Cycle Structure of Permutation Functions over Finite Fields and their Applications in Deterministic Interleavers for Turbo Codes

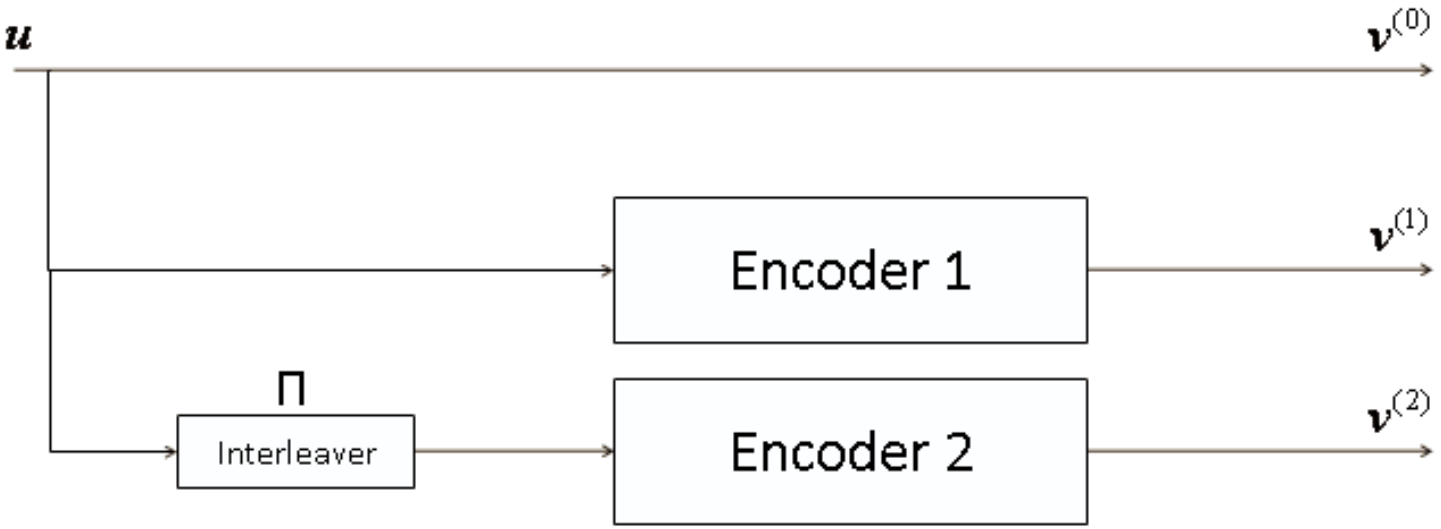
Amin Sakzad
Department of Electrical and Computer Systems Engineering
Monash University
amin.sakzad@monash.edu

[Joint work with M.-R. Sadeghi and D. Panario.]

September 18, 2012

What are they?

A basic structure of an encoder for a turbo code consists of an input sequence, two encoders and an interleaver, denoted by Π:



Types of interleavers and results

There are three types of interleavers: random, pseudo-random and deterministic interleavers. The first two classes of interleavers provide good minimum distance but they require considerable space. Deterministic interleavers have simple structure and are easy to implement; they have good performance.

Types of interleavers and results

There are three types of interleavers: random, pseudo-random and deterministic interleavers. The first two classes of interleavers provide good minimum distance but they require considerable space. Deterministic interleavers have simple structure and are easy to implement; they have good performance.

Recent results on deterministic interleavers have focused on permutation polynomials over the integer ring $\mathbb{Z}_n$. We center on permutation polynomials over finite fields and use their cycle structure to obtain turbo codes that have good performance.

Interleavers and permutations

The interleaver permutes the information block $\mathbf{x} = (x_0, \ldots, x_N)$ so that the second encoder receives a permuted sequence of the same size denoted by $\widetilde{\mathbf{x}} = (x_{\Pi(0)}, \ldots, x_{\Pi(N)})$ for feeding into the Encoder 2.

Interleavers and permutations

The interleaver permutes the information block $\mathbf{x} = (x_0, \ldots, x_N)$ so that the second encoder receives a permuted sequence of the same size denoted by $\widetilde{\mathbf{x}} = (x_{\Pi(0)}, \ldots, x_{\Pi(N)})$ for feeding into the Encoder 2.

The inverse function Π^{-1} will be needed for decoding process when we implement a de-interleaver. However, we observe that some decoding algorithms do not require de-interleavers.

Interleavers and permutations

The interleaver permutes the information block $\mathbf{x} = (x_0, \ldots, x_N)$ so that the second encoder receives a permuted sequence of the same size denoted by $\widetilde{\mathbf{x}} = (x_{\Pi(0)}, \ldots, x_{\Pi(N)})$ for feeding into the Encoder 2.

The inverse function Π^{-1} will be needed for decoding process when we implement a de-interleaver. However, we observe that some decoding algorithms do not require de-interleavers.

An interleaver Π is called self-inverse if $\Pi = \Pi^{-1}$.

Definitions and history

Let p be a prime number, $q = p^m$ and $\mathbb{F}_q$ be the finite field of order q. A permutation function over $\mathbb{F}_q$ is a bijective function which maps the elements of $\mathbb{F}_q$ onto itself. A permutation function P is called self-inverse if $P = P^{-1}$.

Definitions and history

Let p be a prime number, $q = p^m$ and $\mathbb{F}_q$ be the finite field of order q. A permutation function over $\mathbb{F}_q$ is a bijective function which maps the elements of $\mathbb{F}_q$ onto itself. A permutation function P is called self-inverse if $P = P^{-1}$.

There exist an extensive literature on permutation polynomials and permutation functions over finite fields. They have been extensively studied since Hermite in the 19th century; see Lidl and Mullen (1993) for a list of recent open problems.

Well-known permutation polynomials

- Monomials: $M(x) = x^n$ for some $n \in \mathbb{N}$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $(n, q-1) = 1$. The inverse of $M(x)$ is obviously the monomial $M^{-1}(x) = x^m$ where $nm \equiv 1 \pmod{q-1}$.

Well-known permutation polynomials

- Monomials: $M(x) = x^n$ for some $n \in \mathbb{N}$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $(n, q-1) = 1$. The inverse of $M(x)$ is obviously the monomial $M^{-1}(x) = x^m$ where $nm \equiv 1 \pmod{q-1}$.

- Dickson polynomials of the 1st kind:

$$D_n(x,a) = \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{n}{n-k} \binom{n-k}{k} (-a)^k x^{n-2k}$$

is a permutation polynomial over $\mathbb{F}_q$ if and only if $(n, q^2-1) = 1$. Thus, for $a \in \{0, \pm 1\}$, the inverse of $D_n(x,a)$ is $D_m(x,a)$ where $nm \equiv 1 \pmod{q^2-1}$.

Well-known permutation functions

- Mobius transformation: Let $a, b, c, d \in \mathbb{F}_q$, $c \neq 0$ and $ad - bc \neq 0$. Then, the function

$$T(x) = \begin{cases} \frac{ax+b}{cx+d} & x \neq \frac{-d}{c}, \\ \frac{a}{c} & x = \frac{-d}{c}, \end{cases}$$

  is a permutation function.

Well-known permutation functions

- Mobius transformation: Let $a, b, c, d \in \mathbb{F}_q$, $c \neq 0$ and $ad - bc \neq 0$. Then, the function

$$T(x) = \begin{cases} \frac{ax+b}{cx+d} & x \neq \frac{-d}{c}, \\ \frac{a}{c} & x = \frac{-d}{c}, \end{cases}$$

is a permutation function.

It's inverse is simply

$$T^{-1}(x) = \begin{cases} \frac{dx-b}{-cx+a} & x \neq \frac{a}{c}, \\ \frac{-d}{c} & x = \frac{a}{c}. \end{cases} \quad (1)$$

Well-known permutation functions

- Rédei functions: Let $\text{char}(\mathbb{F}_q) \neq 2$ and $a \in \mathbb{F}_q^*$ be a non-square element, then we have

$$(x + \sqrt{a})^n = G_n(x, a) + H_n(x, a)\sqrt{a}.$$

The Rédei function $R_n = \frac{G_n}{H_n}$ with degree n is a rational function over $\mathbb{F}_q$. The Rédei function R_n is a permutation function if and only if $(n, q + 1) = 1$.

Well-known permutation functions

- Rédei functions: Let $\text{char}(\mathbb{F}_q) \neq 2$ and $a \in \mathbb{F}_q^*$ be a non-square element, then we have

$$(x + \sqrt{a})^n = G_n(x, a) + H_n(x, a)\sqrt{a}.$$

The Rédei function $R_n = \frac{G_n}{H_n}$ with degree n is a rational function over $\mathbb{F}_q$. The Rédei function R_n is a permutation function if and only if $(n, q + 1) = 1$.

In addition, if $\text{char}(\mathbb{F}_q) \neq 2$ and $a \in \mathbb{F}_q^*$ be a square element, then R_n is a permutation function if and only if $(n, q - 1) = 1$.

Interleaver

Definition. Let P be a permutation function over $\mathbb{F}_q$ and α a primitive element in $\mathbb{F}_q$. An interleaver $\Pi_P : \mathbb{Z}_q \to \mathbb{Z}_q$ is defined by

$$\Pi_P(i) = \ln(P(\alpha^i)) \tag{2}$$

where $\ln(.)$ denotes the discrete logarithm to the base α over $\mathbb{F}_q^*$ and $\ln(0) = 0$.

Interleaver

Definition. Let P be a permutation function over $\mathbb{F}_q$ and α a primitive element in $\mathbb{F}_q$. An interleaver $\Pi_P : \mathbb{Z}_q \to \mathbb{Z}_q$ is defined by

$$\Pi_P(i) = \ln(P(\alpha^i)) \tag{2}$$

where $\ln(.)$ denotes the discrete logarithm to the base α over $\mathbb{F}_q^*$ and $\ln(0) = 0$.

There is a one-to-one correspondence between the set of all permutations over a fixed finite field $\mathbb{F}_q$ and the set of all interleavers of size q.

The need of cycle structure

Let P be a permutation function over $\mathbb{F}_q$. Then, we have $(\Pi_P)^{-1} = \Pi_{P^{-1}}$. Let P be a self-inverse permutation function over $\mathbb{F}_q$. Then, we have $\Pi_P = (\Pi_P)^{-1}$.

The need of cycle structure

Let P be a permutation function over $\mathbb{F}_q$. Then, we have $(\Pi_P)^{-1} = \Pi_{P^{-1}}$. Let P be a self-inverse permutation function over $\mathbb{F}_q$. Then, we have $\Pi_P = (\Pi_P)^{-1}$.

We pick permutation functions and apply them to produce interleavers following the above definition. This generates deterministic interleavers based on permutations on finite fields.

The need of cycle structure: continued

We are interested in self-inverse interleavers. This requires the study of the cycle structure of the underlying permutation. For self-inverse interleavers we are interested in involutions, that is, of permutations that decompose into cycles of length 1 or 2.

The need of cycle structure: continued

We are interested in self-inverse interleavers. This requires the study of the cycle structure of the underlying permutation. For self-inverse interleavers we are interested in involutions, that is, of permutations that decompose into cycles of length 1 or 2.

We are also interested in using the cycle structure of permutation polynomials to produce good turbo codes.

Previous and new results on cycle structures

The cycle structure of the following permutation polynomials is known:

- monomials x^n, (Rubio-Corrada 2004)
- Dickson polynomials $D_n(x, a)$ where $a \in \{0, \pm 1\}$, (Rubio-Mullen-Corrada-Castro 2008)
- Möbius transformation.

Previous and new results on cycle structures

The cycle structure of the following permutation polynomials is known:

- monomials x^n, (Rubio-Corrada 2004)
- Dickson polynomials $D_n(x, a)$ where $a \in \{0, \pm 1\}$, (Rubio-Mullen-Corrada-Castro 2008)
- Möbius transformation.

In this work:

- we give the cycle structure of Rédei functions.

Previous and new results on cycle structures

The cycle structure of the following permutation polynomials is known:

- monomials x^n, (Rubio-Corrada 2004)
- Dickson polynomials $D_n(x, a)$ where $a \in \{0, \pm 1\}$, (Rubio-Mullen-Corrada-Castro 2008)
- Möbius transformation.

In this work:

- we give the cycle structure of Rédei functions.
- We characterize Rédei function with a cycle of length j, and then extend this to all cycles of the same length.

Previous and new results on cycle structures

The cycle structure of the following permutation polynomials is known:

- monomials x^n, (Rubio-Corrada 2004)
- Dickson polynomials $D_n(x, a)$ where $a \in \{0, \pm 1\}$, (Rubio-Mullen-Corrada-Castro 2008)
- Möbius transformation.

In this work:

- we give the cycle structure of Rédei functions.
- We characterize Rédei function with a cycle of length j, and then extend this to all cycles of the same length.
- An exact formula for counting the number of cycles of certain length is also provided.

Cycle Structure of Mobius Interleavers

Let T be the Mobius transformation. Its cycle structure can be explained in terms of the eigenvalues of the coefficient matrix A_T associated to T

$$A_T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{3}$$

Cycle Structure of Mobius Interleavers

Let T be the Mobius transformation. Its cycle structure can be explained in terms of the eigenvalues of the coefficient matrix A_T associated to T

$$A_T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{3}$$

Theorem. (Sakzad-Sadeghi-Panario-2012) Let Π_T be an interleaver defined by T, and let A_T be as above. Then Π_T is a self-inverse interleaver if $\mathrm{Tr}(A_T) = 0$.

Rédei interleavers and their cycle structure

Definition. Let R_n be a Rédei permutation function over $\mathbb{F}_q$. The interleaver Π_{R_n} defined in (2) is called a Rédei interleaver.

Rédei interleavers and their cycle structure

Definition. Let R_n be a Rédei permutation function over $\mathbb{F}_q$. The interleaver Π_{R_n} defined in (2) is called a Rédei interleaver.

We have that $R_n^{-1} = R_m$ for m satisfying $nm \equiv 1 \pmod{q+1}$.

Rédei interleavers and their cycle structure

Definition. Let R_n be a Rédei permutation function over $\mathbb{F}_q$. The interleaver Π_{R_n} defined in (2) is called a Rédei interleaver.

We have that $R_n^{-1} = R_m$ for m satisfying $nm \equiv 1 \pmod{q+1}$.

Let $j = \mathrm{ord}_s(n)$ if $n^j \equiv 1 \pmod{s}$ and j is as smallest as possible.

Rédei interleavers and their cycle structure

Theorem. (Sakzad-Sadeghi-Panario-2012) Let j be a positive integer. The Rédei function $R_n(x, a)$ of $\mathbb{F}_q$ with $(n, q+1) = 1$ has a cycle of length j if and only if $q+1$ has a divisor s such that $j = \mathrm{ord}_s(n)$.

Rédei interleavers and their cycle structure

Theorem. (Sakzad-Sadeghi-Panario-2012) Let j be a positive integer. The Rédei function $R_n(x, a)$ of $\mathbb{F}_q$ with $(n, q+1) = 1$ has a cycle of length j if and only if $q+1$ has a divisor s such that $j = \mathrm{ord}_s(n)$.

Furthermore, the number N_j of cycles of length j of the Rédei function R_n over $\mathbb{F}_q$ with $(n, q+1) = 1$ satisfies

$$1 + \sum_{i|j} iN_i = (n^j - 1, q+1).$$

Self-inverse Rédei interleavers

Theorem. (Sakzad-Sadeghi-Panario-2012) Let $q+1 = p_0^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, and $p_0 = 2$. The permutation of $\mathbb{F}_q$ given by the Rédei function R_n has cycles of the same length j or fixed points if and only if one of the following conditions holds for each $1 \leq l \leq r$

- $n \equiv 1 \pmod{p_l^{k_l}}$,
- $j = \text{ord}_{p_l^{k_l}}(n)$ and $j | p_l - 1$,
- $j = \text{ord}_{p_l^{k_l}}(n)$, $k_l \geq 2$ and $j = p_l$.

Self-inverse Rédei interleavers

Theorem. (Sakzad-Sadeghi-Panario-2012) The Rédei function R_n of $\mathbb{F}_q$ with $(n, q+1) = 1$ has cycles of length $j = 2$ or 1 if and only if for every divisor $s > 1$ of $q+1$ we have that $n \equiv 1 \pmod{s}$ or $j = 2$ is the smallest integer with $n^j \equiv 1 \pmod{s}$.

Example

(Sakzad-Sadeghi-Panario-2012) Let $q = 7$, $n = 5$ and $a = 3 \in \mathbb{Z}_7^*$ is a non-square. Since $(5, 7+1) = 1$ and $5 \times 5 \equiv 1 \pmod 8$, we get a self-inverse Rédei function

$$R_5(x,3) = \frac{G_5(x,3)}{H_5(x,3)} = \frac{x^5 + 2x^3 + 3x}{5x^4 + 2x^2 + 2}.$$

Thus, since 3 is a primitive element of $\mathbb{F}_7$, we have

$$\begin{aligned} R_5(0,3) = 0, \quad R_5(3^1,3) = 3^6, \quad R_5(3^2,3) = 3^2, \quad R_5(3^3,3) = 3^4, \\ R_5(3^4,3) = 3^3, \quad R_5(3^5,3) = 3^5, \quad R_5(3^6,3) = 3^1. \end{aligned}$$

Hence, Π_R^5 is

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 6 & 2 & 4 & 3 & 5 & 1 \end{pmatrix}.$$

Experiments

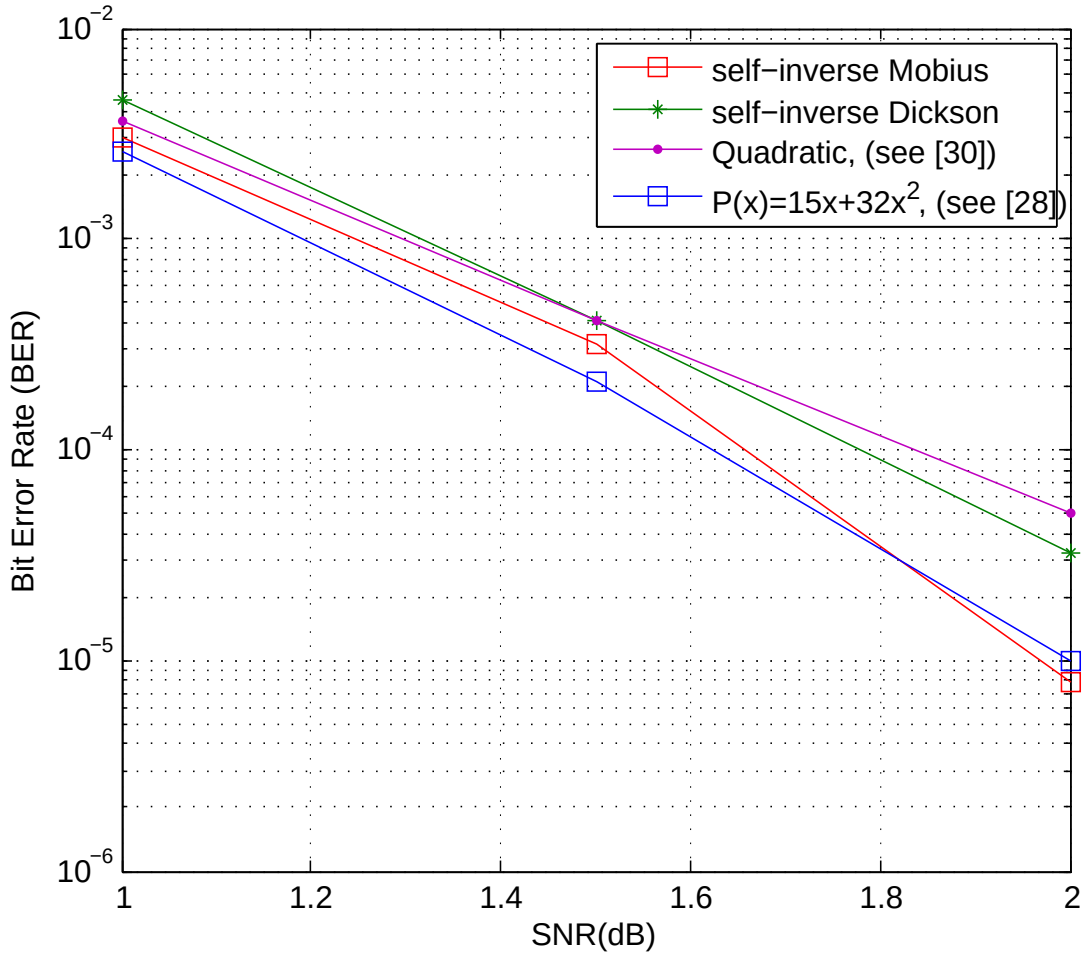
We consider turbo codes generated by two systematic recursive convolutional codes. We investigate several interleaver sizes, and report here on interleavers of size 256 only.

Experiments

We consider turbo codes generated by two systematic recursive convolutional codes. We investigate several interleaver sizes, and report here on interleavers of size 256 only.

Dimension 256 is commonly used, thus this dimension was chosen. The experiments are done based on a visual basic program using a 2.2 GHz Core2 dual processor computer.

Experiments: length 256



In SNRs between 1 and 2 Dickson and Möbius self-inverse interleavers outperform the best introduced self-inverse interleavers (quadratic interleavers) of the same size. In addition, self-inverse Möbius interleavers have the best performance between other known interleavers in SNRs larger than 1.85 (dB); between 1 and 1.85 dB the QPP interleaver (Sun-Takeshita) remains the best one.

Conclusions

We study some deterministic interleavers based on permutation functions over finite fields (in the paper we also considered Skolem sequence interleavers). Self-interleavers are simple and allow for the use of same structure in the encoding and decoding process.

Conclusions

We study some deterministic interleavers based on permutation functions over finite fields (in the paper we also considered Skolem sequence interleavers). Self-interleavers are simple and allow for the use of same structure in the encoding and decoding process.

A byproduct of this work is a study of Rédei functions in detail. We derive an exact formula for the inverse of a Rédei function. The cycle structure of these functions are given. The exact number of cycles of a certain length j is also provided.

Conclusions

We study some deterministic interleavers based on permutation functions over finite fields (in the paper we also considered Skolem sequence interleavers). Self-interleavers are simple and allow for the use of same structure in the encoding and decoding process.

A byproduct of this work is a study of Rédei functions in detail. We derive an exact formula for the inverse of a Rédei function. The cycle structure of these functions are given. The exact number of cycles of a certain length j is also provided.

For a state-of-the-art account see the forthcoming (Winter 2013?):

CRC Handbook of Finite Fields
by Gary Mullen and Daniel Panario

Some references

• S. Ahmad, "Cycle structure of automorphisms of finite cyclic groups", J. Comb. Theory, vol. 6, pp. 370-374, 1969.
• A. Cesmelioglu, W. Meidl and A. Topuzoglu "On the cycle structure of permutation polynomials", Finite Fields and Their Applications, vol. 14, pp. 593-614, 2008.
• S. Lin, D. J. Costello, "Error Control Coding Fundamentals and Application", 2nd ed., New Jeresy, Pearson Prentice Hall, 2003.
• R. Lidl and G. L. Mullen "When Does a Polynomial over a Finite Field Permute the Elements of the Field?", The American Mathematical Monthly, vol. 100, No. 1, pp. 71-74, 1993.
• R. Lidl and G. L. Mullen, "Cycle structure of dickson permutation polynomials", Mathematical Journal of Okayama University, vol. 33, pp. 1-11, 1991.
• R. Lidl and H. Niederreiter, Finite Fields, Cambridge Univ. Press, 1997.
• L. Rédei, "Uber eindeuting umkehrbare Polynome in endlichen Kopern", Acta Scientarium Mathmematicarum, vol. 11, pp. 85-92, 1946-48.
• I. Rubio, G. L. Mullen, C. Corrada, and F. Castro, "Dickson permutation polynomials that decompose in cycles of the same length", 8th International Conference on Finite Fields and their Applications, Contemporary Mathematics, vol 461, pp. 229-239, 2008.
• J. Ryu and O. Y. Takeshita, "On quadratic inverses for quadratic permutation polynomials over integer rings", IEEE Trans. Inform. Theory, vol. 52, no. 3, pp. 1254-1260, Mar. 2006.
• O. Y. Takeshita, "Permutation polynomials interleavers: an algebraic-geometric perspective", IEEE Trans. Inform. Theory, vol. 53, no. 6, pp. 2116-2132, Jun. 2007.
• O. Y. Takeshita and D. J. Costello, "New Deterministic Interleaver Designs for Turbo Codes", IEEE Trans. Inform. Theory, vol. 46, no. 3, pp. 1988-2006, Sep. 2000.
• B. Vucetic, Y. Li, L. C. Perez and F. Jiang, "Recent advances in turbo code design and theory", Proceedings of the IEEE, Vol. 95, pp. 1323-1344, 2007.