Designs, Codes and Cryptography, 16, 121–149 (1999)

Correlation-Immune and Resilient Functions Over a Finite Alphabet and Their Applications in Cryptography

PAUL CAMION[*] paul.camion@inria.fr
ANNE CANTEAUT[**] anne.canteaut@inria.fr
INRIA Projet Codes, Domaine de Voluceau, 78153 Le Chesnay Cedex, FRANCE

Communicated by: D. Jungnickel
Received January 16, 1997; Revised May 28, 1998; Accepted June 10, 1998

Abstract. We extend the notions of correlation-immune functions and resilient functions to functions over any finite alphabet. A previous result due to Gopalakrishnan and Stinson is generalized as we give an orthogonal array characterization, a Fourier transform and a matrix characterization for correlation-immune and resilient functions over any finite alphabet endowed with the structure of an Abelian group. We then point out the existence of a tradeoff between the degree of the algebraic normal form and the correlation-immunity order of any function defined on a finite field and we construct some infinite families of t-resilient functions with optimal nonlinearity which are particularly well-suited for combining linear feedback shift registers. We also point out the link between correlation-immune functions and some cryptographic objects as perfect local randomizers and multipermutations.

Keywords: correlation-immune functions, resilient functions, orthogonal arrays, pseudo-random generators, multipermutations

1. Introduction

Resilient functions were introduced independently by Chor *et al.* [11] and Bennett, Brassard and Robert [1]; they were originally applied respectively to the generation of random strings in presence of faulty processors and to key distribution especially for quantum cryptography. Several other applications afterwards emerged and the theory of resilient functions (or the equivalent combinatorial structure of orthogonal arrays) is now almost omnipresent in cryptography.

These functions are first of all used for designing running-keys for stream ciphers; in the common case, the running-key generator is composed of several linear feedback shift registers combined by a Boolean function. This combining function should then be a correlation-immune function in order to resist Siegenthaler's correlation attack [36]; a resilient function is usually chosen so that the output digits are uniformly distributed. Its algebraic normal form should additionally have a high degree so that the resulting pseudo-random sequence has a high linear complexity. In a more general view, Maurer and Massey [25] showed that an additive stream cipher can be provably-secure under the restriction that the number of plaintext digits that the enemy can obtain is limited: the running-key generator thus should be a perfect local randomizer, what is equivalent to the structure of an orthogonal

[*] Centre National de la Recherche Scientifique
[**] Grant-holder from the DRET

array. Another application consists in designing "conventional" cryptographic primitives, *i.e.* primitives based on a network with some boxes. Such a network contains both confusion boxes for hiding any structure and diffusion boxes for merging several inputs. Schnorr and Vaudenay [32] recommend that the diffusion boxes should be functions realizing perfect diffusion in order to avoid some cryptanalysis, especially collision attacks. These functions are called multipermutations and they can be deduced from orthogonal arrays of maximal strength. These objects are also used in threshold schemes for secret sharing.

In this paper we extend the notions of correlation-immune functions and resilient functions to functions over any finite alphabet. We generalize in Section 2 the characterizations of q-ary resilient functions given by Gopalakrishnan and Stinson [18]: we give an orthogonal array characterization, a characterization by means of characters (similar to a Fourier transform characterization) when the alphabet is endowed with the structure of an Abelian group and a matrix characterization. We then study in Section 3 the properties of the algebraic normal form of correlation-immune functions over a finite field. We here show that there is a tradeoff between the nonlinearity order and the correlation-immunity order of any q-ary function and we obtain an inequality involving both degree and correlation-immunity order of the function which generalizes Siegenthaler's inequality for Boolean functions [35]. Following this result we construct a family of t-resilient functions with optimal nonlinearity over some finite fields, which are well-suited for combining LFSRs. We also give in Section 4 a new construction of resilient functions by composition of resilient functions of smaller order; this construction can immediately be applied to the combination of linear feedback shift registers. Section 5 then points out the link between correlation-immune functions and several other cryptographic notions. We generalize the concept of perfect local randomizers introduced by Maurer and Massey. We also apply the previous results to perfect diffusion boxes used for designing cryptographic primitives. Thanks to the equivalence between multipermutations and correlation-immune functions we give a bound on the diffusion performed at the binary level by a multipermutation over $\mathbf{F}_{2^m}$.

2. Three characterizations of correlation-immune functions over a finite alphabet

Let $\mathcal{F}$ denote a finite alphabet with q elements ($q \geq 2$) and E be a finite set. Let $f : \mathcal{F}^n \rightarrow E$ be a function and let $\{X_1, X_2, ..., X_n\}$ be a set of random input variables assuming values from $\mathcal{F}$ with independent uniform distributions (*i.e.* every input vector occurs with probability $\frac{1}{q^n}$).

The function f may satisfy the following properties:

- f is *balanced* if the random variable $Y = f(X_1, ..., X_n)$ is uniformly distributed in E.
- f is *correlation-immune over $\mathcal{F}$ with respect to the subset* $T \subset \{1, 2, \ldots, n\}$ if the probability distribution of the output Y is unaltered when the inputs $(X_i)_{i \in T}$ are fixed and $\{X_i, i \notin T\}$ is a set of independent uniformly distributed random variables.
- f is *t-th order correlation-immune over $\mathcal{F}$* if for every T of cardinality at most t, f is correlation-immune with respect to T.
- f is *t-resilient over $\mathcal{F}$* if f is t-th order correlation-immune over $\mathcal{F}$ and balanced.

2.1. Correlation immune functions and orthogonal arrays

Correlation-immune functions are closely related to the combinatorial structures introduced by Rao as orthogonal arrays [28].

Definition 1. An orthogonal array $\mathcal{A}$ of size M, with n constraints, of strength t and index λ over the alphabet $\mathcal{F}$ (or with q levels) is an $M \times n$ array of elements of $\mathcal{F}$ which has the property that in any subset of t columns of $\mathcal{A}$, each of the q^t vectors of $\mathcal{F}^t$ appears exactly λ times as a row. Such an array is denoted by (M, n, q, t). Clearly $M = \lambda q^t$.

In [9] it was observed that the characterization by Xiao and Massey [41] of a t-th order correlation-immune function $f : \{0,1\}^n \to \{0,1\}$ is equivalent to the following property: the array of which rows are the vectors of $f^{-1}(1)$ is an orthogonal array of strength t. Let $\mathbf{F}_q$ denote the finite field with q elements. In [18] Gopalakrishnan and Stinson show directly that $f : \mathbf{F}_q^n \to \mathbf{F}_q^\ell$ is t-th order correlation-immune over $\mathbf{F}_q$ if and only if for all y in $\mathbf{F}_q^\ell$, $f^{-1}(y)$ consists of the rows of an orthogonal array of strength t. In fact characterizing the t-th order correlation immune functions in terms of orthogonal arrays is merely translating the probability definition into an enumeration definition. This characterization then requires no particular algebraic structure neither for the input alphabet $\mathcal{F}$ nor for the output set E.

PROPOSITION 1 *Let $f : \mathcal{F}^n \to E$ where both $\mathcal{F}$ and E are finite sets. The function f is a t-th order correlation-immune function over $\mathcal{F}$ if and only if $\forall y \in E$, $f^{-1}(y)$ consists of the rows of an orthogonal array of strength t over $\mathcal{F}$.*

Additionally, f is t-resilient if

$$\forall y, y' \in E, |f^{-1}(y)| = |f^{-1}(y')|$$

This general characterization points out the link between resilient functions and error-correcting codes when the input alphabet $\mathcal{F}$ is an Abelian group: Delsarte [15] actually proved that the array formed by the words of a code over a finite Abelian group is an orthogonal array of maximal strength $d^\perp - 1$ where $d^\perp$, called the *dual distance of the code,* is given by the MacWilliams transform of its Hamming distance distribution.

PROPOSITION 2 **[15]** *Let $\mathcal{C}$ be a code of length n and size M over an Abelian group $\mathcal{F}$ with q elements. The array whose rows consist of the codewords of $\mathcal{C}$ is an orthogonal array with n constraints, of size M and strength t over $\mathcal{F}$ if and only if $1 \le t \le d^\perp - 1$. The dual distance $d^\perp$ of the code $\mathcal{C}$ is the smallest index $i > 0$ such that $A'_i > 0$ where $(A'_0, \dots, A'_n)$ is the Mac Williams transform of the average Hamming distance distribution $(A_0, \dots, A_n)$ of $\mathcal{C}$:*

$$\sum_{i=0}^{n} A'_i X^{n-i} Y^i = A'(X,Y) = A(X + (q-1)Y, X - Y)$$

where $A(X,Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i$.

Moreover if $\mathcal{C}$ is an additive code, $d^\perp$ is the minimum distance of its dual code $\mathcal{C}^\perp$.

Since a t-resilient function $f : \mathcal{F}^n \rightarrow \mathcal{F}^\ell$ corresponds to a partition of $\mathcal{F}^n$ into q^ℓ orthogonal arrays of strength t and with the same size, Delsarte's result implies that such a function can be obtained from the cosets of a linear code whose dual code has minimum distance $t + 1$. This result proved by Stinson [37] for codes over a finite field can then be generalized to any linear code over a finite ring.

PROPOSITION 3 *Let $\mathcal{C}$ be a linear code of length n, dimension k and minimum distance d over a finite ring $\mathcal{F}$ and let G be a generator matrix for $\mathcal{C}$. The associated function*

$$\begin{array}{rcl} f : \mathcal{F}^n & \rightarrow & \mathcal{F}^{n-k} \\ x & \mapsto & xG^T \end{array}$$

is a $(d - 1)$-resilient function over $\mathcal{F}$.

Any linear resilient function f can then be identified to a syndrome function.

Massey and Stinson [38] recently extended this construction to any systematic codes over a finite field. This results still holds for systematic codes defined on any finite Abelian group.

PROPOSITION 4 *Let $\mathcal{C}$ be a systematic code of length n and size q^k over a finite Abelian group $\mathcal{F}$ and let I be an information set for $\mathcal{C}$. The function f defined by*

$$\begin{array}{rcl} f : \mathcal{F}^n & \rightarrow & \mathcal{F}^{n-k} \\ x & \mapsto & e \textit{ if and only if } x \in \mathcal{C} + \bar{e} \end{array}$$

where $\bar{e}$ is the vector of $\mathcal{F}^n$ which vanishes in I and whose restriction onto $\{1,\ldots,n\} \setminus I$ equals e, is a $(d^\perp - 1)$-resilient function where $d^\perp$ is the dual distance of $\mathcal{C}$.

Using this link between codes and resilient functions, Bierbrauer, Gopalakrishnan and Stinson [3] derived some bounds on the highest possible resilience-order for a function $f : \mathbf{F}_2^n \rightarrow \mathbf{F}_2^\ell$ from some bounds on the size of a code with given length and minimum distance. Since these bounds — Plotkin bound, linear programming bound ... — are still valid for codes over any finite Abelian group [13], we obtain general expressions for them. Explicit tables for highest possible resilience-order of a function $f : \mathcal{F}^n \rightarrow \mathcal{F}^\ell$ are for instance given in [10, chapter 6] for any Abelian group $\mathcal{F}$ with 2, 4 or 8 elements and for $1 \leq \ell < n \leq 20$.

2.2. *Characterization by means of characters*

In [41] Xiao and Massey characterized Boolean correlation-immune functions through a condition on their Fourier transform. The main interest of this characterization is that it is considerably easier to use than the probabilistic definition. This property was generalized by Gopalakrishnan and Stinson [18] when both input and output sets are finite fields. We here give a similar characterization which is valid for any finite sets $\mathcal{F}$ and E endowed with the structure of an Abelian group.

A *character* of a finite Abelian group $(\mathcal{F}, +)$ is an homomorphism from $\mathcal{F}$ into the multiplicative group $\mathbf{C}^\star$ of complex numbers. A well-known property is that the characters of $\mathcal{F}$ form an Abelian group $\mathcal{F}'$, called the characters group, which is isomorphic with $\mathcal{F}$. Since the characters can be numbered by the elements of $\mathcal{F}$, we denote by $< x, y >$ the complex image of the element $x \in \mathcal{F}$ under the character χ_y.

For example if $\mathcal{F}$ is the additive group $(\mathbf{F}_q, +)$ of the Galois field $\mathbf{F}_q$ where $q = p^s$, p a prime, then $< x, y >= \theta^{Tr_{\mathbf{F}_q/\mathbf{F}_p}(xy)}$ where θ is a primitive p-th root of unity in $\mathbf{C}$. If $\mathcal{F}$ is the additive group $(\mathbf{Z}_q, +)$, *i.e.* a cyclic group of order q, then $< x, y >= \theta^{xy}$ where θ is a primitive q-th root of unity in $\mathbf{C}$ and where the product xy is performed in the ring $\mathbf{Z}_q$.

We will need the following classical lemma:

LEMMA 1 *Let F and G be two Abelian groups with respective characters groups F' and G'. Then the characters group of $H = F \times G$ is $F' \times G'$.*
For $h = (f, g) \in F \times G$ and $h' = (f', g') \in F \times G$, we have

$$< h, h' >=< f, f' >< g, g' >$$

As soon as we handle characters it is particularly convenient to use the Fourier transform.

Definition 2. The group algebra $\mathbf{C}\mathcal{F}$ of an Abelian group $\mathcal{F}$ over the field $\mathbf{C}$ of complex numbers consists of all formal sums:

$$\mathbf{a} = \sum_{x \in \mathcal{F}} a_x Z^x, \quad a_x \in \mathbf{C}$$

where, as usual, Z^x replaces x in order for the Abelian group law to become multiplicative. All operations in $\mathbf{C}\mathcal{F}$ are defined in the usual way.

A character may then be extended linearly to the algebra $\mathbf{C}\mathcal{F}$:

$$< \mathbf{a}, y >=< \sum_{x \in \mathcal{F}} a_x Z^x, y >= \sum_{x \in \mathcal{F}} a_x < x, y >$$

We will denote by $\hat{a}_y$ the complex number $< \mathbf{a}, y >$, called a Fourier coefficient of $\mathbf{a}$. The Fourier transform is then the linear mapping

$$\begin{array}{ccc} \mathbf{C}\mathcal{F} & \rightarrow & \mathbf{C}\mathcal{F}' \\ \mathbf{a} & \mapsto & \sum_{y \in \mathcal{F}} \hat{a}_y Z^y \end{array}$$

Since the matrix S of group characters of $\mathcal{F}$ defined by $S(x, y) =< x, y >$ is orthogonal, there exists an inverse Fourier transform and $\mathbf{a}$ is then uniquely determined by its Fourier coefficients $(\hat{a}_y)_{y \in \mathcal{F}}$.

We now show how the Fourier transform characterization of Gopalakrishnan and Stinson can be stated for general Abelian groups. This result can be straightforwards deduced from a theorem proved by Delsarte [14, Theorem 4.4], which defines the combinatorial structure of orthogonal array in terms of characters.

Let $\mathcal{F}$ be an Abelian group. The n-th Cartesian power $\mathcal{F}^n$ is then an Abelian group in its turn. The Hamming weight of an element x of $\mathcal{F}^n$ is the number $w_H(x)$ of components of x in $\mathcal{F}$ which are distinct from zero. We give here a slightly modified version of Theorem 4.4 of Delsarte, which originally referred to the property of t-design.

THEOREM 1 *Let $\mathcal{F}$ be a finite Abelian group with q elements. A set $\mathcal{M}$ of λq^t vectors of $\mathcal{F}^n$ consists of the rows of an orthogonal array with n constraints, strength t and index λ over $\mathcal{F}$ if and only if*

$$\forall y \in \mathcal{F}^n,\ 1 \leq w_H(y) \leq t,\ \ \sum_{x \in \mathcal{M}} < x, y >= 0$$

We now deduce a general characterization of correlation-immune functions in terms of Fourier transform.

THEOREM 2 *Let $\mathcal{F}$ and E be two finite Abelian groups. The function $f : \mathcal{F}^n \rightarrow E$ is t-th order correlation-immune over $\mathcal{F}$ if and only if:*

$$\forall v \in E,\ \forall u \in \mathcal{F}^n, 1 \leq w_H(u) \leq t,\ \ \sum_{x \in \mathcal{F}^n} < x, u >< f(x), v >= 0$$

Moreover f is t-resilient if and only if it additionally satisfies:

$$\forall v \in E, v \neq 0,\ \ \sum_{x \in \mathcal{F}^n} < f(x), v >= 0$$

Proof: We write $\hat{a}_{y,u}$ for $\sum_{x \in f^{-1}(y)} < x, u >$ with the convention $\hat{a}_{y,u} = 0$ when $f^{-1}(y) = \emptyset$.
The above condition can then be written as:

$$\forall v \in E,\ \forall u \in \mathcal{F}^n, 1 \leq w_H(u) \leq t,\ \ \sum_{y \in E} \hat{a}_{y,u} < y, v >= 0$$

Since the matrix of group characters of the Abelian group E is invertible this condition is equivalent to

$$\forall u \in \mathcal{F}^n, 1 \leq w_H(u) \leq t,\ \ \hat{a}_{y,u} = 0$$

According to Theorem 1, this comes down to say that for all y in E, the elements of $f^{-1}(y)$ are the rows of an orthogonal array of strength t over $\mathcal{F}$.

The second condition can be written as:

$$\forall v \in E, v \neq 0,\ \ \sum_{y \in E} |f^{-1}(y)| < y, v >= 0$$

The exhibited Fourier coefficients of $\sum_{y \in E} |f^{-1}(y)| Z^y$ show that the function $y \mapsto |f^{-1}(y)|$ is constant on E, *i.e.* f is balanced. ■

EXAMPLE: Let $\mathcal{F}$ be the cyclic group $(\mathbf{Z}_q, +)$ and $\mathcal{A}_{a,b}$ be the array whose rows are the 4-tuples $(x_1, x_2, x_1 + ax_2, x_1 + bx_2)$ where $a, b \in \mathbf{Z}_q^\star$. Since this array has 4 constraints and its size is q^2, Singleton bound implies that its strength t is at most 2. According to Theorem 1 $\mathcal{A}_{a,b}$ is an orthogonal array of strength 2 over $\mathbf{Z}_q$ if and only if

$$\forall y \in \mathbf{Z}_q^4,\ 1 \leq w_H(y) \leq 2, \quad \sum_{x \in \mathcal{A}_{a,b}} \theta^{xy} = 0$$

This condition is equivalent to say that the dual of $\mathcal{A}_{a,b}$ in the characters group contains no element of Hamming weight less than or equal to 2, *i.e.*

$$\forall y \in \mathbf{Z}_q^4,\ 1 \leq w_H(y) \leq 2,\ \exists x \in \mathcal{A}_{a,b},\ \ \theta^{xy} \neq 1$$

where θ is a primitive q-th root of unity. Writing this condition for all y of weight 2, we obtain that $\mathcal{A}_{a,b}$ is an orthogonal array of strength 2 if and only if a, b and $(a-b)$ are not zero divisors. It follows that the strength of such an orthogonal array is at most 1 when q is even. A more general condition on the inexistence of such orthogonal arrays can be found in [20].

□

2.3. Matrix characterization

Gopalakrishnan and Stinson [18] gave a third characterization of correlation-immune and resilient functions which is expressed in terms of matrices. It actually results from the linear combination lemma, originally proved for binary random variables in [41] and generalized in [18] to random variables over a finite field. Following a short and general proof due to Brynielsson [6] we show that this lemma still holds when the alphabet is endowed with the structure of the ring $\mathbf{Z}_q$ or of the field $\mathbf{F}_q$. Notice that the size of $\mathbf{Z}_q$ is unrestricted whereas $|\mathbf{F}_q|$ is a prime power.

LEMMA 2 **(Linear Combination Lemma)** *Let $\mathcal{F}$ be a set with q elements endowed with the structure of either the finite field $\mathbf{F}_q$ or the ring $\mathbf{Z}_q$. The discrete random variable Y is independent of the n random variables $X_1, X_2, \ldots, X_n$ defined on $\mathcal{F}$ if and only if Y is independent of the sum $c \cdot X = c_1X_1 + c_2X_2 + \ldots + c_nX_n$ for every choice of $c_1, c_2, \ldots, c_n$ not all zeroes, in $\mathcal{F}$.*

Proof: The above condition is obviously necessary since we have:

$$\begin{aligned} \forall y \in E,\ Pr(c \cdot X = z | Y = y) &= \sum_{c \cdot x = z} Pr(X = x | Y = y) \\ &= \sum_{c \cdot x = z} Pr(X = x) \\ &= Pr(c \cdot X = z) \end{aligned}$$

This condition is also sufficient: let $a_x = Pr(X = x | Y = y)$ and $b_x = Pr(X = x)$. We consider in the group algebra $\mathbf{C}\mathcal{F}^n$ the elements $\mathbf{a} = \sum_{x \in \mathcal{F}^n} a_x Z^x$ and $\mathbf{b} = \sum_{x \in \mathcal{F}^n} b_x Z^x$. We will now show that, for every $c \in \mathcal{F}^n$, the Fourier coefficients $\hat{a}_c$ and $\hat{b}_c$ are equal. Indeed we just write for $c \neq 0$:

$$\begin{aligned} \hat{a}_c &= \sum_{x \in \mathcal{F}^n} Pr(X = x | Y = y) < x, c > \\ &= E_{Y=y}\left(< X, c >\right) \\ &= E_{Y=y}\left(\theta^{c \cdot X}\right) \text{ if } \mathcal{F} = \mathbf{Z}_q \\ &= E_{Y=y}\left(\theta^{Tr_{\mathbf{F}_q/\mathbf{F}_p}(c \cdot X)}\right) \text{ if } \mathcal{F} = \mathbf{F}_q \end{aligned}$$

Since each sum $c \cdot X$ is independent of Y provided that $c \neq 0$, we have:

$$\hat{a}_c = E\left(< X, c >\right) = \sum_{x \in \mathcal{F}^n} Pr(X = x) < x, c >= \hat{b}_c$$

Besides, for $c = 0$, we have:

$$\hat{a}_0 = \sum_{x \in \mathcal{F}^n} a_x = 1 = \sum_{x \in \mathcal{F}^n} b_x = \hat{b}_0 \qquad \blacksquare$$

As in [18] this generalized linear combination lemma leads to a characterization of t-th order correlation-immune functions and t-resilient functions in terms of matrices.

THEOREM 3 *Let $\mathcal{F}$ be a finite alphabet with q elements endowed with the structure of either the finite field $\mathbf{F}_q$ or the ring $\mathbf{Z}_q$. Let E be a finite set and f a function from $\mathcal{F}^n$ onto E.*
Let $N(u) = (\eta_{i,j})_{i,j \in \mathcal{F}}$ be the $q \times q$ real matrix defined by

$$\eta_{i,j} = q^n Pr(u_1 X_1 + \ldots + u_n X_n = i \text{ and } f(X) = j)$$

- *f is t-th order correlation-immune over $\mathcal{F}$ if and only if for all $u \in \mathcal{F}^n$ such that $1 \leq w_H(u) \leq t$, the rows of matrix $N(u)$ are all identical.*
- *f is t-resilient over $\mathcal{F}$ if and only if for all $u \in \mathcal{F}^n$ such that $1 \leq w_H(u) \leq t$, all the elements of matrix $N(u)$ equal $\frac{q^{n-1}}{|E|}$.*

Proof: Let u be any element of $\mathcal{F}^n$ such that $1 \leq w_H(u) \leq t$ and let T be its support. By definition f is t-th order correlation-immune over $\mathcal{F}$ if and only if its output $f(X)$ is independent of $(X_i)_{i \in T}$. According to the linear combination lemma, this is equivalent to

$$\forall u,\ 1 \leq w_H(u) \leq t,\ \ \eta_{i,j} = q^n Pr(u_1 X_1 + \ldots + u_n X_n = i) Pr(f(X) = j)$$

Since all input variables are uniformly distributed, $Pr(u_1 X_1 + \ldots + u_n X_n = i) = \frac{1}{q}$ for any $u \neq 0$. A necessary and sufficient condition for f to be t-th order correlation-immune is then:

$$\forall i,\ \ \eta_{i,j} = q^{n-1} Pr(f(X) = j)$$

Furthermore, f is balanced if and only if $Pr(f(X) = j) = \frac{1}{|E|}$. The function f is then t-resilient if and only if

$$\forall i, j,\ \ \eta_{i,j} = \frac{q^{n-1}}{|E|} \qquad \blacksquare$$

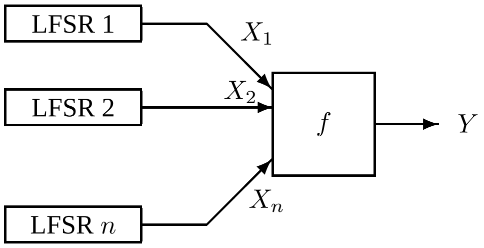

Figure 1. Combining LFSRs

3. Nonlinearity order of correlation-immune functions over any finite field

Resilient functions are particularly appropriate for combining the outputs of linear feedback shift registers since such a combination leads to a pseudo-random generator which resists correlation attacks [36]. But a high correlation-immunity order is not sufficient for ensuring the security of the resulting generator: the nonlinearity order of the combining function is a fundamental parameter too, since it determines the linear complexity of the generator. In this section we only consider functions from $\mathcal{F}^n$ to $\mathcal{F}^\ell$ where $\mathcal{F}$ is the finite field $\mathbf{F}_q$. $\mathbf{F}_q^\ell$ is here identified with the finite field $\mathbf{F}_{q^\ell}$.

3.1. *Nonlinearity order of a $\mathbf{q}$-ary correlation-immune function*

The linear complexity of a q-any linear recurring sequence $\mathbf{s}$, denoted by $L(\mathbf{s})$, is the length of the smallest linear feedback shift register driving $\mathbf{s}$. It is a fundamental parameter for pseudo-random generators since Massey [23] proved that Berlekamp algorithm for decoding BCH codes [2] enables to recover the minimal feedback polynomial of a sequence from the knowledge of its $2L(s)$ first digits. But, even if the feedback polynomial is primitive, the linear complexity, which is equal to the length of the LFSR, may not be as large as we wish. A well-known method for increasing it consists in using several LFSRs with different feedback polynomials. Their output sequences are then taken as arguments of a combining function $f : \mathbf{F}_q^n \rightarrow \mathbf{F}_q$ whose output then forms the running-key, as depicted in Figure 1.

The linear complexity of the resulting sequence is then determined by the algebraic normal form of the combining function.

Definition 3. [22, Theorem 1.71] For any function $f : \mathbf{F}_q^n \rightarrow \mathbf{F}_{q^\ell}$ there exists a unique polynomial function θ in the algebra $\mathbf{F}_{q^\ell}[x_1, \ldots, x_n]/(x_1^q - x_1, \ldots, x_n^q - x_n)$ such that, for all x in $\mathbf{F}_q^n$, $f(x) = \theta(x)$. This polynomial θ is called the *algebraic normal form* of f.

The influence of the algebraic normal form of the combining function on the linear complexity of the resulting sequence was investigated in [5, 19, 17, 21, 31, 33].

PROPOSITION 5 *Let* $\mathbf{a}$ *and* $\mathbf{b}$ *be two sequences in* $\mathbf{F}_q$ *(with characteristic* p*) whose minimal characteristic polynomials are respectively* f_0 *and* g_0*.*

- $$L(\mathbf{a}+\mathbf{b}) \leq L(\mathbf{a}) + L(\mathbf{b})$$

  where equality holds if and only if $gcd(f_0, g_0) = 1$.

- $$L(\mathbf{ab}) \leq L(\mathbf{a})L(\mathbf{b})$$

  where equality holds if and only if at least one of the polynomials f_0 and g_0 has only simple roots and all the zero products $\alpha\beta$ are distinct for all α and β such that $f_0(\alpha) = 0$ and $g_0(\beta) = 0$ in a common splitting field. This condition is notably satisfied if f_0 and g_0 have co-prime orders.

  A general lower bound on $L(\mathbf{ab})$ can also be deduced from the multiplicities of the roots of f_0 and g_0 and from the number of distinct products $\alpha\beta$ [19].

- *Let s be an integer, $0 \leq s_i < p$, and $s = \sum_{i=0}^{e} s_i p^i$ with $0 \leq s_i < p$ be its decomposition in the radix p.*

  $$L(\mathbf{a}^s) \leq \prod_{i=0}^{e} \binom{L(\mathbf{a}) - 1 + s_i}{s_i}$$

  where equality holds if f_0 is a primitive polynomial of $\mathbf{F}_q[X]$.

A combining function over a finite field $\mathbf{F}_q$ with characteristic p must therefore have a high resilience-order and its algebraic normal form must contain a monomial whose degree s in each one of its variables maximizes $w_p(s) = \sum_{i=0}^{e} s_i$ where s is written as $\sum_{i=0}^{e} s_i p^i$ in the radix p. For a Boolean function this actually means that both total degree of its algebraic normal form and resilience-order must be as high as possible. Unfortunately, there exits a tradeoff between these parameters: Siegenthaler proved in [35] that for any Boolean function f from $\mathbf{F}_2^n$ to $\mathbf{F}_2$, the degree d of the algebraic normal form and the correlation-immunity order t always satisfy $d + t \leq n$. We here exhibit a similar relation for any function from $\mathbf{F}_q^n$ to $\mathbf{F}_{q^\ell}$. Actually those relations for $q > 2$ are derived from stronger properties.

THEOREM 4 *Let f be a function from $\mathbf{F}_q^n$ onto $\mathbf{F}_{q^\ell}$. If f is t-th order correlation-immune (resp. t-resilient) over $\mathbf{F}_q$, then any monomial of its algebraic normal form contains at most $(n-t)$ variables (resp. $(n-t-1)$ variables provided $q^\ell \neq 2$ or $n \neq \ell + t$) having simultaneously degree $q-1$.*

Proof:
Let L_α be the Lagrange univariate idempotents in the algebra $\mathbf{F}_{q^\ell}[x]/(x^q - x)$:

$$L_\alpha(x) = \prod_{\substack{\beta \in \mathbf{F}_q \\ \beta \neq \alpha}} (x - \beta)$$

By construction we have:

$$\forall \beta \neq \alpha, L_\alpha(\beta) = 0 \text{ and } L_\alpha(\alpha) = \prod_{\gamma \in \mathbf{F}_q^*} \gamma = -1$$

The algebraic normal form of f is then

$$\theta(x_1, \cdots, x_n) = \sum_{\alpha \in \mathbf{F}_q^n} (-1)^n f(\alpha) \left(\prod_{i=1}^{n} L_{\alpha_i}(x_i) \right)$$

Let $(n-j)$ variables be fixed amongst $x_1, \ldots, x_n$, for example and without loss of generality we choose the first $(n-j)$ ones. Since each L_{α_i} is a monic polynomial of degree $(q-1)$, the coefficient of $x_1^{q-1} \cdots x_{n-j}^{q-1}$ in θ is the polynomial $p_j(x_{n-j+1}, \cdots, x_n)$ defined by

$$p_j(x_{n-j+1}, \cdots, x_n) = \sum_{\beta \in \mathbf{F}_q^j} (-1)^n \left(\prod_{i=1}^{j} L_{\beta_i}(x_{n-j+i}) \right) \sum_{\alpha \in \mathbf{F}_q^{n-j}} f(\alpha, \beta)$$

If f is t-th order correlation-immune, we have for all $j \leq t$ and for all β in $\mathbf{F}_q^j$

$$|\{\alpha \in \mathbf{F}_q^{n-j},\ f(\alpha, \beta) = v\}| = \frac{|f^{-1}(v)|}{q^j} = \lambda q^{t-j}$$

where λ is a positive integer. We then deduce that if $j \leq t$, we have

$$\forall \beta \in \mathbf{F}_q^j, \quad \sum_{\alpha \in \mathbf{F}_q^{n-j}} f(\alpha, \beta) = \lambda q^{t-j} \sum_{v \in \mathbf{F}_{q^\ell}} v$$

This implies that

$$\forall j < t, \ \ p_j(x_{n-j+1}, \cdots, x_n) \equiv 0 \bmod q$$

Since this is true for any other choice of $n-j$ variables amongst $x_1, \ldots, x_n$ with $j < t$, it ensures that any monomial of θ contains no product of $(n-t+1)$ or more variables having simultaneously degree $q-1$, as asserted.

Furthermore if f is balanced, $\lambda = q^{n-\ell-t}$. In this case we obtain for all $\beta \in \mathbf{F}_q^t$

$$\begin{aligned} \sum_{\alpha \in \mathbf{F}_q^{n-t}} f(\alpha, \beta) &= q^{n-\ell-t} \sum_{v \in \mathbf{F}_{q^\ell}} v \\ &\equiv 0 \bmod q \text{ if } n - \ell - t > 0 \\ &= \sum_{v \in \mathbf{F}_{q^\ell}} v \equiv 0 \bmod q \text{ if } n = \ell + t \text{ and } q^\ell \neq 2 \end{aligned}$$ ■

Remark. The previous proof also implies a stronger condition on the algebraic normal form of some t-th order correlation-immune functions, even if they are not balanced: if $f : \mathbf{F}_q^n \rightarrow \mathbf{F}_{q^\ell}$ is a t-th order correlation-immune function over $\mathbf{F}_q$ such that:

$$\forall v \in \mathbf{F}_{q^\ell}, \ \ \frac{|f^{-1}(v)|}{q^t} = 0 \bmod q$$

then the assertion of the theorem for balanced functions holds.

As a weak corollary of this theorem, we obtain the following generalization of Siegenthaler's inequality.

COROLLARY 1 *Let $f : \mathbf{F}_q^n \to \mathbf{F}_{q^\ell}$ be a t-th order correlation-immune function over $\mathbf{F}_q$. Then the total degree d of its algebraic normal form satisfies*

$$d + t \leq (q-1)n$$

If f is additionally balanced and $n \neq \ell + t$ or $q^\ell \neq 2$, then

$$d + t \leq (q-1)n - 1$$

EXAMPLE: Let f be the function over $\mathbf{F}_{16}$ defined by

$$\begin{array}{rcl} f : \mathbf{F}_{16} \times \mathbf{F}_{16} & \to & \mathbf{F}_{16} \\ (x,y) & \mapsto & (x^{14} + y^7 + 1)^{11} \end{array}$$

This function is 1-resilient over $\mathbf{F}_{16}$ since each one of the involved exponentiations is a permutation of $\mathbf{F}_{16}$. Its algebraic normal form is given by:
$f(x,y) = x^{14}y^{14} + x^{14}y^{11} + x^{14}y^{10} + x^{13}y^{11} + x^{12}y^{11} + x^7y^{14} + x^{13}y^7 + x^6y^{14} + x^{13}y^3 + x^{14} + x^7y^7 + y^{14} + x^{13} + x^7y^6 + x^{12} + x^5y^7 + y^{11} + y^{10} + x^7 + y^7 + x^6 + y^6 + x^5 + x^4 + y^3 + y^2 + 1$

In accordance with the previous theorem, this algebraic normal form contains no variable of degree 15. Moreover its total degree reaches the bound given in Corollary 1. □

The correlation-immunity order of a q-ary function f actually satisfies a more restrictive condition which takes into account the degree of the algebraic normal form of all functions $p_2 \circ f \circ p_1$ obtained by applying a permutation on all inputs and outputs of f. If f is t-th order correlation-immune, such a function $p_2 \circ f \circ p_1$ is actually still t-th order correlation-immune (see further Corollary 4). Permutations on $\mathbf{F}_q$ provide for instance such permutations p_1 and p_2.

PROPOSITION 6 *Let f be a function from $\mathbf{F}_q^n$ onto $\mathbf{F}_{q^\ell}$. Its correlation-immunity order t satisfies*

$$\delta + t \leq (q-1)n$$

where δ is the maximum degree of the algebraic normal forms of $p_2 \circ f \circ p_1$ with $p_1 = (\pi_1, \ldots, \pi_n)$ and $p_2 = (\phi_1, \ldots, \phi_\ell)$ when the π_i and ϕ_i run over the set of all permutations of $\mathbf{F}_q$. Moreover if f is balanced and $n \neq \ell + t$ or $q^\ell \neq 2$, we have

$$\delta + t \leq (q-1)n - 1$$

3.2. *Algebraic Normal Form of q-ary functions which are correlation-immune over* $\mathbf{F}_{q^k}$

We now give a similar bound for the optimal nonlinearity of any function f from $(\mathbf{F}_{q^k})^n$ to $\mathbf{F}_q$ which is correlation-immune over $\mathbf{F}_{q^k}$.

THEOREM 5 *Let f be a function from $(\mathbf{F}_q)^{kn}$ onto $\mathbf{F}_q$ where $k > 1$. Its algebraic normal form is then a polynomial θ with kn variables in the algebra $\mathcal{A} = \mathbf{F}_q[x_{i,j}, 1 \leq i \leq n,\ 0 \leq j \leq k-1]/(x_{i,j}^q - x_{i,j})$.*
If f is t-th order correlation-immune (resp. t-resilient) over $\mathbf{F}_{q^k}$, then any monomial of θ contains at most $(kn-t)$ variables (resp. $(kn-t-1)$ variables) having simultaneously degree $q-1$.

Proof: Let us first consider f as a function from $(\mathbf{F}_{q^k})^n$ onto $\mathbf{F}_{q^k}$. Its normal form is then a polynomial $\mu \in \mathbf{F}_{q^k}[x_1, \ldots, x_n]/(x_i^{q^k} - x_i)$. Let α be a primitive element in $\mathbf{F}_{q^k}$. Then $\mathbf{F}_{q^k} = \mathbf{F}_q + \alpha\mathbf{F}_q + \ldots + \alpha^{k-1}\mathbf{F}_q$ and to any $x_i \in \mathbf{F}_{q^k}$ can be associated a polynomial of the algebra $\mathbf{F}_{q^k}[x_{i,j},\ 0 \leq j \leq k-1]/(x_{i,j}^q - x_{i,j})$.
The function f can therefore be written as a polynomial θ in the algebra $\mathbf{F}_{q^k}[x_{i,j}]$ modulo the ideal generated by $x_{i,j}^q - x_{i,j}$, $1 \leq i \leq n,\ 0 \leq j \leq k-1$. Since f takes its values in $\mathbf{F}_q$, we have $\theta^q(x) = \theta(x)$ for all $x \in \mathbf{F}_q^{kn}$. Thus $\theta = \theta^q$ and all coefficients of θ lie in $\mathbf{F}_q$.

We now write x_i^s for all $s < q^k$ as a polynomial in $x_{i,0}, \ldots, x_{i,k-1}$. Let $s = s_0 + s_1 q + \ldots + s_{k-1}q^{k-1}$ be the q-ary decomposition of s. We then have:

$$\begin{aligned} x_i^s &= \prod_{j=0}^{k-1}(x_{i,0} + \alpha x_{i,1} + \ldots + \alpha^{k-1}x_{i,k-1})^{s_j q^j} \\ &= \prod_{j=0}^{k-1}(x_{i,0} + \alpha^{q^j} x_{i,1} + \ldots + \alpha^{(k-1)q^j} x_{i,k-1})^{s_j} \end{aligned}$$

This polynomial therefore contains a monomial having degree $(q-1)$ in r variables only if the decomposition of s in the radix q contains r terms s_i equal to $q-1$. Thus $x_i^{q^k-1}$ is the only one which may contain a product of k variables of degree $q-1$ and all the other x_i^s for $s < q^k - 1$ contain at best a product of $k-1$ variables of degree $q-1$. According to Theorem 4, μ contains no product of more than $n-t$ variables of degree $q^k - 1$ since f is t-th order correlation-immune over $\mathbf{F}_{q^k}$. The algebraic normal form θ then contains no monomial of degree $q-1$ in more than $k(n-t) + (k-1)t$ variables, *i.e.* $kn - t$ variables.

If f is additionally balanced, we have for all $v \in \mathbf{F}_q$,$|f^{-1}(v)| = q^{nk-1}$. Since $k > 1$ and $t < n$, $\frac{|f^{-1}(v)|}{q^{kt}} \equiv 0 \bmod q$. In view of the remark following Theorem 4, we then obtain the expected result. ■

Remark. As for Theorem 4 a sufficient condition for having the property asserted for balanced functions is:

$$\forall v \in \mathbf{F}_q, \quad \frac{|f^{-1}(v)|}{q^{kt}} = 0 \bmod q$$

COROLLARY 2 *Let $f : \mathbf{F}_q^{kn} \rightarrow \mathbf{F}_q$ be a t-th order correlation-immune function over $\mathbf{F}_{q^k}$. The total degree d of its algebraic normal form then satisfies*

$$d + t \leq (q-1)kn$$

If f is additionally balanced and $k > 1$, then

$$d + t \leq (q-1)kn - 1$$

EXAMPLE:

Let ϕ: $\begin{array}{ccc} \mathbf{F}_8 \times \mathbf{F}_8 & \rightarrow & \mathbf{F}_8 \\ (x;y) & \mapsto & (x^3+y^3)^3 \end{array}$

Let α be a root of $X^3 + X + 1$. To each element x in $\mathbf{F}_8$ we associate the polynomial $x_0 + \alpha x_1 + \alpha^2 x_2$ and we now consider ϕ as a function from $\mathbf{F}_2^6$ to $\mathbf{F}_2^3$. Each of its components f_0, f_1, f_2 defined by $\phi = f_0 + \alpha f_1 + \alpha^2 f_2$ is a Boolean function with 6 Boolean variables and it is obviously 1-resilient over $\mathbf{F}_8$. According to the previous theorem it contains no product of more than 4 variables. Computing their algebraic normal form shows that all of them have optimal nonlinearity.

$f_0(x_0;x_1;x_2;y_0;y_1;y_2) = x_0 + y_0 + x_1y_2 + x_2y_1 + x_0x_1y_1 + x_1y_0y_1 + x_2y_0y_1 + x_0x_1y_2 + x_0x_2y_2 + x_0x_2y_0y_1 + x_0x_1y_0y_2$

$f_1(x_0;x_1;x_2;y_0;y_1;y_2) = x_2 + y_2 + x_0y_1 + x_1y_0 + x_0y_2 + x_2y_0 + x_0x_2y_1 + x_1y_0y_2 + x_2y_1y_2 + x_1x_2y_2 + x_0x_2y_2 + x_2y_0y_2 + x_1y_1y_2 + x_1x_2y_1 + x_0y_0y_2 + x_0x_2y_0 + x_0x_2y_1y_2 + x_1x_2y_0y_2$

$f_2(x_0;x_1;x_2;y_0;y_1;y_2) = x_1 + y_1 + x_2 + y_2 + x_2y_1 + x_1y_2 + x_0y_1 + x_1y_0 + x_0x_1y_0 + x_0y_0y_1 + x_2y_0y_1 + x_0x_1y_2 + x_0x_2y_0 + x_0y_0y_2 + x_0x_2y_1 + x_1y_0y_2 + x_0x_1y_1 + x_1y_0y_1 + x_1x_2y_1 + x_1y_1y_2 + x_0x_2y_2 + x_2y_0y_2 + x_1x_2y_0y_1 + x_0x_1y_1y_2 + x_0x_2y_1y_2 + x_1x_2y_0y_2$

□

3.3. *Construction of $\boldsymbol{t}$-resilient functions with optimal nonlinearity order over any finite field*

Definition 4. A t-th order correlation-immune (resp. t-resilient) function f from $\mathbf{F}_q^n$ into $\mathbf{F}_q$ has *optimal nonlinearity order* if its algebraic normal form contains a monomial with $n-t$ variables (resp. $n-t-1$) having degree $q-1$, the others having degree $q-2$.

We now construct t-resilient functions $f : \mathbf{F}_q^n \rightarrow \mathbf{F}_q$ with optimal nonlinearity order. We especially give a whole family of t-resilient functions $f : \mathbf{F}_{2^m}^n \rightarrow \mathbf{F}_{2^m}$ with optimal nonlinearity order for all values of n and t when m is odd. Such functions are then well-suited by combining LFSRs.

We first construct $(n-1)$-resilient functions with n variables over $\mathbf{F}_q$, *i.e.* (q^t,n,q,t) orthogonal arrays of index unity.

LEMMA 3 *Let (A) be the algebra $\mathbf{F}_q[z]/(z^q - z)$ with $q > 2$. We have in $\mathcal{A}$ that $degree(z^{i(q-2)}) < q-2$ for all $2 \leq i < q-1$, and for even q, $degree(z^{j\frac{q-2}{2}}) < q-2$ for all $3 \leq j \leq q-2$.*

Proof: Indeed, we have

$$z^{i(q-2)} = z^{q+q(i-1)-2i} = z^q z^{i-1-2i} = z^{q-i-1}$$

Since $i \geq 2$, the degree of this monomial is at most $q-3$.

We now consider the monomial $z^{j\frac{q-2}{2}}$ where $j = 2a+b$ with $b \in \{0,1\}$. If $b=0$, we can apply the previous result since $2 \leq a \leq q-2$. If $b=1$, we have $1 \leq a < \frac{q-2}{2}$. We now write

$$z^{j\frac{q-2}{2}} = z^{a(q-2)+\frac{q-2}{2}} = z^{q-a-1+\frac{q-2}{2}} = z^{\frac{q-2}{2}-a}$$

This implies that the degree of $z^{j\frac{q-2}{2}}$ equals $\frac{q-2-2a}{2}$; thus $degree(z^{j\frac{q-2}{2}}) < q-2$.

$\blacksquare$

PROPOSITION 7 *For all $q = p^m$ with $p \neq 3$ and $q > 4$ there exists an 1-resilient function $f : \mathbf{F}_q^2 \rightarrow \mathbf{F}_q$ with optimal nonlinearity order.*

Proof: For odd characteristic $p > 3$, we define $f(x,y) = (x^{q-2} + y^{q-2} + 1)^{q-2}$, and for even $q > 4$, $f(x,y) = (x^{q-2} + y^{\frac{q-2}{2}} + 1)^{q-5}$. Since $gcd(q-2, q-1) = 1$ and for even $q > 4$, $gcd(\frac{q}{2}-1, q-1) = 1,\ gcd(q-5, q-1) = 1$, all these exponentiations permute the finite field $\mathbf{F}_q$. The function f is then 1-resilient in both cases. In view of Lemma 3 we point out that, in the first case, the coefficient of $x^{q-2}y^{q-2}$ is $(q-2)(q-3)$ which is not a multiple of $p > 3$. In the second case we see that the coefficient of $x^{q-2}y^{q-2}$ is $3\binom{q-5}{3} \equiv 1 \bmod 2$

$\blacksquare$

PROPOSITION 8 *For all $q = p^m$ with $p \neq 3$ and $q \not\equiv 1 \bmod 3$ there exists an $(n-1)$-resilient function $f : \mathbf{F}_q^n \rightarrow \mathbf{F}_q$ with optimal nonlinearity order for any n if q is even and for any odd n if q is odd.*

Proof: We prove this assertion by induction on n.

- q even: the assertion for $n = 2$ is proved by the previous proposition. Suppose now that there exists a $(n-1)$-resilient function g with n variables over $\mathbf{F}_q$. We then consider the function with $(n+1)$ variables defined by

  $$f(x_1, \ldots, x_{n+1}) = (g(x_1, \ldots, x_n) + x_{n+1}^{\frac{q}{2}-1})^3$$

  This function is n-resilient since $gcd(3, q-1) = 1$ by assumption and $gcd(q-2, q-1) = 1$. The coefficient corresponding to the term $(x_1 \ldots x_{n+1})^{q-2}$ equals 1 in $\mathbf{F}_q$; this function then has optimal nonlinearity order.

  This still holds for $q = 2$: $f(x_1, \ldots, x_n) = x_1 + \ldots + x_n$ is an $(n-1)$-resilient function with optimal nonlinearity order over $\mathbf{F}_2$.

- q odd: for $n = 3$ we consider

  $$f(x_1, x_2, x_3) = (x_1^{q-2} + x_2^{q-2} + x_3^{q-2})^3$$

Since $q \not\equiv 1 \bmod 3$, this function is 2-resilient and the coefficient of the term $(x_1x_2x_3)^{q-2}$ equals 6; it does therefore not vanish because p is odd and strictly greater than 3.

Suppose now that there exists a $(2r-2)$-resilient function g with $(2r-1)$ variables over $\mathbf{F}_q$. We then consider the function with $(2r+1)$ variables defined by

$$f(x_1, \ldots, x_{2r+1}) = (g(x_1, \ldots, x_{2r-1}) + x_{2r}^{q-2} + x_{2r+1}^{q-2})^3$$

This function is then $2r$-resilient and the coefficient of the term $(x_1 \ldots x_{2r+1})^{q-2}$ equals 6.

■

It is now easy to construct t-resilient functions with n variables and with optimal nonlinearity order thanks to the following lemma:

LEMMA 4 *Let $q \neq 2$ or $t \neq n-1$. Let $f_1, f_2 : \mathbf{F}_q^n \to \mathbf{F}_q$ be two t-resilient functions with optimal nonlinearity order such that $degree(f_1 - f_2) = degree(f_1)$. Then $g : \mathbf{F}_q^{n+1} \to \mathbf{F}_q$ defined by*

$$g(x_1, \ldots, x_{n+1}) = x_{n+1}^{q-1} f_1(x_1, \ldots, x_n) + (1 - x_{n+1}^{q-1}) f_2(x_1, \ldots, x_n)$$

is a t-resilient function with optimal nonlinearity order.

We then deduce the following theorem:

THEOREM 6 *Let $q = p^m$ with $p \neq 3$ and $q \not\equiv 1 \bmod 3$. For all $n > 1$, there exists a t-resilient function $f : \mathbf{F}_q^n \to \mathbf{F}_q$ with optimal nonlinearity order for all $t < n$ if q is even, and for all even $t < n$ if q is odd.*

Proof: By Proposition 8, if t satisfies the above assumptions, there exists a t-resilient function $g : \mathbf{F}_q^{t+1} \to \mathbf{F}_q$ with optimal nonlinearity order. Applying Lemma 4 with $f_1 = g$ and $f_2 = \alpha g$, where $\alpha \in \mathbf{F}_q \setminus \{0, 1\}$ leads to a t-resilient function with $t+2$ variables and optimal nonlinearity order . If we iterate this construction $n-t-1$ times, we obtain a t-resilient function with n variables and optimal nonlinearity order. Siegenthaler [35] proved this result in the Boolean case. ■

EXAMPLE: We here construct a 2-resilient function with 4 variables over $\mathbf{F}_8$.
Proposition 8 enables us to construct functions g_1 and g_2 which are respectively 1-resilient with 2 variables and 2-resilient with 3 variables. Both normal forms have optimal nonlinearity order:
$g_1(x_1, x_2) = (x_1^6 + x_2^3)^3 = x_1^6x_2^6 + x_1^5x_2^3 + x_1^4 + x_2^2$
$g_2(x_1, x_2, x_3) = (g_1(x_1, x_2) + x_3^3)^3 = x_1^6x_2^6x_3^6 + x_1^5x_2^3x_3^6 + x_1^4x_2^5x_3^4 + x_1^5x_2^7 + x_1^4x_2^7x_3 + x_1^2x_2^6x_3^4 + x_1^7x_2^2x_3 + x_1^4x_3^6 + x_1^6x_2^3 + x_1^5x_2^3x_3 + x_1^4x_2^4 + x_1^2x_2^4x_3^2 + x_2^2x_3^6 + x_2^4x_3^3 + x_2^6 + x_1^4x_3 + x_1^2x_2x_3 + x_1x_2x_3^2 + x_3^4 + x_2^2x_3 + x_3^2$

We now apply Lemma 4 with $f_1 = g_2$ and $f_2 = \alpha g_2$ where $\alpha \in \mathbf{F}_8 \setminus \{0, 1\}$. We then obtain a 2-resilient function f with 4-variables and optimal nonlinearity order $d = 25$. Its algebraic normal form is:

$$\begin{aligned}
& f(x_1,x_2,x_3,x_4) = (\alpha+1)x_1^6x_2^6x_3^6x_4^7 + (\alpha+1)x_1^5x_2^3x_3^6x_4^7 \\
& +(\alpha+1)x_1^4x_2^5x_3^4x_4^7 + (\alpha+1)x_1^5x_2^7x_4^7 + (\alpha+1)x_1^4x_2^7x_3x_4^7 \\
& +(\alpha+1)x_1^2x_2^6x_3^4x_4^7 + \alpha x_1^6x_2^6x_3^6 + (\alpha+1)x_1^7x_2^2x_3x_4^7 \\
& +(\alpha+1)x_1^4x_3^6x_4^7 + (\alpha+1)x_1^6x_2^3x_4^7 + (\alpha+1)x_1^5x_2^3x_3x_4^7 \\
& +(\alpha+1)x_1^4x_2^4x_4^7 + (\alpha+1)x_1^2x_2^4x_3^2x_4^7 + (\alpha+1)x_2^2x_3^6x_4^7 \\
& +\alpha x_1^5x_2^3x_3^6 + (\alpha+1)x_2^4x_3^3x_4^7 + \alpha x_1^4x_2^5x_3^4 + (\alpha+1)x_2^6x_4^7 \\
& +\alpha x_1^5x_2^7 + \alpha x_1^4x_2^7x_3 + (\alpha+1)x_1^4x_3x_4^7 + \alpha x_1^2x_2^6x_3^4 \\
& +(\alpha+1)x_1^2x_2x_3x_4^7 + (\alpha+1)x_1x_2x_3^2x_4^7 + (\alpha+1)x_3^4x_4^7 \\
& +\alpha x_1^7x_2^2x_3 + \alpha x_1^4x_3^6 + (\alpha+1)x_2^2x_3x_4^7 + \alpha x_1^6x_2^3 + \alpha x_1^5x_2^3x_3 \\
& +(\alpha+1)x_3^2x_4^7 + \alpha x_1^4x_2^4 + \alpha x_1^2x_2^4x_3^2 + \alpha x_2^2x_3^6 + \alpha x_2^4x_3^3 \\
& +\alpha x_2^6 + \alpha x_1^4x_3 + \alpha x_1^2x_2x_3 + \alpha x_1x_2x_3^2 + \alpha x_3^4 + \alpha x_2^2x_3 + \alpha x_3^2
\end{aligned}$$

Since it contains a monomial with $3 = t+1$ variables of degree $q-2$ and one of degree $q-1$, it has optimal nonlinearity order according to Theorem 4. □

4. Construction of new correlation-immune functions by composition

Correlation-immune and resilient functions are essential for generating pseudo-random sequences. But constructing some functions having both a great number of input variables and a high correlation-immunity order is still a problem. The construction using error-correcting codes is quite general but it usually leads to linear functions. Using the characterizations given in Section 2, we now propose a new method for constructing correlation-immune and resilient functions by composition of correlation-immune functions of smaller order. $\mathcal{F}$ is here a finite alphabet of size q endowed with the structure of some Abelian group.

4.1. Construction by composition

Definition 5. Let $(g_i)_{1\leq i\leq k}$ be a family of k functions:

$$g_i : \mathcal{F}^n \to \mathcal{F}^d = \mathcal{A}, \text{ where } d \leq n$$

We define the function g from $\mathcal{F}^{nk}$ into $\mathcal{A}^k$ by $g(x_1,\ldots,x_k) = (g_1(x_1),\ldots,g_k(x_k))$. Let h be a function:

$$h : \mathcal{A}^k \to \mathcal{F}^\ell, \text{ where } \ell \leq kd$$

The composed function $f = h \circ g$ is defined by:

$$\begin{array}{cccc} f: & \mathcal{F}^{nk} & \to & \mathcal{F}^\ell \\ & (x_1,\ldots,x_k) & \mapsto & h(g_1(x_1),\ldots,g_k(x_k)) \end{array}$$

PROPOSITION 9 *If every g_i is balanced and if h is r-th order correlation-immune over $\mathcal{A}$, then $h \circ g$ is r-th order correlation-immune over $\mathcal{F}^n$.*

Proof: Let $v \in \mathcal{F}^\ell$ and let $R = \{i_1, \ldots, i_r\}$ be a r-element subset of $\{1, \ldots, k\}$ and $\bar{R} = \{j_1, \ldots, j_{k-r}\}$ be the complementary set.
Since h is r-th order correlation-immune over $\mathcal{A}$, $h^{-1}(v)$ is an orthogonal array with k constraints, strength r and index λ_v over the alphabet $\mathcal{A}$. Given a vector $a = (a_{i_1}, \ldots, a_{i_r}) \in \mathcal{A}^r$, the number of elements $z = (z_1, \ldots, z_k) \in \mathcal{A}^k$ in $h^{-1}(v)$ such that $(z_{i_1}, \ldots, z_{i_r}) = a$ is then equal to λ_v.
We denote by g_R the function $(x_{i_1}, \ldots, x_{i_r}) \mapsto (g_{i_1}(x_{i_1}), \ldots, g_{i_r}(x_{i_r}))$ and by $g_{\bar{R}}$ the function $(x_{j_1}, \ldots, x_{j_{k-r}}) \mapsto (g_{j_1}(x_{j_1}), \ldots, g_{j_{k-r}}(x_{j_{k-r}}))$.
By assumption, every g_i is balanced; this entails that $|g_i^{-1}(a_i)| = |\mathcal{F}|^{n-d}$.
Then $\forall b = (b_{j_1}, \ldots, b_{j_{k-r}})$, $g_{\bar{R}}^{-1}(b)$ is a subset of $\mathcal{F}^{n(k-r)}$ of size $|\mathcal{F}|^{(n-d)(k-r)}$. In the same way $|g_R^{-1}(a)| = |\mathcal{F}|^{(n-d)r}$ and $\{g_R^{-1}(a)\}_{a \in \mathcal{A}^r}$ is a partition of $(\mathcal{F}^n)^r$. Hence every r-tuple of $(\mathcal{F}^n)^r$ appears as the projection on R of exactly $\lambda_v |\mathcal{F}|^{(n-d)(k-r)}$ elements in $(h \circ g)^{-1}(v)$. It means that $(h \circ g)^{-1}(v)$ is an orthogonal array with k constraints, strength r, index $\lambda_v q^{(n-d)(k-r)}$ over the alphabet $\mathcal{F}^n$. ■

PROPOSITION 10 *If $f = h \circ g$ is r-th order correlation-immune over $\mathcal{F}^n$ and if $\forall 1 \leq i \leq k$, g_i is t-th order correlation-immune over $\mathcal{F}$, then f is t'-th order correlation-immune over $\mathcal{F}$ where $t' = (t+1)(r+1) - 1$.*

Proof: Let $\mathcal{B} = \mathcal{F}^n$ and $u \in \mathcal{B}^k$. We write $u = (u_1, \ldots, u_k), u_i \in \mathcal{B}$. The Hamming weight of u in $\mathcal{B}^k$, *i.e.* $|\{i/u_i \neq 0\}|$, is denoted by $W_H(u)$ while the Hamming weight of u in $\mathcal{F}^{nk}$, *i.e.* the number of non-zero components of u in $\mathcal{F}$ is denoted by $w_H(u)$.
The function f is r-th order correlation-immune over $\mathcal{B}$ if and only if $\forall v \in \mathcal{F}^\ell$, $f^{-1}(v)$ is an orthogonal array of strength r over $\mathcal{B}$. By Theorem 1 we have

$$\forall u \in \mathcal{B}^k,\ 1 \leq W_H(u) \leq r, \qquad \sum_{x \in f^{-1}(v), x \in \mathcal{B}^k} < x, u >= 0$$

Now if $W_H(u) > r$ and $w_H(u) < (r+1)(t+1)$, there is an index $i \in \{1, \ldots, k\}$ such that $1 \leq w_H(u_i) \leq t$. Then we get by Lemma 1:

$$\begin{aligned} \sum_{x \in f^{-1}(v), x \in \mathcal{F}^{nk}} < x, u > &= \sum_{y \in h^{-1}(v)} \sum_{x \in g^{-1}(y)} < x, u > \\ &= \sum_{y \in h^{-1}(v)} \prod_{i=1}^{k} \sum_{x_i \in g_i^{-1}(y_i)} < x_i, u_i > \end{aligned}$$

Since g_i is t-th order correlation-immune, at least one of the factors $\sum_{x_i \in g_i^{-1}(y_i)} < x_i, u_i >$ is zero. Thus we obtain:

$$\forall u \in \mathcal{F}^{nk},\ 1 \leq w_H(u) \leq t', \qquad \sum_{x \in f^{-1}(v), x \in \mathcal{F}^{nk}} < x, u >= 0 \qquad ■$$

As a consequence of these two propositions we obtain the following theorem.

THEOREM 7 *If every g_i is t-resilient over $\mathcal{F}$ and if h is r-th order correlation-immune (resp. r-resilient) over $\mathcal{F}^d$, then $h \circ g$ is t'-th order correlation-immune (resp. t'-resilient) over $\mathcal{F}$, where $t' = (t+1)(r+1) - 1$.*

EXAMPLE:

$$\text{Let } g_1 = g_2 : \begin{array}{ccc} \mathbf{F}_2^3 & \to & \mathbf{F}_2^2 \\ (x_1, x_2, x_3) & \mapsto & (x_1 + x_2, x_1 + x_3) \end{array}$$

This function is 1-resilient over $\mathbf{F}_2$.
Let $h : (\mathbf{F}_2^2)^2 \to \mathbf{F}_2$ described by the transposed of its truth table T_h:

$$T_h^T = \left[\begin{array}{cccccccc} 0&0&0&0&1&1&1&1 \\ 0&0&1&1&1&1&0&0 \\ \hline 0&1&1&1&0&0&0&1 \\ 1&1&1&0&0&1&0&0 \end{array}\right] \begin{array}{c} x_1 \\ x_2 \\ x_3 \\ x_4 \end{array}$$

The function h is 1-resilient over $\mathbf{F}_2^2$ and it is nonlinear as a function from $(\mathbf{F}_2)^4$ onto $\mathbf{F}_2$ since $h(x_1, x_2, x_3, x_4) = x_1 + x_4 + x_2x_3 + x_2x_4$.
According to Theorem 7 the composed function is a Boolean function with 6 input variables which is 3-resilient over $\mathbf{F}_2$.

Its truth table T_f is then a binary orthogonal array with 6 constraints, of size 32, index 4 and strength 3:

$$\left[\begin{array}{cccccccccccccccccccccccccccccccc} 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0 \\ 0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1&0&1&0&0&1&1&0&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 0&1&0&1&0&1&0&1&0&1&1&0&0&1&1&0&0&1&0&1&0&1&0&1&0&1&1&0&0&1&1&0 \\ 1&0&0&1&1&0&0&1&0&1&0&1&0&1&0&1&0&1&1&0&0&1&1&0&0&1&0&1&0&1&0&1 \end{array}\right] \begin{array}{c} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{array}$$

Since its algebraic normal form is $f(x_1, x_2, x_3, x_4, x_5, x_6) = x_1 + x_2 + x_4 + x_6 + x_1x_5 + x_1x_6 + x_3x_5 + x_3x_6$, this Boolean function has optimal degree. □

The previous construction enables us to construct correlation-immune and resilient functions with a great number of variables and then to combine a great number of different LFSRs. Thanks to Theorem 7 we obtain the correlation-immunity order of f without writing its truth table which is usually very large. In the following example we construct a 5-resilient Boolean function of degree 4 for combining 12 LFSRs.

EXAMPLE:

$$g_1 = g_2 : \begin{array}{ccc} \mathbf{F}_2^6 & \to & \mathbf{F}_2^3 \\ x & \mapsto & xH^T \end{array}$$

where H is the parity-check matrix of the [6,3]-binary code $\mathcal{C}$,

$$H = \begin{bmatrix} 1&0&0&1&1&0 \\ 0&1&0&1&0&1 \\ 0&0&1&0&1&1 \end{bmatrix}$$

Since the dual code $\mathcal{C}^\perp$ has minimum distance 3, the corresponding function g_1 is a 2-resilient function over $\mathbf{F}_2$.

Let α be a root of $X^3 + X + 1$. We represent each element of $\mathbf{F}_8$ by 3 bits following the decomposition $\mathbf{F}_8 = \alpha^2\mathbf{F}_2 + \alpha\mathbf{F}_2 + \mathbf{F}_2$. We then define h as:

$$\begin{array}{rcl} h : \mathbf{F}_8 \times \mathbf{F}_8 & \rightarrow & \mathbf{F}_2 \\ (x, y) & \mapsto & (x^3 + y^3)^3_{|0} \end{array}$$

where $z_{|0}$ denotes the low-weight bit of z over $\mathbf{F}_2^3$.
By construction, h is 1-resilient over $\mathbf{F}_8$. The composed function $f = h \circ g$ then results in a 5-resilient Boolean function of degree 4 with 12 variables. □

Zhang and Zheng presented at Eurocrypt'95 some results about the construction of new binary resilient functions from old ones by addition (Section 3 in [42]) and by composition with a permutation (Section 4 in [42]). These results are immediate corollaries of the previous theorem and they can be generalized to functions over any finite Abelian group $\mathcal{F}$.

COROLLARY 3 *Let $(g_i)_{1\leq i\leq k}$ be a family of k functions from $\mathcal{F}^n$ onto $\mathcal{F}^d$ which are t-resilient over $\mathcal{F}$, and $h : (\mathcal{F}^d)^k \rightarrow \mathcal{F}^d$ be the addition over $\mathcal{F}^d$. Then the composed function*

$$\begin{array}{rccc} f : & \mathcal{F}^{nk} & \rightarrow & \mathcal{F}^d \\ & (x_1, \ldots, x_k) & \mapsto & g_1(x_1) + \ldots + g_k(x_k) \end{array}$$

is t'-resilient over $\mathcal{F}$ where $t' = k(t + 1) - 1$.

COROLLARY 4 *Let $g : \mathcal{F}^n \rightarrow \mathcal{F}^d$ be a t-resilient function over $\mathcal{F}$ and h be a permutation of $\mathcal{F}^d$. Then $h \circ g$ is still a t-resilient function over $\mathcal{F}$.*

Another interest of this result is that it enables us to construct large orthogonal arrays whose strength is close to the theoretical bounds. The parameters of the orthogonal arrays $g_i^{-1}(z), z \in \mathcal{A}$ are (q^{m-d}, m, q, t); those of $h^{-1}(z), z \in \mathcal{F}^\ell$ are $(q^{dk-\ell}, k, q^d, r)$. This results in orthogonal arrays $f^{-1}(z), z \in \mathcal{F}^\ell$ with parameters $(q^{km-\ell}, km, q, (t + 1)(r + 1) - 1)$.

EXAMPLE: We here consider two identical functions g_1 and g_2 obtained from the translated codes of the Preparata code $\mathcal{P}(5)$ (see Proposition 4). Since $\mathcal{P}(5)$ is a nonlinear systematic binary code of length 64, size 2^{52} and dual distance 28, the function

$$g_1 = g_2 : \mathbf{F}_2^{64} \rightarrow \mathbf{F}_2^{12}$$

is 27-resilient over $\mathbf{F}_2$.
Let now π_1, π_2 and π_3 be three permutations of the alphabet $\mathbf{F}_2^{12}$. The function

$$\begin{array}{rcl} h : (\mathbf{F}_2^{12})^2 & \rightarrow & \mathbf{F}_2^{12} \\ (x_1, x_2) & \mapsto & \pi_3(\pi_1(x_1) + \pi_2(x_2)) \end{array}$$

is a 1-resilient function over $\mathbf{F}_2^{12}$.
The composed function

$$f : \mathbf{F}_2^{128} \rightarrow \mathbf{F}_2^{12}$$

is then 55-resilient over $\mathbf{F}_2$. For all $v \in \mathbf{F}_2^{12}$, the arrays $f^{-1}(v)$ are therefore orthogonal arrays with 64 constraints, of size 2^{116} and strength 55. Their strength then equals the highest strength one can get for an orthogonal array obtained with a known linear code [4]. □

4.2. Composition of linear functions and concatenated codes

We here focus on the functions obtained by the composition of linear functions g_i with a linear function h. Such a function $f = h \circ g$ is obviously linear; it can therefore be identified to a syndrome function. We now express the associated code in terms of concatenated codes.

We here define concatenated codes having several inner codes. Justesen codes are a particular case of this construction.

Definition 6. **[16]** Let $(\mathcal{B}_i)_{1 \leq i \leq n_e}$ be a family of $[n_b, k_b, d_b]$-linear codes over $\mathbf{F}_q$, $\mathcal{E}$ an $[n_e, k_e, d_e]$-linear code over $\mathbf{F}_{q^{k_b}}$ and $(\theta_i)_{1 \leq i \leq n_e}$ a family of isomorphisms of vector spaces

$$\theta_i : \mathbf{F}_{q^{k_b}} \rightarrow \mathcal{B}_i$$

We define the $\mathbf{F}_q$-linear isomorphism Θ as:

$$\begin{array}{rccc} \Theta : & \mathbf{F}_{q^{k_b}}^{n_e} & \rightarrow & \mathcal{B}_1 \times \ldots \times \mathcal{B}_{n_e} \\ & x = (x_1, \ldots, x_{n_e}) & \mapsto & (\theta_1(x_1), \ldots, \theta_{n_e}(x_{n_e})) \end{array}$$

The concatenated code of inner codes $(\mathcal{B}_i)_{1 \leq i \leq n_e}$ and outer code $\mathcal{E}$ is the code

$$(\mathcal{B}_i) \square_\Theta \mathcal{E} = \{(\theta_1(x_1), \ldots, \theta_{n_e}(x_{n_e})), \text{ where } (x_1, \ldots, x_{n_e}) \in \mathcal{E}\}$$

This code is a linear code over $\mathbf{F}_q$ of length $n_b n_e$, dimension $k_b k_e$ and minimum distance $d_b d_e$.

PROPOSITION 11 *Let $(g_i)_{1 \leq i \leq k}$ be a family of k linear t-resilient functions*

$$\begin{array}{rccc} g_i : & \mathbf{F}_q^n & \rightarrow & \mathbf{F}_q^d \\ & x_i & \mapsto & x_i G_i^T \end{array}$$

where G_i is a systematic generator matrix of an $[n, d, t+1]$-linear code over $\mathbf{F}_q$.
Let ψ be an isomorphism from $\mathbf{F}_{q^d}$ onto $\mathbf{F}_q^d$ and Ψ_j the associated isomorphism

$$\begin{array}{rccc} \Psi_j : & (\mathbf{F}_{q^d})^j & \rightarrow & (\mathbf{F}_q)^{dj} \\ & (x_1, \ldots, x_j) & \mapsto & (\psi(x_1), \ldots, \psi(x_j)) \end{array}$$

Let then h be a linear r-resilient function over $\mathbf{F}_{q^d}$ defined by

$$\begin{array}{rccc} h : & (\mathbf{F}_{q^d})^k & \rightarrow & \mathbf{F}_q^{d\ell} \\ & x & \mapsto & \Psi_\ell \left[\Psi_k^{-1}(x) G^T\right] \end{array}$$

where G is a generator matrix of a $[k, \ell, r+1]$-linear code over $\mathbf{F}_{q^d}$.

The composed function $f = h \circ g$ is then a linear $[(r+1)(t+1) - 1]$-resilient function which can be written as

$$\begin{array}{rccc} f : & \mathbf{F}_q^{nk} & \rightarrow & \mathbf{F}_q^{d\ell} \\ & x & \mapsto & x M^T \end{array}$$

where M is a generator matrix of the $[kn, d\ell, (t+1)(r+1)]$-linear code $(\mathcal{C}_i)\square_\Theta\mathcal{E}$ and where the isomorphism $\Theta = (\theta_1, \ldots, \theta_k)$ is defined by

$$\begin{array}{rccc} \theta_i\text{:} & \mathbf{F}_q^d & \rightarrow & \mathcal{C}_i \\ & x & \mapsto & \psi(x)G_i \end{array}$$

Proof: Since $f = h \circ g$ is linear, we only have to prove that $f^{-1}(0) = ((\mathcal{C}_i)\square_\Theta\mathcal{E})^\perp$. Let $x \in ((\mathcal{C}_i)\square_\Theta\mathcal{E})^\perp$ and let v be its image under g. We now consider the vector $\bar{v} \in (\mathbf{F}_q^n)^k$ defined by

$$\forall 1 \leq i \leq k, \;\; \bar{v}_i = (v_i, 0, \ldots, 0)$$

Since all matrices G_i are in systematic form, we have $g(\bar{v}) = v = g(x)$. For all index i, $\bar{v}_i$ can then be written as the sum of x_i and a codeword of $\mathcal{C}_i^\perp$. We then get

$$\forall u \in \mathcal{E}, \;\; \bar{v} \cdot \Theta(u) = x \cdot \Theta(u) = 0$$

since x is in the dual code of $(\mathcal{C}_i)\square_\Theta\mathcal{E}$. On the other hand we have for all u in $\mathcal{E}$:

$$\begin{aligned} \bar{v} \cdot \Theta(u) &= \sum_{i=1}^{k} \bar{v}_i(\psi(u_i)G_i) \\ &= \sum_{i=1}^{k} v_i\psi(u_i) \\ &= \Psi_k^{-1}(v) \cdot u \end{aligned}$$

We then deduce that $\Psi_k^{-1}(v)$ is an element of $\mathcal{E}^\perp$. We therefore conclude that

$$f(x) = \Psi_\ell\left(\Psi_k^{-1}(v)G^T\right) = 0$$

Since both vector-spaces $f^{-1}(0)$ and $((\mathcal{C}_i)\square_\Theta\mathcal{E})^\perp$ have the same dimension, we have proved that f is associated to the concatenated code $(\mathcal{C}_i)\square_\Theta\mathcal{E}$. ■

This proposition also enables us to explicitly describe the codewords of the dual of a concatenated code.

COROLLARY 5 *Let $(\mathcal{B}_i)_{1\leq i\leq n_e}$ be a family of $[n_b, k_b, d_b]$-linear codes over $\mathbf{F}_q$, $\mathcal{E}$ an $[n_e, k_e, d_e]$-linear code over $\mathbf{F}_{q^{k_b}}$ and $\Theta = (\theta_1, \ldots, \theta_{n_e})$ an $\mathbf{F}_q$-linear isomorphism from $\mathbf{F}_{q^{k_b}}^{n_e}$ onto $\mathcal{B}_1 \times \ldots \times \mathcal{B}_{n_e}$ defined by*

$$\begin{array}{rccc} \theta_i : & \mathbf{F}_{q^{k_b}} & \rightarrow & \mathcal{B}_i \\ & x & \mapsto & \psi(x_i)G_i \end{array}$$

where G_i is a systematic generator matrix of $\mathcal{B}_i$ and ψ is an isomorphism from $\mathbf{F}_{q^{k_b}}$ onto $\mathbf{F}_q^{k_b}$.

The dual of the concatenated code $(\mathcal{B}_i)\square_\Theta\mathcal{E}$ then consists of all codewords of $\mathcal{E}^\perp$ in which each component y_i is replaced by a vector of $\mathbf{F}_q^{n_b}$ with syndrome y_i relatively to $\mathcal{B}_i^\perp$.

$$(\mathcal{B}_i)\square_\Theta\mathcal{E} = \{(x_1, \ldots, x_{n_e}) \text{ where } (\psi^{-1}(x_1G_1^T), \ldots, \psi^{-1}(x_{n_e}G_{n_e}^T)) \in \mathcal{E}^\perp\}$$

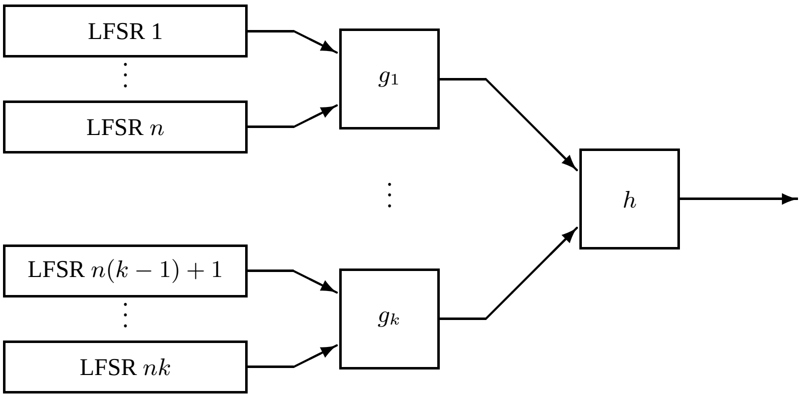

Figure 2. Combining LFSRs with a composed function

4.3. Application to combining functions

These resilient functions obtained by composition are particularly appropriate for combining LFSRs. Their use enables to reduce the number of operations required for computing the output of the pseudo-random generator from the outputs of the registers since all functions g_i can be evaluated in parallel (see Fig 2).

Another advantage of this construction arises when the combining function is used as a secret key. In this case the function is transmitted as the sequence of its outputs, *i.e.* ℓq^n q-ary digits for $f : \mathbf{F}_q^n \rightarrow \mathbf{F}_q$. If a composed function is used, we only have to send the small functions $(g_i)_{1 \leq i \leq k}$ and h, *i.e.* $(kdq^n + q^{kd})$ digits, while transmitting any function for combining kn q-ary LFSRs requires q^{kn} digits. For instance we have constructed in a previous example a Boolean resilient function for combining 12 LFSRs. This function can be described with only 56 bytes (even 32 bytes if we take $g_1 = g_2$) instead of 512 bytes in the general case.

5. Other related cryptographic objects

The original interest of correlation-immune functions in cryptography consists in conceiving pseudo-random generators by combining several LFSRs. But some other applications appeared after Siegenthaler's work. For instance Maurer and Massey [25] defined a whole class of pseudo-random generators, called perfect local randomizers, which lead to a provably-secure stream cipher under some conditions. Similar objects appear in the design of some conventional cryptographic primitives: in [32] Schnorr and Vaudenay recommend that the diffusion boxes of a primitive should realize perfect diffusion. We show here that these objects are connected with correlation-immune functions and we generalize them to any finite alphabet.

5.1. Perfect local randomizers over a finite alphabet

Since a pseudo-random generator transforms a k-digit secret sequence into a longer one, such a running-key can obviously not be completely random and the associated stream cipher can not be provably secure. However Maurer and Massey defined running-key generators, called the *perfect local randomizers* [25], leading to a provably-secure stream cipher under the assumption that the enemy is able to obtain only a limited number of plaintext digits. We here generalize this definition to any finite alphabet:

Definition 7. Let $\mathcal{F}$ be a finite alphabet. A function $f : \mathcal{F}^k \rightarrow \mathcal{F}^n$ where $k < n$ is a (k, n)*-perfect local randomizer of order* t over $\mathcal{F}$ if any subset of t or less digits of the output is a set of independent uniformly distributed digits when the k input digits are uniformly random.

This means that the knowledge of t digits of the output of a perfect local randomizer of order t does not suffice for deducing the value of any other digit of this output. An additive stream cipher using such a running-key generator is therefore provably-secure if we assume that the enemy cannot have access to more than t digits of the plaintext in a known-plaintext attack.

This concept exactly corresponds to the combinatorial structure of an orthogonal array. All results of Section 2 then apply. We sum up these properties in the following characterizations of the notion of perfect local randomizer.

PROPOSITION 12 *Let $\mathcal{F}$ be a finite alphabet with q elements. The following assertions are equivalent:*

1. *The function $f : \mathcal{F}^k \rightarrow \mathcal{F}^n$ where $k < n$ is a (k, n)-perfect local randomizer of order t over $\mathcal{F}$.*
2. *The array whose rows consist of the vectors $(f(x))_{x \in \mathcal{F}^k}$ is an orthogonal array with n constraints, of size q^k and strength t over $\mathcal{F}$.*
3. *The function $\phi : \mathcal{F}^n \rightarrow \mathbf{F}_2$ defined by $\phi(x) = 1$ if and only if $x \in f(\mathcal{F}^k)$ is t-th order correlation-immune over $\mathcal{F}$.*
4. *The function f is the encoder for a code of length n, size q^k and dual distance $t + 1$ over $\mathcal{F}$ provided $\mathcal{F}$ is endowed with the structure of an Abelian group.*

5.2. Multipermutations

Correlation-immune functions also appear in the design of conventional cryptographic primitives which consist of small boxes connected by a graph structure as many secret-key ciphers or hash functions. Following Shannon's classification [34] we distinguish two different types of boxes in such a primitive depending on their action on the data:

- *confusion boxes* which aim at concealing any algebraic or statistical structure of the input data.

- *diffusion boxes* which aim at diffusing any modification of their inputs in their outputs. The main purpose of using such a box in a secret-key cipher is that the whole information contained by the secret key and by the plaintext spreads into the ciphertext. They are also essential in hash functions because their use avoids some collision attacks.

Many criteria were developed for confusion boxes (strict avalanche criterion, propagation criterion . . .). One of the strongest conditions is that they should contain perfect nonlinear or bent functions [30, 27]. Schnorr and Vaudenay [32] claimed that diffusion boxes should be multipermutations.

Definition 8. A (r, n) multipermutation over a finite alphabet $\mathcal{F}$ is a function π from $\mathcal{F}^r$ to $\mathcal{F}^n$ such that 2 different $(r+n)$-tuples of the form $(x, \pi(x))$ differ in at least $n+1$ positions.

The use of a multipermutation in a box with r inputs and n outputs implies that a modification of t values amongst all inputs and outputs of the box leads to a modification of at least $(n - t + 1)$ other inputs and outputs. This therefore realize perfect diffusion in the sense that a modification of only one input spreads into all the outputs. Another consequence of this property is that the knowledge of any $(r - 1)$ or less values amongst all inputs and outputs of such a box does not permit to determine any of the other inputs/outputs.

Multipermutations are essential in the design of cryptographic primitives since functions which do not realize perfect diffusion may be subject to some clever cryptanalysis in which the flow of information is controlled throughout the computation network. As an illustration of this statement, Vaudenay [40] constructed collisions to MD4 restricted to its first two rounds and he showed that some generalizations of SAFER are vulnerable. This criterion has been applied to the design of the ciphers SHARK [29] and SQUARE [12]: the diffusion layer of both of these block ciphers contains linear multipermutations defined by Reed-Solomon codes.

Since multipermutations obviously correspond to orthogonal arrays of maximal strength [39], we obtain the following characterizations.

PROPOSITION 13 *Let $\mathcal{F}$ be an alphabet with q elements. The following assertions are equivalent:*

1. *The function $\pi : \mathcal{F}^r \to \mathcal{F}^n$ is an (r, n)-multipermutation over $\mathcal{F}$.*

2. *The array whose rows are the vectors $(x, \pi(x))_{x \in \mathcal{F}^r}$ is an orthogonal array with $r + n$ constraints, of size q^r and strength r over $\mathcal{F}$.*

3. *The code whose codewords are the $(r + n)$-tuples $(x, \pi(x))_{x \in \mathcal{F}^r}$ is an MDS code of length $r + n$ and size q^r.*

4. *The function g_π from $\mathcal{F}^r$ onto $\mathcal{F}^{r+n}$ defined by $g_\pi(x) = (x, \pi(x))$ is an $(r, r + n)$-perfect local randomizer of order r over $\mathcal{F}$.*

5. *The function f_π from $\mathcal{F}^{r+n}$ onto $\mathbf{F}_2$ defined by $f_\pi(x, y) = 1$ if and only if $y = \pi(x)$ is r-th order correlation-immune over $\mathcal{F}$.*

In practice cryptographic primitives use multipermutations over $\mathbf{F}_{2^m}$. This means that the inputs and outputs of the corresponding diffusion box are considered as elements of the field $\mathbf{F}_{2^m}$. However all the arguments developed in [40] for the use of multipermutations can also be applied at the bit level: the security of a function may then be weakened if it does not perform a high diffusion at the bit level, *i.e.* when its inputs and outputs are considered as binary strings of length m. At the binary level the diffusion performed by a multipermutation then corresponds to the correlation-immunity order of the associated Boolean function f_π over $\mathbf{F}_2$. This order t has indeed the following cryptographic significance: the knowledge of any $t-1$ bits of inputs and outputs of the box does not allow to determine any of the other bits. We now consider f_π as a Boolean function and we first give some bounds on the degree of its algebraic normal form.

PROPOSITION 14 *Any (r,n) multipermutation π over $\mathbf{F}_{2^m}$ corresponds to a Boolean function $f_\pi : \mathbf{F}_2^{m(r+n)} \rightarrow \mathbf{F}_2$ which is r-th order correlation-immune over $\mathbf{F}_{2^m}$. Moreover the degree of the algebraic normal form of f_π satisfies:*

$$mn - 1 + \max_{i,j} degree(\pi_{i,j}) \leq d \leq m(r+n) - r$$

where $\pi = (\pi_1, \ldots, \pi_n)$ is considered as a function from $\mathbf{F}_2^{mr}$ to $\mathbf{F}_2^{mn}$ and $\pi_{i,j}$ is the j-th binary component of π_i.

Proof: The right hand of the inequality directly comes from Theorem 5. The left one can be deduced from the explicit form of f_π: let us consider π as a set of mn Boolean functions defined by:

$$\begin{array}{cccc} \pi_{i,j} : & \mathbf{F}_2^{mr} & \rightarrow & \mathbf{F}_2 \\ & (x_{1,0}, \ldots, x_{r,m-1}) & \mapsto & \pi_{i,j}(x_{1,0}, \ldots, x_{r,m-1}) \end{array}$$

By definition $f_\pi(x_{1,0}, \ldots, x_{r+n,m-1}) = 1$ if and only if, for all $1 \leq i \leq n$ and $0 \leq j < m$, $x_{r+i,j} = \pi_{i,j}(x_{1,0}, \ldots, x_{r,m-1})$. We then obtain the following algebraic normal form of f_π

$$f_\pi(x) = \prod_{1 \leq i \leq n} \prod_{0 \leq j \leq m-1} [\pi_i^{(j)}(x_1^{(0)}, \ldots, x_r^{(m-1)}) - x_{r+i}^{(j)} - 1]$$

which contains all the monomials $\pi_{k,\ell}(x) \prod_{(i,j) \neq (k,\ell)} x_{r+i,j}$. Its degree is therefore greater than or equal to $mn - 1 + \max_{i,j} deg(\pi_{i,j})$. ■

Applying Siegenthaler's inequality to f_π gives an upper bound on its binary correlation-immunity order depending on its degree.

THEOREM 8 *Let π be an (r,n) multipermutation over $\mathbf{F}_{2^m}$ and let $f_\pi : \mathbf{F}_2^{m(r+n)} \rightarrow \mathbf{F}_2$ be the associated Boolean function. Its binary correlation-immune order t then satisfies*

$$r \leq t \leq mr - \max_{i,j} degree(\pi_{i,j})$$

Proof: The binary correlation-immunity order t is obviously greater than r. The second part of the inequality directly comes from Siegenthaler's inequality and from the remark associated to Theorem 4. In fact we have

$$\frac{|f_\pi^{-1}(1)|}{2^t} = 2^{mr-t} \equiv 0 \bmod 2 \quad\text{and}\quad \frac{|f_\pi^{-1}(0)|}{2^t} = 2^{mr-t}(2^{mn}-1) \equiv 0 \bmod 2$$

since Bush bound ensures that $t < mr$ because it points out the non-existence of binary orthogonal arrays of size 2^{mr}, strength mr with $n(r+m)$ constraints provided $mr > 1$.

■

EXAMPLE:

$$\begin{array}{llll} \text{Let } \pi : & \mathbf{F}_8^2 & \to & \mathbf{F}_8^2 \\ & (x;y) & \mapsto & ((x^3+y^3)^3; (x^3+R(y^3)+(y^3 \wedge \alpha))^3) \end{array}$$

where α is a root of X^3+X+1, R denotes the circular rotation to the right, $+$ is the bitwise XOR and $\wedge$ the bitwise AND.

Schnorr and Vaudenay proved in [32, Theorem 4] that this function is a (2,2)-multipermutation over $\mathbf{F}_8$.

We now consider the Boolean function $\pi_{1,0}$ corresponding to the low-weight component of $\pi_1(x;y)$:

$$\begin{array}{rcl} \pi_{1,0} : \mathbf{F}_2^6 & \to & \mathbf{F}_2 \\ (x,y) & \mapsto & (x^3+y^3)^3_{|0} \end{array}$$

where $z_{|0}$ denotes the low-weight bit of z. The algebraic normal form of this function is

$\pi_{1,0}(x_0,x_1,x_2,y_0,y_1,y_2) = x_0+y_0+x_1y_2+x_2y_1+x_0x_1y_1+x_1y_0y_1+x_2y_0y_1+x_0x_1y_2+x_2y_0y_2+x_0x_2y_2+x_0x_2y_0y_1+x_0x_1y_0y_2$.

It then has degree 4. The previous theorem therefore gives $2 \leq t \leq 6-4$. It follows that this multipermutation performs the worst possible diffusion at the binary level.

□

6. Conclusion

Since correlation-immunity and resilience are not algebraic but purely combinatorial properties we have apprehended these notions in a very general context. We have characterized them in terms of combinatorial structures, in terms of Fourier transform and in terms of matrices. These multiple points of view make these objects powerful since they can be described in many different and complementary ways. The combinatorial approach implies for example some bounds on the maximal correlation-immunity order of a function, the Fourier transform approach enabled us to construct new resilient functions by composition, *etc*.

Correlation-immune and resilient functions over a finite field can also be expressed as a polynomial function. This other approach is essential when they are used for combining linear feedback shift registers since the nonlinearity order of this polynomial conditions the linear complexity of the resulting pseudo-random sequence. We have proved here that there is a tradeoff between the nonlinearity and the correlation-immunity order of any function over $\mathbf{F}_q$ and we have constructed a family of q-ary t-resilient functions whose nonlinearity order achieves this bound. Using these functions as combining functions is then of great interest since they provide to the resulting generator the highest possible resistance to both correlation attacks and attacks using Berlekamp-Massey algorithm. This inequality governing the degree of q-ary correlation-functions also gives a bound on the diffusion performed at the binary level by a perfect diffusion function over $\mathbf{F}_{2^m}$.

Acknowledgments

We are grateful to the anonymous reviewers for their detailed comments which improved the clarity and the coherence of the manuscript. We also wish to thank Nicolas Sendrier for many helpful discussions and Jim Massey for having pointed out to us the general proof given by Brynielsson of the Linear Combination Lemma.

References

1. C.H. Bennett, G. Brassard and J.-M. Robert, Privacy amplification by public discussion. *SIAM J. Computing*, Vol. 17, No. 2 (1988) pp. 210–229.
2. E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill (1968).
3. J. Bierbrauer, K. Gopalakrishnan and D.R. Stinson, Bounds for resilient functions and orthogonal arrays, Advances in Cryptology - CRYPTO'94 (Y.G. Desmedt, ed.), Lecture Notes in Computer Science, Springer-Verlag, New York, 839 (1994) pp. 247–256.
4. A.E. Brouwer and T. Verhoeff, An updated table of minimum-distance bounds for binary linear codes, *IEEE Transactions on Information Theory*, Vol. 39 (1993) pp. 662–677. Also available on http://www.win.tue.nl/math/dw/voorlincod.html.
5. L. Brynielsson, On the linear complexity of combined shift register sequences. Advances in Cryptology - EUROCRYPT '85 (F. Pichler, ed.), Lecture Notes in Computer Science, Springer-Verlag, New York, 219 (1986) pp. 156–160.
6. L. Brynielsson, A short proof of the Xiao-Massey lemma, *IEEE Transactions on Information Theory*, 35(6):1344, 1989.
7. P. Camion and A. Canteaut, Construction of t-resilient functions over a finite alphabet. *Advances in Cryptology - EUROCRYPT'96* (U. Maurer, ed.), Lecture Notes in Computer Science, Springer-Verlag, New York, 1070 (1996) pp. 283–293.
8. P. Camion and A. Canteaut, Generalization of Siegenthaler inequality and Schnorr-Vaudenay multipermutations, Advances in Cryptology - CRYPTO'96 (N. Koblitz, ed.), Lecture Notes in Computer Science, Springer-Verlag, New York, 1109 (1996).
9. P. Camion, C. Carlet, P. Charpin and N. Sendrier, On correlation-immune functions, Advances in Cryptology - CRYPTO'91 (J. Feigenbaum, ed.), Lecture Notes in Computer Science, Springer-Verlag, New York, 576 (1992) pp. 86–100.
10. A. Canteaut, Attaques de cryptosystèmes à mots de poids faible et construction de fonctions t-résilientes, PhD thesis, Université Paris VI, France (1996).
11. B. Chor, O. Goldreich, J. Hastad, J. Freidmann, S. Rudich and R. Smolensky, The bit extraction problem or t-resilient functions, Proc. 26th IEEE Symposium on Foundations of Computer Science (1985) pp. 396–407.
12. J. Daemen, L. Knudsen and V. Rijmen, The block cipher SQUARE, Fast Software Encryption (E. Biham, ed.), Lecture Notes in Computer Science, Springer-Verlag, New York, 1267 (1997).
13. P. Delsarte, Bounds for unrestricted codes, by linear programming, *Philips Research Reports*, Vol. 27 (1972) pp. 272–289.
14. P. Delsarte, An algebraic approach to the association schemes of coding theory, PhD thesis, Université catholique de Louvain, Belgium (1973).
15. P. Delsarte, Four fundamental parameters of a code and their combinatorial signifiance, *Information and Control*, Vol. 23, No. 5 (1973) pp. 407–438.
16. G.D. Forney, Jr, *Concatenated codes*, The MIT Press, Cambridge, MA (1966).
17. J. DJ. Golić, On the linear complexity of functions of periodic GF(q) sequences, *IEEE Transactions on Information Theory*, Vol. IT-35, No. 1 (1989) pp. 69–75.
18. K. Gopalakrishnan and D.R. Stinson, Three characterizations of non-binary correlation-immune and resilient functions, *Designs, Codes and Cryptography*, Vol. 5 (1995) pp. 241–251.

19. R. Göttfert and H. Niederreiter, On the minimal polynomial of the product of linear recurring sequences, *Finite Fields and Their Applications*, Vol. 1, No. 2 (1995) pp. 204–218.
20. M. Hall and L.J. Paige, Complete mappings of finite groups, Pacific Journal of Mathematics, Vol. 5 (1955) pp. 541–549.
21. T. Herlestam, On functions of linear shift register sequences, Advances in Cryptology - EUROCRYPT '85 (F. Pichler, ed.), Lecture Notes in Computer Science, Springer-Verlag, New York, 219 (1986) pp. 119–129.
22. R. Lidl and H. Niederreiter, *Finite fields*. Cambridge University Press (1983).
23. J.L. Massey, Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, Vol. 15 (1969) pp. 122–127.
24. U.M. Maurer, *Provable security in cryptography*, PhD thesis, ETH Zürich, Switzerland (1990).
25. U.M. Maurer and J.L. Massey, Perfect local randomness in pseudo-random sequences, Advances in Cryptology - CRYPTO'89 (G. Brassard, ed.), Lecture Notes in Computer Science, Springer-Verlag, New York, 435 (1990) pp. 100–112.
26. U.M. Maurer and J.L. Massey, Local randomness in pseudorandom sequences, *Journal of Cryptology*, Vol. 4 (1991) pp. 135–149.
27. W. Meier and O. Staffelbach, Nonlinearity criteria for cryptographic functions, Advances in Cryptology - EUROCRYPT'89 (J.-J. Quisquater and J. Vandewalle, eds.), Lecture Notes in Computer Science, Springer-Verlag, New York, 434 (1990) pp. 549–562.
28. C.R. Rao, Factorial experiments derivable from combinatorial arrangements of arrays, *J. Roy. Statist.*, Vol. 9 (1947) pp. 128–139.
29. V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers and E. De Win, The cipher SHARK, Fast Software Encryption (D. Gollmann, ed.), Lecture Notes in Computer Science, Springer-Verlag, New York, 1039 (1996).
30. O.S. Rothaus. On bent functions. *Journal of combinatorial Theory (A)*, 20:300–305, 1976.
31. R.A. Rueppel and O.J. Staffelbach, Products of linear recurring sequences with maximum complexity, *IEEE Transactions on Information Theory*, Vol. 33, No. 1 (1987) pp. 124–131.
32. C.-P. Schnorr and S. Vaudenay, Black box cryptanalysis of hash networks based on multipermutations, Advances in Cryptology - EUROCRYPT'94 (A. De Santis, ed.), Lecture Notes in Computer Science, Springer-Verlag, New York, 950 (1995) pp. 47–57.
33. E.S. Selmer, Linear recurrence relations over finite fields, PhD thesis, University of Bergen, Norway (1966).
34. C.E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, Vol. 28 (1949) pp. 656–715.
35. T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, Vol. IT-30, No. 5 (1984) pp. 776–780.
36. T. Siegenthaler, Decrypting a class of stream ciphers using ciphertext only, *IEEE Transactions on Computers*, Vol. C-34, No. 1 (1985) pp. 81–84.
37. D.R. Stinson, Resilient functions and large sets of orthogonal arrays, *Congressus Numer.*, Vol. 92 (1993) pp. 105–110.
38. D.R. Stinson and J.L. Massey, An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions, *Journal of Cryptology*, Vol. 8, No. 3 (1995) pp. 167–173.
39. S. Vaudenay, La sécurité des primitives cryptographiques, PhD thesis, Université Paris 7, France (1995).
40. S. Vaudenay, On the need for multipermutations: cryptanalysis of MD4 and SAFER, Fast Software Encryption (B. Preneel, ed.), Lecture Notes in Computer Science, Springer-Verlag, New York, 1008 (1995) pp. 286–297.
41. G. Xiao and J.L. Massey, A spectral characterization of correlation-immune combining functions, *IEEE Transactions on Information Theory*, Vol. IT-34, No. 3 (1988) pp. 569–571.
42. X. Zhang and Y. Zheng, On nonlinear resilient functions, Advances in Cryptology - EUROCRYPT'95 (L. Guillou and J.J. Quisquater, ed.) Lecture Notes in Computer Science, Springer-Verlag, New York, 921 (1995) pp. 274–288.