapping of $\mathbb{F}_2^n$. We have the

Corollary 5 *Let f be a n-variable bijection. Then*

(i) any nonzero linear form of the f_i's,

(ii) any product of at most $n-1$ f_i's

have degree $\leq n-1$.

Proof *(i)* comes from lemma 1 and proposition 2 put together, while *(ii)* follows from proposition 4. □

4 2-round SPN

4.1 Description

Let $n = qm$ the blocksize of a SP network, each round of which is composed as follows:

- a non linear layer composed by q parallel substitutions boxes $S_1, \ldots, S_q$. Each S-box is a m-variable bijection. We assume that all S_i are the same, and we simply denote it S. The reason for this assumption is that it does not change the proof and makes it easier and lighter to read;

- a linear layer composed by a invertible linear mapping L on $\mathbb{F}_2^n$, the structure of which is not relevant for our proof.

Let $X = (x_1, \ldots, x_n)$ be the input variables. The following equations describe the 2-round SP scheme, and introduce intermediate variables $Y = (y_1, \ldots, y_n)$, $Z = (z_1, \ldots, z_n)$, $T = (t_1, \ldots, t_n)$ as well as final output $U = (u_1, \ldots, u_n)$. Each n-bit vector is naturally divided into q groups of m variables. For instance $(x_1, \ldots, x_n)$ is divided into $(x_1, \ldots, x_m)$, $(x_{m+1}, \ldots, x_{2m})$, $\ldots$, $(x_{(q-1)m+1}, \ldots, x_{qm})$, and these subvectors will be denoted $X_1, \ldots, X_q$ respectively. An analogous convention defines $Y_1, \ldots, Y_q$, $Z_1, \ldots, Z_q$, $T_1, \ldots, T_q$, and $U_1, \ldots, U_q$.

$$
\begin{array}{l}
\textbf{(First round)}\\
\textit{(Non linear layer)}\\
\qquad\left\{\begin{array}{lcl}
(y_1, \ldots, y_m) & = & S(x_1, \ldots, x_m)\\
 & \ldots & \\
(y_{(q-1)m+1}, \ldots, y_{qm}) & = & S(x_{(q-1)m+1}, \ldots, x_{qm})
\end{array}\right.\\
\textit{(Linear layer)}\\
\qquad\qquad (z_1, \ldots, z_n) = L(y_1, \ldots, y_n)\\
\textbf{(Second round)}\\
\textit{(Non linear layer)}\\
\qquad\left\{\begin{array}{lcl}
(t_1, \ldots, t_m) & = & S(z_1, \ldots, z_m)\\
 & \ldots & \\
(t_{(q-1)m+1}, \ldots, t_{qm}) & = & S(z_{(q-1)m+1}, \ldots, z_{qm})
\end{array}\right.\\
\textit{(Linear layer)}\\
\qquad\qquad (u_1, \ldots, u_n) = L(t_1, \ldots, t_n)
\end{array}
\tag{1}
$$

Λ denotes the matrix of L in the canonical basis of $\mathbb{F}_2^n$. We will make explicit use of $(\Lambda_{i,j})_{1 \leq i,j \leq q}$, that are q^2 square $m \times m$ submatrices of Λ defined by

$$
\Lambda = \begin{bmatrix} \Lambda_{1,1} & \ldots & \Lambda_{1,q} \\ \vdots & & \vdots \\ \Lambda_{q,1} & \ldots & \Lambda_{q,q} \end{bmatrix}.
$$

With all our notations, the following four writings have the same meaning:

$$(z_1, \ldots, z_n) = L(y_1, \ldots, y_n),$$

$$(z_1, \ldots, z_n) = (y_1, \ldots, y_n).\Lambda,$$

$$
\left\{\begin{array}{lcl}
Z_1 & = & Y_1.\Lambda_{1,1} \oplus \ldots \oplus Y_q.\Lambda_{q,1}\\
 & \ldots & \\
Z_q & = & Y_1.\Lambda_{1,q} \oplus \ldots \oplus Y_q.\Lambda_{q,q}.
\end{array}\right.
$$

$$
\left\{\begin{array}{lcl}
(z_1, \ldots, z_m) & = & (y_1, \ldots, y_m).\Lambda_{1,1} \oplus \ldots \oplus (y_{(q-1)m+1}, \ldots, y_{qm}).\Lambda_{q,1},\\
 & \ldots & \\
(z_{(q-1)m+1}, \ldots, z_{qm}) & = & (y_1, \ldots, y_m).\Lambda_{1,q} \oplus \ldots \oplus (y_{(q-1)m+1}, \ldots, y_{qm}).\Lambda_{q,q},
\end{array}\right.
$$

Here each vector is identified with a row-matrix, and $(y_{(i-1)m+1}, \ldots, y_{im}).\Lambda_{i,j} = Y_i.\Lambda_{i,j}$ represents a (row) vector-matrix product (with compatible sizes as easily checked).

4.2 Statement

We aim to study the algebraic degree of Y, Z, T, U as (multivariate polynomial) expression of the input variables $x_1, \ldots, x_n$. The following theorem summarizes the results, while next subsection is devoted to the proof.

Theorem 6 *Let equations (1) define a 2-round SP network with $n = qm$ variables. Put $X = (x_1, \ldots, x_n)$ the input variables, and consider Y, Z, T, U as algebraic expressions of the x_i's. Then:*

(i) $\deg(Z) = \deg(Y) \leq m - 1$*;*

(ii) $\deg(U) \leq \deg(T) \leq q(m - 1)$*;*

4.3 Proof of theorem 6

Since Z (resp. U) is linearly computed from Y (resp. T), it is clear that $\deg(Z) \leq \deg(Y)$ (resp. $\deg(U) \leq \deg(T)$). Now let us examine the degrees of Y and T.

(i) The degree of Y is $\leq m - 1$
$Y_1 = (y_1, \ldots, y_m)$ only depends on variables $x_1, \ldots, x_m$. Since S is a bijection, the degree of each y_i is $\leq m - 1$. The same argument holds for $Y_2, \ldots, Y_q$, completing the proof of the statement for Y.

The degree of Z is equal to the one of Y Each Z_i is a linear form of the Y_j (*via* the matrix Λ). But the subsets of variables x_j that are involved in expression of the Y_j are pairwise disjoint, such that terms of degree max can not cancel each other when linearly combined.

(ii) The degree of T is $\leq q(m - 1)$
We will proove that the partial degree $\deg_{X_i}(T_j)$ is $\leq m - 1$ for $1 \leq i, j \leq q$. We write the proof for $i = 1$, the general case works in a similar way.
Fix $j_0 \in \{1, \ldots, q\}$. Consider the ANF of T_{j_0} as a polynomial of variables $x_1, \ldots, x_m$ with coefficients that are themselves multivariates polynomials in variables $x_{m+1}, \ldots, x_{qm}$. Let $h(x_{m+1}, \ldots, x_{qm})$ be the coefficient of the monomial $x_1 \ldots x_m$. Now write

$$\begin{aligned} T_{j_0} &= S(Z_j) \\ &= S(Y_1.\Lambda_{1,j_0} \oplus \ldots \oplus Y_q.\Lambda_{q,j_0}) \\ &= S(S(X_1).\Lambda_{1,j_0} \oplus \ldots \oplus S(X_q).\Lambda_{q,j_0}) \\ &= S(S(x_1, \ldots, x_m).\Lambda_{1,j_0} \oplus \ldots \oplus S(x_{(q-1)m+1}, \ldots, x_{qm}).\Lambda_{q,j_0}) \qquad (2) \end{aligned}$$

Fix $x_{m+1}, \ldots, x_{qm}$ to any numerical value $x^*_{m+1}, \ldots, x^*_{qm} \in \mathbb{F}_2^{(q-1)m}$, and put

$$\begin{aligned} T^*_{j_0} = \; & S(S(x_1, \ldots, x_m).\Lambda_{1,j_0} \oplus S(x^*_{m+1}, \ldots, x^*_{2m}).\Lambda_{2,j_0} \oplus \ldots \\ & \oplus S(x^*_{(q-1)m+1}, \ldots, x^*_{qm}).\Lambda_{q,j_0}). \end{aligned}$$

The multivariate polynomial function $(x_1, \ldots, x_m) \mapsto T^*_{j_0}$ is bijective, as equation (2) easily shows that it is a composition of bijections. It follows that the degree of $T^*_{j_0}$ with respect to $x_1, \ldots, x_m$ is $\leq m - 1$. Then, the ANF of $T^*_{j_0}$ does not contain the monomial $x_1 \ldots x_m$, whose coefficient is $h(x^*_{m+1}, \ldots, x^*_{qm})$. In other words, $h(x^*_{m+1},\ldots,x^*_{qm}) = 0$. Now the crucial point is that this latest equality holds for **any** fixed numerical choice of $x^*_{m+1},\ldots,x^*_{qm}$, and therefore h is identically zero as a multivariate polynomial in the variables $x_{m+1},\ldots,x_{qm}$. We finally get that T_{j_0} is a multivariate polynomial in variables $x_1,\ldots,x_n$ whose partial degree with respect to the first group $X_1 = (x_1,\ldots,x_m)$ of variables is $\leq m-1$, *ie* that does not contain any monomial in which the variables $x_1,\ldots,x_m$ all appear.

An identical argument prooves that, in fact, T_{j_0} has partial degree $\leq m-1$ with respect to every group X_i, $i = 1,\ldots,q$. In other words, the ANF of T_{j_0} does not contain any monomial in which all the variables of a given group X_i appear, for any $i = 1,\ldots,q$. It finally follows that the ANF of T_{j_0} does not contain any monomial whose total degree strictly exceeds $q(m-1)$, and that completes the proof of the statement for T.

4.4 What about going further ?

We briefly explain the reason why the argument collapses at round 3. We have, for example

$$U_1 = T_1.\Lambda_{1,1} \oplus \ldots \oplus T_q.\Lambda_{q,1}$$

We have proved, as intermediate steps of previous lines, that $X_1 \mapsto T_1$, ..., $X_1 \mapsto T_q$ are bijective mappings, but there is no reason that their sum should still be a bijective mapping (the only property that is preserved by summing bijective mappings altogether is that their degree remains $\leq m-1$). In other words, the mapping

$$X_1 \mapsto S(U_1) = S(T_1.\Lambda_{1,1} \oplus \ldots \oplus T_q.\Lambda_{q,1})$$

can be non bijective, and then can contain monomials of (maximal) degree m. The only upper bound we can easily deduce is that the degree of the global 3-round SP output is $\leq qm-1$, since the global SP is bijective and hence balanced. Actually, we performed experiments on toy examples and they showed that the latter bound can be reached.

5 3-round Feistel

5.1 Description

Let $n = 2m$ be an even integer. Define the following 3-round Feistel on n-bit blocks:

$$\begin{array}{ll} \hline L_1 = R_0, & R_1 = L_0 \oplus f(R_0), \\ L_2 = R_1, & R_2 = L_1 \oplus g(R_1), \\ L_3 = R_2, & R_3 = L_2 \oplus h(R_2). \\ \hline \end{array} \tag{3}$$

where the 3 round functions f, g, h are assumed to be m-variable bijections. We set

$$\begin{array}{rcl} (L_0, R_0) & = & (x_1,\ldots,x_n), \\ (L_1, R_1) & = & (y_1,\ldots,y_n), \\ (L_2, R_2) & = & (z_1,\ldots,z_n), \\ (L_3, R_3) & = & (t_1,\ldots,t_n). \end{array}$$

Throughout this section, the "algebraic degree" of any expression is meant with respect to - explicit or implicit - variables $x_1, \ldots, x_n$ in the algebraic expansion of the expression.

5.2 Statement

We aim to study the algebraic degree of (L_i, R_i)'s as (multivariate polynomial) expression of the input variables $x_1, \ldots, x_n$. Since $L_i = R_{i-1}$, it suffices of course to study the degree of the R_i's. The following theorem summarizes the results, while next subsection is devoted to the proof. Some remarks mention results for partial degrees (with respect to $x_1, \ldots, x_m$ on one hand, and $x_{m+1}, \ldots, x_{2m}$ on the other hand) of the R_i's.

Theorem 7 *Let equations (3) define a 3-round Feistel scheme with $n = 2m$ variables. Put $(L_0, R_0) = (x_1, \ldots, x_n)$, and consider R_1, R_2, R_3 as algebraic expressions of the x_i's. Then:*

(i) $\deg(R_1) \leq m - 1$*;*

(ii) $\deg(R_2) \leq 2m - 3$*;*

(iii) $\deg(R_3) \leq 2m - 2$*;*

5.3 Proof of theorem 7

(i) The degree of R_1 is $\leq m - 1$
We have

$$(y_{m+1}, \ldots, y_{2m}) = (x_1, \ldots, x_m) \oplus f(x_{m+1}, \ldots, x_{2m}), \tag{4}$$

ie

$$\left\{ \begin{array}{rcl} y_{m+1} & = & x_1 \oplus f_1(x_{m+1}, \ldots, x_{2m}) \\ \cdots & & \\ y_{2m} & = & x_m \oplus f_m(x_{m+1}, \ldots, x_{2m}) \end{array} \right. \tag{5}$$

f is a m-variable bijection, hence each f_i has degree $\leq m - 1$ (corollary 5) and therefore, each $y_i,\ i = m+1, \ldots, 2m$ has itself degree $\leq m - 1$.

Remark. Results for partial degrees can be established here directly from the algebraic expression of R_1. We have:

$$\begin{array}{rcl} \deg_{x_1, \ldots, x_m}(R_1) & = & 1, \\ \deg_{x_{m+1}, \ldots, x_{2m}}(R_1) & = & \max(\deg(f_1), \ldots, \deg(f_m)) \leq m - 1. \end{array}$$

(ii) The degree of R_2 is $\leq 2m - 3$
We compute R_2 as a function of x_i's. We have

$$\begin{array}{rcl} (z_{m+1}, \ldots, z_{2m}) & = & (y_1, \ldots, y_m) \oplus g(y_{m+1}, \ldots, y_{2m}) \\ & = & (x_{m+1}, \ldots, x_{2m}) \oplus g((x_1, \ldots, x_m) \oplus f(x_{m+1}, \ldots, x_{2m})) \end{array}$$

ie

$$\left\{ \begin{array}{rcl} z_{m+1} & = & x_{m+1} \oplus g_1((x_1, \ldots, x_m) \oplus f(x_{m+1}, \ldots, x_{2m})) \\ \cdots & & \\ z_{2m} & = & x_{2m} \oplus g_m((x_1, \ldots, x_m) \oplus f(x_{m+1}, \ldots, x_{2m})) \end{array} \right. \tag{6}$$

Let us examine the expression of z_{m+k}, for $k = 1, \ldots, m$. Since g is a m-variable bijection, each $g_k,\ k = 1, \ldots, m$ is balanced and its ANF only contains terms of degree $\leq m-1$. Write

$$g_k(\xi_1, \ldots, \xi_m) = \sum_{0 \leq r \leq m-1} \sum_{1 \leq i_1 < \cdots < i_r \leq m} \alpha^{(k)}_{i_1,\ldots,i_r} \xi_{i_1} \ldots \xi_{i_r}$$

where $r = 0$ corresponds to the constant term $g_k(0, \ldots, 0)$. We derive

$$\begin{aligned} & g_k((x_1, \ldots, x_m) \oplus f(x_{m+1}, \ldots, x_{2m})) \\ &\quad = \quad g_k(x_1 \oplus f_1(x_{m+1}, \ldots, x_{2m}), \ldots, x_m \oplus f_m(x_{m+1}, \ldots, x_{2m})) \\ &\quad = \quad \sum_{0 \leq r \leq m-1} \sum_{1 \leq i_1 < \cdots < i_r \leq m} \alpha^{(k)}_{i_1,\ldots,i_r} \\ &\qquad\quad (x_{i_1} \oplus f_{i_1}(x_{m+1}, \ldots, x_{2m})) \ldots (x_{i_r} \oplus f_{i_r}(x_{m+1}, \ldots, x_{2m})) \end{aligned} \tag{7}$$

A basic development of the right hand side raises terms of the form

$$x_{i_1} \ldots x_{i_r} f_{j_1}(x_{m+1}, \ldots, x_{2m}) \ldots f_{j_s}(x_{m+1}, \ldots, x_{2m}) \tag{8}$$

with

$$\begin{cases} 1 \leq i_1 < \cdots < i_r \leq m, \\ 1 \leq j_1 < \cdots < j_s \leq m, \\ r + s \leq m - 1. \end{cases}$$

The degree of each f_j is $\leq m-1$ because f is bijective. The same holds for the products of f_j's, because there are $s \leq m-1$ factors f_j's and thus corollary 5 applies. We get the following upper bound for the degree of each term (8):

- if $s = 0$, then $r \leq m-1$ and

$$\deg(\textit{term } (8)) = r \leq m-1;$$

- if $s = 1$, then $r \leq m-2$ and

$$\deg(\textit{term } (8)) \leq r + \deg(f_{j_1}) \leq (m-2) + (m-1) = 2m-3;$$

- if $s \geq 2$, then $r \leq m-3$ and

$$\deg(\textit{term } (8)) \leq r + \deg(\text{product of several } f_j\text{'s}) \leq (m-3)+(m-1) = 2m-4.$$

We have proved that $\deg(g_k((x_1, \ldots, x_m) \oplus f(x_{m+1}, \ldots, x_{2m}))) \leq 2m-3$, and so is $\deg(z_{m+k})$, for $k = 1, \ldots, m$. That completes the proof of the statement for R_2.

Remark. Consider equation (6) and write it in the following compact form :

$$R_2 = R_0 \oplus g(L_0 \oplus f(R_0)).$$

If we fix R_0, the partial function $L_0 \mapsto R_0 \oplus g(L_0 \oplus f(R_0))$ is bijective on $\mathbb{F}_2^m$ because g is. Hence its degree (more exactly, the degree of each of its scalar component) is less than $m-1$. In similar way, if we now fix L_0, the partial function $R_0 \mapsto g(L_0 \oplus f(R_0))$, is bijective on $\mathbb{F}_2^m$ because g and f are. Hence its degree is $\leq m-1$, and so is the degree of $R_0 \mapsto R_0 \oplus g(L_0 \oplus f(R_0))$. We conclude:

$$\begin{aligned} \deg_{x_1,\ldots,x_m}(R_2) &\leq m-1, \\ \deg_{x_{m+1},\ldots,x_{2m}}(R_2) &\leq m-1 \end{aligned}$$

Hence any monomial of R_2 cannot contain the whole "left" (nor "right") variables, *ie* no monomial is multiple of $x_1 \ldots x_m$ (nor multiple of $x_{m+1} \ldots x_{2m}$). What is remarkable from the upper bound for total degree of R_2 is that whenever $m-1$ "left" (resp. "right") variables appear in a given monomial, then at most $m-2$ "right" (resp. "left") ones appear in the same monomial. In other words, there is no monomial containing $m-1$ left variables and $m-1$ right variables simultaneously.

(iii) The degree of R_3 is $\leq 2m-2$
We have

$$(t_{m+1}, \ldots, t_{2m}) = (z_1, \ldots, z_m) \oplus h(z_{m+1}, \ldots, z_{2m}) \tag{9}$$

ie

$$\left\{ \begin{array}{rcl} t_{m+1} &=& z_1 \oplus h_1(z_{m+1}, \ldots, z_{2m}) \\ \cdots && \\ t_{2m} &=& z_m \oplus h_m(z_{m+1}, \ldots, z_{2m}) \end{array} \right. \tag{10}$$

Note that $z_1, \ldots, z_m$ are degree $\leq m-1$, because of the bound on R_1 and $R_1 = L_2 = (z_1, \ldots, z_m)$. Hence, to proove the statement, it suffices to proove that $h_k(z_{m+1}, \ldots, z_{2m})$, for $k = 1, \ldots, m$, have degree $\leq 2m-2$ (recall that the degree of any expression is meant with respect to the – implicit – variables x_i's). We will use the same strategy as previously. Actually, it will not work exactly in the same way, and will require some refinement.
First we "slide" expression (7) one round forward. What we mean is that (7) is still valid when moving:

- x_i to y_i;
- g_k to h_k (and moving the α's coefficients to some new ones, say β's);
- f_i to g_i.

This rewriting gives

$$\begin{aligned} & h_k(y_1 \oplus g_1(y_{m+1}, \ldots, y_{2m}), \ldots, y_m \oplus g_m(y_{m+1}, \ldots, y_{2m})) \\ & \quad = \quad h_k(0, \ldots, 0) \oplus \sum_{1 \leq r \leq m-1} \; \sum_{1 \leq i_1 < \cdots < i_r \leq m} \beta^{(k)}_{i_1,\ldots,i_r} \\ & \qquad\qquad (y_{i_1} \oplus g_{i_1}(y_{m+1}, \ldots, y_{2m})) \ldots (y_{i_r} \oplus g_{i_r}(y_{m+1}, \ldots, y_{2m})) \end{aligned} \tag{11}$$

Then we have to examine terms of the form

$$y_{i_1} \ldots y_{i_r} g_{j_1}(y_{m+1}, \ldots, y_{2m}) \ldots g_{j_s}(y_{m+1}, \ldots, y_{2m}) \tag{12}$$

with

$$\left\{ \begin{array}{l} 1 \leq i_1 < \cdots < i_r \leq m, \\ 1 \leq j_1 < \cdots < j_s \leq m, \\ r + s \leq m-1. \end{array} \right.$$

In the previous case, the crucial point was that the factors $x_{i_1}\cdot\ldots\cdot x_{i_r}$ and the factors $f_{j_1}(x_{m+1},\ldots,x_{2m})\ldots f_{j_s}(x_{m+1},\ldots,x_{2m})$ have separate groups of variables x_i – more precisely, the former only contain variables $x_1,\ldots,x_m$ although the latter only contain variables $x_{m+1},\ldots,x_{2m}$. As $(y_1,\ldots,y_m) = (x_{m+1},\ldots,x_{2m})$ this separation no longer holds, and if we expand the left hand side of (11) with respect to the variables x_i, all of them would be mixed altogether. Indeed, if the previous strategy could be applied in the same way, we would get that the degree of (11) is $\leq 2m-3$, which is not compliant to what we are aiming to proove[1].

Let us express the terms (12) with respect to variables x_i's. Using (4) and $(y_1,\ldots,y_m) = (x_{m+1},\ldots,x_{2m})$, we get expressions of the form

$$\begin{aligned} & x_{m+i_1}\ldots x_{m+i_r}\ [g_{j_1}\ldots g_{j_s}]((x_1,\ldots,x_m)\oplus f(x_{m+1},\ldots,x_{2m})) \\ & \quad = x_{m+i_1}\ldots x_{m+i_r}\ g^*((x_1,\ldots,x_m)\oplus f(x_{m+1},\ldots,x_{2m})) \end{aligned} \tag{13}$$

with

$$\begin{cases} 1\leq i_1<\cdots<i_r\leq m, \\ 1\leq j_1<\cdots<j_s\leq m, \\ r+s\leq m-1. \end{cases}$$

Here $g^* = g_{j_1}\ldots g_{j_s}$ denotes the pointwise product of the functions $g_{j_1},\ldots,g_{j_s}$. The new trick here is that we apply corollary 5 to both product of several g_j's and f_i's, since f and g are bijections : the pointwise products $[f_{\ell_1}\ldots f_{\ell_t}]$, with $t\leq m-1, 1\leq \ell_1<\cdots<\ell_t\leq m$ are m-variable functions with degree $\leq m-1$, and so is g^*, as the product of $s\leq m-1$ functions g_i's.

Now write

$$g^*(\xi_1,\ldots,\xi_m) = \sum_{0\leq s\leq m-1}\ \sum_{1\leq k_1<\cdots<k_s\leq m} \gamma_{k_1,\ldots,k_s}\xi_{k_1}\ldots\xi_{k_s},$$

where $s=0$ corresponds to the constant term $g^*(0,\ldots,0)$. Then (13) becomes

$$\begin{aligned} & x_{m+i_1}\ldots x_{m+i_r} \sum_{0\leq s\leq m-1}\ \sum_{1\leq k_1<\cdots<k_s\leq m} \gamma_{k_1,\ldots,k_r}(x_{k_1}\oplus f_{k_1}(x_{m+1},\ldots,x_{2m}))\ldots \\ & \qquad\qquad (x_{k_s}\oplus f_{k_s}(x_{m+1},\ldots,x_{2m})) \\ = \quad & x_{m+i_1}\ldots x_{m+i_r} \sum_{0\leq s\leq m-1}\ \sum_{1\leq k_1<\cdots<k_s\leq m} \gamma_{k_1,\ldots,k_s}\left(\sum_{0\leq t\leq s}\right. \\ & \qquad \left.\sum_{(\ell_1,\ldots,\ell_s)\in\mathcal{S}(k_1,\ldots,k_s)} x_{\ell_1}\ldots x_{\ell_t}\ [f_{\ell_{t+1}}\ldots f_{\ell_s}](x_{m+1},\ldots,x_{2m})\right) \\ = \quad & \sum_{0\leq s\leq m-1}\ \sum_{1\leq k_1<\cdots<k_s\leq m} \gamma_{k_1,\ldots,k_s}\left(\sum_{0\leq t\leq s}\right. \\ & \qquad \left.\sum_{(\ell_1,\ldots,\ell_s)\in\mathcal{S}(k_1,\ldots,k_s)} x_{\ell_1}\ldots x_{\ell_t}\ x_{m+i_1}\ldots x_{m+i_r}\ [f_{\ell_{t+1}}\ldots f_{\ell_s}](x_{m+1},\ldots,x_{2m})\right) \end{aligned} \tag{14}$$

[1] The upper bound that we target corresponds to our observations on a toy example, hence is tight.

with
$$\begin{cases} 1 \le i_1 < \cdots < i_r \le m, \\ 1 \le j_1 < \cdots < j_s \le m, \\ 1 \le \ell_1, \ldots, \ell_s \le m, \ \ell_i \text{ pairwise distinct}, \\ r + s \le m - 1, \\ t \le s. \end{cases}$$

The summation $\sum_{(\ell_1,\ldots,\ell_s)\in\mathcal{S}(k_1,\ldots,k_s)}$ ranges over all s-tuples for which the ℓ_i's are pairwise disjoint and the set $\{\ell_1, \ldots, \ell_s\}$ is equal to the set $\{k_1, \ldots, k_s\}$. The terms appearing in (14) have the form:

$$x_{\ell_1} \ldots x_{\ell_t} \ x_{m+i_1} \ldots x_{m+i_r} \ [f_{\ell_{t+1}} \cdots f_{\ell_s}](x_{m+1}, \ldots, x_{2m}) \qquad (15)$$

which we will be refered as "*term* (15)". Let us examine their degree:

- if $r = 0$, then $\deg([f_{\ell_{t+1}} \cdots f_{\ell_s}](x_{m+1}, \ldots, x_{2m})) \le m - 1$, because $s - t \le m - 1$ and corollary 5. Hence,

$$\begin{aligned} \deg(\textit{term}\ (15)) &= t + \deg([f_{\ell_{t+1}} \cdots f_{\ell_s}](x_{m+1}, \ldots, x_{2m})) \\ &\le (m-1) + (m-1) \\ &= 2m - 2; \end{aligned}$$

- if $r \ge 1$, then on one hand $t \le s \le m - 1 - r \le m - 2$ and, on the other hand,

$$\deg(x_{m+i_1} \ldots x_{m+i_r} \ [f_{\ell_{t+1}} \cdots f_{\ell_s}](x_{m+1}, \ldots, x_{2m})) \le m$$

  because the degree of any multivariate polynomial expression is always upper bounded by the number of variables. Hence,

$$\begin{aligned} \deg(\textit{term}\ (15)) &= t + \deg(x_{m+i_1} \ldots x_{m+i_r} \ [f_{\ell_{t+1}} \cdots f_{\ell_s}](x_{m+1}, \ldots, x_{2m})) \\ &\le (m-2) + m \\ &= 2m - 2. \end{aligned}$$

That completes the proof of the statement for R_3.

Remark Expression of R_3 with respect to (L_0, R_0) is

$$\begin{aligned} R_3 &= R_1 \oplus h(L_1 \oplus g(R_1)) \\ &= L_0 \oplus f(R_0) \oplus h(R_0 \oplus g(L_0 \oplus f(R_0))) \end{aligned}$$

If we fix R_0, the partial function $L_0 \mapsto f(R_0)$ (resp. $L_0 \mapsto h(R_0 \oplus g(L_0 \oplus f(R_0)))$) is a bijection on $\mathbb{F}_2^m$ beacause f is (resp. beacause g and h are). Hence both functions have degree $\le m-1$, and their sum $L_0 \mapsto R_3$ has also degree $\le m-1$, that is

$$\deg_{x_1,\ldots,x_m} R_3 \le m - 1.$$

Now if we fix L_0, the partial function $R_0 \mapsto g(L_0 \oplus f(R_0))$ is a bijection on $\mathbb{F}_2^m$, hence has degree $\le m - 1$. Therefore, $R_0 \mapsto R_0 \oplus g(L_0 \oplus f(R_0))$ has itself degree $\le m - 1$, but is no longer a bijection so that there is no reason *a priori* why $R_0 \mapsto h(R_0 \oplus g(L_0 \oplus f(R_0)))$ should be a bijection and should have degree $\le m-1$. Indeed, in the experiments we performed, there were some cases where the partial degree was m.

It is even more remarkable that degree of R_3 is $\le 2m - 2$. The facts, that we encountered during the proof and that we want to stress out here, are that

- in any monomial, there are at most $m-1$ "left" variables that appear;
- there are some monomials multiples of $x_{m+1} \dots x_{2m}$, but whenever it occurs, there are at most $m-2$ "left" variables appearing in the monomial.

It is also the reason why it is impossible to go further in the sequent rounds. For a 4-round Feistel, the only upper bound we can obtain is that the degree of the output is $\leq 2m-1$, since the global Feistel function is bijective. Actually, we performed experiments on toy examples and they showed that the bound can be reached.

6 Distinguishing aspects

One can be tempted to use the various results on what we could call the "degree profile" to distinguish a reduced round Feistel or SP scheme from a random function. Indeed, a random function with n variables has degree n with probability 1/2. Of course, the relevance of the distinguishing issue makes sense if one targets to distinguish the scheme from a **balanced** random function. In this case, the degree cannot exceed $n-1$, and since there are n monomials with degree $(n-1)$, the probability for a balanced random function to have degree exactly $n-1$ is equal to $1-2^{-n}$. A similar argument shows that the probability degree exactly $n-2$ is $1-2^{-n-\binom{n}{2}}$. These probabilities values are very close to 1, such that false alarms when applying this distinguisher is of negligible probability.
Unfortunately, the results strongly make use of the ANF ceofficients of the global function, especially the "high-weight" coefficients, that is to say those of monomials of degree n and $n-1$.
The correspondance formulas between values and ANF coefficients are recalled in section 2. If one examines them carefully, they stress that, given $u \in \mathbb{F}_2^n$, the ANF coefficient a_u only depends on the values $f(x)$, where $x \preceq u$. We can say in a certain manner that some ANF coefficients can be computed from a sample of the list of values of f. But, as this "sample" is reduced enough for coefficients of monomial of very low degree, it grows as the degree of the targetted monomial does. And finally, the computation of the degree-n monomial coefficient requires the complete list of values. Besides, the following combinatorial argument prooves that there cannot exist any trick to get rid of this feature.

> Assume that there exist a "sampling" subset S such that the degree-n monomial coefficient of f, say c, can be computed from the (sampled list of) values $f(x),\ x \in S$. On the other hand, we still always have
>
> $$c = \sum_{x \in \mathbb{F}_2^n} f(x)$$
>
> Now choose any $x_0 \notin S$ and flip the corresponding value of f. Then c is itself flipped and the degree of the function is flipped from n to some integer $\leq n-1$, or conversely. It follows as an evidence that the degree f cannot be computed from any sampling subset, a contradiction.

The complexity of all our work seems to be basically lower bounded by the (pre-)computation of the ANF form of the scheme. This is well-known to be feasible in $O(n2^n)$ (by a recursive form of the Mobius transform, similar to fast Discrete Fourier Transform). It turns to be obviously irrelevant since it is greater than the complexity $O(2^n)$ of computing the whole dictionnary of the function. In any case, it cannot compete with the most significant results of the quoted references propose distinguishers, which complexities vary from $O(2^{n/2})$ to $O(2^{3n/4})$, depending on the number of rounds and the model of adversary.
Nevertheless, at this point we have not investigated yet the possibility that some relation between the n degree-$(n-1)$ coefficients altogether could be exhibited using an appropriate sampling subset of the values of f. This could be a way for further research. Another direction to investigate comes from examining the partial degrees with respect to some subset of variables (e.g. "left" or "right" subset for a Feistel scheme), to distinguish Feistel or SP schemes from random functions. For example, in the case of Feistel schemes, the partial function w.r.t. "left" variables deals with monomials which degree is at most $n/2$, and the complexity to retrieve the ANF coefficients is $O(n2^{n/2})$. The latter complexity is significantly lower than $O(n2^n)$, and has same order of magnitude as literature's complexities.
Finally, we believe that the same kind of degree-distinguishing can be made efficient if we deal with unbalanced Feistel schemes, as in [4].

References

[1] Luby M., Rackoff C., How to construct pseudorandom permutations from pseudorandom functions, SIAM Journal of Computing, vol. 17, N.2, pp. 373–386, April 1998.

[2] Patarin J., Generic Attacks on Feistel Schemes. Asiacrypt'01 (Lecture Notes on Computer Science 2248), pp. 222–238, Springer.

[3] Patarin J., Security of Random Feistel Schemes with 5 or more Rounds, Crypto'04 (Lecture Notes on Computer Science 3152), pp. 106–122, Springer

[4] Patarin J., Nachef V., Berbain C., Generic Attacks on Feistel Schemes with Expanding Functions,

[5] Patarin J., Generic Attacks on Feistel Schemes, e-print 2008/036.

A Proof of the results on boolean functions

A.1 Proof of lemma 1

(i) follows from the Mobius inversion applied to $u = (1, \ldots, 1)$. *(ii)* is an easy consequence of *(i)*, since the summation contains $wt(f)$ terms equal to 1 and $2^n - wt(f)$ terms equal to 0. *(iii)* follows - again elementarily - from *(ii)* (recall that $n > 1$ by assumption), but, of course, its converse may not be true.

A.2 Proof of proposition 2

The proof relies on the use the Fourier and Walsh transform. First recall that the Fourier transform $\widehat{f}$ of a n-variable scalar boolean function f is defined by

$$\forall v \in \mathbb{F}_2^n \ \widehat{f}(v) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{x.v}$$

where the computation is performed over the ring of integers, and that we have the Fourier inversion formula:

$$\forall x \in \mathbb{F}_2^n, \ f(x) = 2^{-n} \sum_{v \in \mathbb{F}_2^n} \widehat{f}(v)(-1)^{x.v}$$

The Walsh transform $\tilde{f}$ of a scalar boolean function f is defined as the Fourier transform of the sign function $(-1)^f$.

$$\forall v \in \mathbb{F}_2^n \ \tilde{f}(v) = \widehat{(-1)^f}(v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x.v}.$$

The following lemma is straightforward, and we skip its proof.

Lemma 8 *The scalar boolean function f is balanced if and only if $\tilde{f}(0) = 0$.*

Now let us come to the proof of proposition 2.
(i) ⇒ (ii). Let $\lambda = (\lambda_1, \ldots, \lambda_t) \in \mathbb{F}_2^t - \{0\}$. We have

$$\begin{aligned} \widetilde{\lambda.f}(0) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{\lambda.f(x)} = \sum_{y \in \mathbb{F}_2^t} (\#f^{-1}(y)) \ (-1)^{\lambda.y} \\ &= 2^{n-t} \sum_{y \in \mathbb{F}_2^t} (-1)^{\lambda.y} = 0, \end{aligned}$$

as desired.
(ii) ⇒ (i). Define $g : \mathbb{F}_2^t \to \mathbb{Z}$, by $y \mapsto \#f^{-1}(y)$. Let us compute the Fourier transform of g. For $\lambda \neq 0$, we have by assumption $\lambda.f$ is balanced, then by lemma 8 $\widetilde{\lambda.f}(0) = 0$, and hence

$$\widehat{g}(\lambda) = \sum_{y \in \mathbb{F}_2^t} (\#f^{-1}(y)) \ (-1)^{\lambda.y} = \sum_{x \in \mathbb{F}_2^n} (-1)^{\lambda.f(x)} = \widetilde{\lambda.f}(0) = 0.$$

On the other hand, $\widehat{g}(0) = \sum_{y \in \mathbb{F}_2^t} \#f^{-1}(y) = \#\mathbb{F}_2^n = 2^n$. It follows, by Fourier inversion formula, that

$$\forall y \in \mathbb{F}_2^t, \ \#f^{-1}(y) = g(y) = 2^{-t} \sum_{\lambda \in \mathbb{F}_2^t} \widehat{g}(\lambda)(-1)^{\lambda.y} = 2^{n-t},$$

as desired.

A.3 Proof of proposition 4

We actually proof that,

$$\begin{aligned} &\forall 1 \leq i_1 < \cdots < i_r \leq t, \ \text{with } 1 \leq r \leq \min(t, n-1), \\ &\text{the support of } f_{i_1} \ldots f_{i_r}(x) = 1 \text{ has cardinality } 2^{n-r}. \end{aligned} \tag{16}$$

It will give the expected conclusion applying *(ii)* of lemma 1, noting that $r \leq \min(t, n-1)$ *de facto* implies 2^{n-r} is even.
We would like to propose two different proofs. Both use combinatorial arguments. The first one is much simpler mainly exploit the vectorial structure of the function f. The second one is more tricky, it only considers the scalar components $f_1, \dots, f_t$ by themselves, and makes a nice use of inclusion-exclusion-like argument (what motivated us to propose it as well).

First proof

Fix $1 \leq i_1 < \cdots < i_r \leq t$, with $1 \leq r \leq \min(t, n-1)$. Consider the "subfunction" $f^* : \mathbb{F}_2^n \to \mathbb{F}_2^r,\ x \mapsto (f_{i_1}(x), \dots f_{i_r}(x))$: it is itself balanced, as it is easy to see appyling criterion (2) of proposition 2.
Now, an element $x \in \mathbb{F}_2^n$ satisfies $[f_{i_1} \dots f_{i_r}](x) = 1$ if, and only if $f_{i_1}(x) = \cdots = f_{i_r}(x) = 1$, that is, if $f^*(x)$ is the "all one" vector $(1, \dots, 1) \in \mathbb{F}_2^r$. Hence the support of $f_{i_1} \dots f_{i_r}$ is $f^{*\ -1}((1, \dots, 1)$ and, since f^* is balanced, contains 2^{n-r} elements.

Second proof

The basic point of the proof is the following

Lemma 9 *(i) Basic version: let g and h two n-variable scalar boolean functions. Then*

$$wt(f \oplus g) = wt(f) + wt(g) - 2wt(fg)$$

(ii) Iterative version: let $g_1, \dots, g_s$ be s n-variable scalar boolean functions. Then

$$\begin{aligned} wt(g_1 \oplus \ldots \oplus g_s) &= \sum_{1 \leq k \leq s} wt(g_k) - 2 \sum_{1 \leq k_1 < k_2 \leq s} wt(g_{k_1} g_{k_2}) \\ &\quad +4 \sum_{1 \leq k_1 < k_2 < k_3 \leq s} wt(g_{k_1} g_{k_2} g_{k_3}) \\ &\quad \cdots + (-2)^{s-1} wt(g_1 \dots g_s) \end{aligned}$$

Proof *(i)* It is clear by a inclusion-exclusion principle that

$$\begin{aligned} \mathrm{Supp}(f \oplus g) &= (\mathrm{Supp}(f) \cup \mathrm{Supp}(g)) - (\mathrm{Supp}(f) \cap \mathrm{Supp}(g)) \\ &= (\mathrm{Supp}(f) \cup \mathrm{Supp}(g)) - \mathrm{Supp}(fg) \end{aligned}$$

from which conclusion follows immediately. *(ii)* follows recursively from *(i)*. □

Now, assume that condition *(ii)* holds in proposition 4. We proove (16) by strong induction on r.
The result holds for $r = 1$ because of condition *(ii)*. Assume that the result holds up to $r-1$, that is every product of $s \leq r-1$ f_i's has weight 2^{n-s}. Apply lemma 9*(ii)* with $g_k = f_{i_k}$ and $s = r$:

$$\begin{aligned} wt(f_{i_1} \oplus \ldots \oplus f_{i_r}) &= \sum_{1 \le k \le r} wt(f_{i_k}) - 2 \sum_{1 \le k_1 < k_2 \le r} wt(f_{i_{k_1}} f_{i_{k_2}}) \\ &+4 \sum_{1 \le k_1 < k_2 < k_3 \le r} wt(f_{i_{k_1}} f_{i_{k_2}} f_{i_{k_3}}) \\ &+ \cdots + (-2)^{r-1} wt(f_{i_1} \ldots f_{i_r}) \end{aligned}$$

Using induction hypothesis, we get:

$$\begin{aligned} 2^{n-1} &= \binom{r}{1} 2^{n-1} - 2\binom{r}{2} 2^{n-2} + \binom{r}{3} (-2)^2 2^{n-2} \\ &+ \cdots + \binom{r}{r-1} (-2)^{r-2} 2^{n-r+1} \\ &+(-2)^{r-1} wt(f_{i_1} \ldots f_{i_r}) \end{aligned}$$

such that,

$$2^{n-1}(1 - \binom{r}{1} + \binom{r}{2} - \binom{r}{3} + \cdots + (-1)^{r-1} \binom{r}{r-1}) = (-2)^{r-1} wt(f_{i_1} \ldots f_{i_r})$$

which gives the desired

$$wt(f_{i_1} \ldots f_{i_r}) = 2^{n-r}$$

since $1 - \binom{r}{1} + \binom{r}{2} - \binom{r}{3} + \cdots + (-1)^{r-1}\binom{r}{r-1} + (-1)^r = 0$.
Since $s \le r \le \min(t, n-1) < n$, 2^{n-r} is a even integer and we conclude in the same way as in the first proof.

Remark

It is easy, using same kind of tricks, to deal with the case where f is a bijection, and $r = n$: the support of $f_1 \ldots f_n$ is reduced to a single point, precisely the element $f^{-1}(1, \ldots, 1)$.