Self-Inverse Interleavers for Turbo Codes

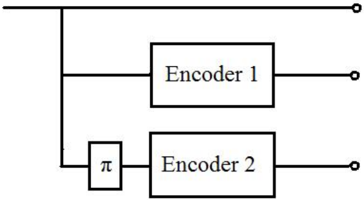
Amin Sakzad
Department of Mathematics and Computer Science
Amirkabir University of Technology
amin@math.carleton.ca

[Joint work with D. Panario, M. R. Sadeghi and N. Eshghi]

Finite Fields Workshop, July 2010

What are they?

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



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} is also necessary for decoding process when we implement a de-interleaver. 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 $P = P^{-1}$.

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 $(n, q-1) = 1$.

- 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 $(n, q^2 - 1) = 1$.

Well-known permutation functions

- Möbius 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.

- Rédei functions: Let $\mathrm{char}(\mathbb{F}_q) \neq 2$ 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 $(n, q + 1) = 1$.

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

$$\Pi_P(i) = \ln(P(\alpha^i)) \tag{1}$$

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 $\Pi_P = (\Pi_P)^{-1}$.

We pick a permutation polynomial or a permutation function and apply it to produce an interleaver following the above definition. This generates deterministic interleavers based on permutations on finite fields.

We are interested in self-inverse interleavers. This requires the study of permutations that decompose into cycles of length 1 or 2.

Previous and new results on cycle structures

Permutation monomials x^n with a cycle of length j as well as with all cycles of the same length have been characterized. The cycle structure of Dickson permutation polynomials $D_n(x, a)$ where $a \in \{0, \pm 1\}$ have been studied. Furthermore, the cycle structure of Möbius transformation have been fully described.

We give the cycle structure of Rédei functions. More precisely, 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.

Möbius interleavers

Let T be a Möbius transformation over $\mathbb{F}_q$. The Π_T as defined in (1) is called a Möbius interleaver. The inverse function of T is

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

It is easy to see that $T = T^{-1}$ when we have $a = d$, $-b = b$ and $c = -c$.

Cycle structure of Möbius transformation

Theorem. Let T be a Möbius transformation, and let t be the characteristic polynomial of the matrix A_T associated with T.

1. Suppose $t(x)$ is irreducible. If $k = \text{ord}\left(\frac{\alpha_1}{\alpha_2}\right) = \frac{q+1}{s}$, $1 \leq s < \frac{q+1}{2}$, then T has $s-1$ cycles of length k and one cycle of length $k-1$. In particular T is a full cycle if $s = 1$.
2. Suppose $t(x)$ is reducible and $\alpha_1, \alpha_2 \in \mathbb{F}_q^*$ are roots of $t(x)$ and $\alpha_1 \neq \alpha_2$. If $k = \text{ord}\left(\frac{\alpha_1}{\alpha_2}\right) = \frac{q-1}{s}$, $s \geq 1$, then T has $s-1$ cycles of length k, one cycle of length $k-1$ and two cycles of length 1.
3. Suppose $t(x) = (x-\alpha_1)^2$, $\alpha_1 \in \mathbb{F}_q^*$ where $q = p^m$. Then T has $p^{m-1}-1$ cycles of length p, one cycle of length $p-1$ and one cycle of length 1.

Self-inverse Möbius interleavers

In order to have these cycles in terms of cases of the above theorem we consider:

1. If the polynomial t is irreducible and $tr(A_T) = 0$, then we have $\frac{q+1}{2} - 1$ cycles of length two and one cycle of length one.
2. If t is reducible and $tr(A_T) = 0$, then we have $\frac{q-1}{2} - 1$ cycles of length 2 and three cycles of length 1.
3. This happens only if $p = 2$. The permutation T has $2^{m-1} - 1$ cycles of length 2 and two cycles of length 1 where $q = 2^m$.

Example. Let $n = 3$, $a = \alpha^3 = d$, $b = \alpha^2$ and $c = \alpha$. Then we get

$$T(x) = \begin{cases} \frac{\alpha^3 x + \alpha^2}{\alpha x + \alpha^3} & x \neq \alpha^2, \\ \alpha^2 & x = \alpha^2. \end{cases}$$

It is clear that T is a permutation function over $\mathbb{F}_{2^3}$ with compositional inverse T. A Möbius interleaver $\Pi_T : \mathbb{Z}_8 \to \mathbb{Z}_8$ can be defined by $\Pi_T(i) = \ln(T(\alpha^i))$. Thus, we get

$$\begin{array}{ll} T(0) = \frac{\alpha^2}{\alpha^3} = \alpha^{-1} = \alpha^6, & T(\alpha^1) = \frac{\alpha}{\alpha^5} = \alpha^{-4} = \alpha^3, \\ T(\alpha^2) = \alpha^2, & T(\alpha^3) = \frac{1}{\alpha^6} = \alpha^{-6} = \alpha^1, \\ T(\alpha^4) = \frac{\alpha^6}{\alpha^2} = \alpha^4, & T(\alpha^5) = \frac{\alpha^4}{\alpha^4} = 1 = \alpha^7, \\ T(\alpha^6) = \frac{0}{\alpha} = 0, & T(\alpha^7) = \frac{\alpha^5}{1} = \alpha^5. \end{array}$$

The above equalities induce the following Möbius interleaver

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 2 & 1 & 4 & 7 & 0 & 5 \end{pmatrix}.$$

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 (1) is called a Rédei interleaver.

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

Theorem. 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 $j = \text{ord}_s(n)$. 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

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

Self-inverse Rédei interleavers

Theorem. 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 $1 \leq l \leq r$

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

Theorem. 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 $n^2 \equiv 1 \pmod{s}$.

Example: Let $q=7$, $n=5$ and $a=3\in\mathbb{Z}_7^*$ is a non-square. Since $(5,7+1)=1$ and $5.5\equiv 1 \pmod 8$, 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

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

We observe that the three fixed points are 0, $3^2\equiv 2 \pmod 7$, and $3^5\equiv 5 \pmod 7$ in contrast with the monomial case.

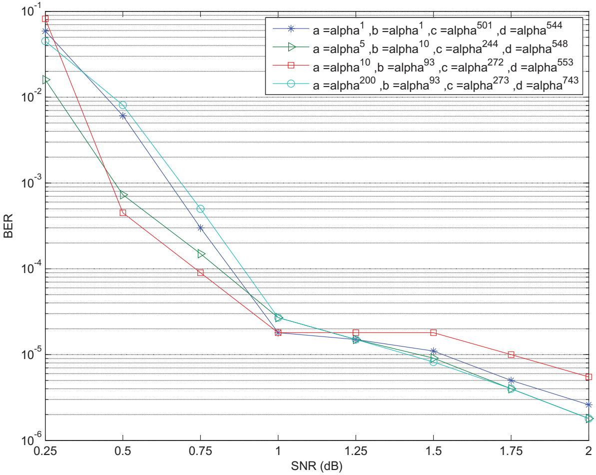
Conclusions and further work

We study some deterministic interleavers based on permutation functions over finite fields. Four well-known permutation functions including polynomials and rational functions are investigated. In the paper we also considered Skolem sequence interleavers.

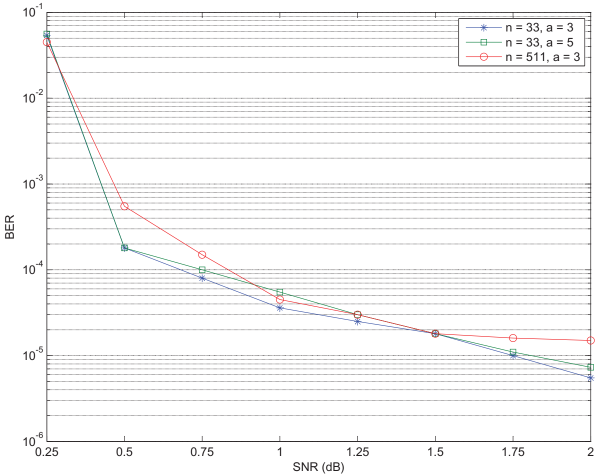
A byproduct of this work is a study of Rédei functions in detail. We derive an exact formula for the inverse of a Rédei function. The cycle structure of these functions are given. The exact number of cycles of a certain length j is also provided.

We are measuring their performance via simulations. Self-interleavers are simple and allow for the use of same structure in the encoding and deconding process. We expect that there will be considerable savings.

Conclusions



Conclusions



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.