FACTA UNIVERSITATIS (NIŠ)
SER.: ELEC. ENERG. vol. 21, no. 3, December 2008, 365-372

On a Large Class of Non-Linear Coding Methods Based on Boolean Invertible Matrices

Costas Karanikas and Nikolaos D. Atreas

Abstract: The main target of this work is to construct a large enumerated class of non-linear coding methods, based on a discrete invertible transform called Riesz Product, which is associated to a class of boolean invertible matrices of order $m \times m$. The particular class of matrices is uniquely determined by a couple of permutations of the first m natural numbers $\{1,2,...,m\}$, so for any $m = 1,2,3,...$, we get at least $(m!)^2$ different non-linear coding methods.

The resulting encoding/decoding method is very fast and requires low memory. It can be used both as a new encryption tool or as a boolean random generator.

Keywords: Non-linear coding, Boolean invertibile matrices, permutations, Riesz products.

1 Introduction

THE MAIN TENET of this work is to construct a large class of non-linear encryption methods, such that for any message of length $m = 2,3,...$, any pair of numbers smaller than or equal to $m!$ determines uniquely a non-linear encryption method. The stages of this process are the following:

Stage 1: For any pair of permutations q_1 and q_2 of the first m natural numbers, we define a unique boolean matrix of order $m \times m$, called Z matrix.

Stage 2: We define non-linear transforms, called Riesz Product Transforms (RP Transforms) associated to Z matrices.

Manuscript received on October 12, 2008.

The authors are with Department of Informatics, Aristotle University of Thessaloniki, 54124, Thessaloniki, Greece

Let $\mathbb{R}$ be the space of all real numbers and let $C[0,1]$ be the space of all continuous functions on $[0,1]$. Inspired by the well known Riesz Product transform:

$$\mathbb{R}^m \to C[0,1]: \ a=\{a_1,a_2,...,a_m\} \to \prod_{k=1}^{m}(1+a_k\cos(2\pi 4^k x))$$

associated with trigonometric functions (due to F. Riesz's idea to construct singular measures and trigonometric dynamical systems (1912)), we define the following:

Definition 1. *Let $H=\{h_{k,n}\}$ be a matrix of order $m\times m$ and let $a=\{a_1,...,a_m\}$ be a sequence of reals. A Riesz Product transform (RP coding), associated to the matrix H and to the sequence of coefficients a is the map*

$$RP:\mathbb{R}^m\to\mathbb{R}^m: \ RP(a)=\prod_{k=1}^{m}(1+a_k h_{n,k}).$$

Theorem 1. *Let $H=\{h_{k,n}\}$ be an invertible boolean matrix of order $m\times m$ and let $a_k>-1$ for any k, then the RP coding associated to the matrix H is invertible.*

In section 2 we present an overview on Riesz Product transforms.

In general, matrix inversion is expensive in storage and computations. So, we seek for boolean invertible matrices whose corresponding RP coding has low time and memory requirements. In section 3 we introduce a large class of matrices called Z-class meeting our criteria.

In section 4 we present several examples of boolean RP transforms and we use RP transform to create a boolean random generator.

Section 5 is the appendix containing proofs of the theorems.

2 An Overview on RP Transforms

For the rest of this section we present the initial ideas and previous works related on boolean RP transforms.

In [1] and [2] we constructed large classes of sparse boolean matrices, i.e. matrices with a low number of non zero entries. These matrices have sparse inverse matrices with advantages in computations and have been used for several applications, i.e. compression, detection of local information and prediction. Below, we present a typical example of such a matrix and its inverse:

$$U=\begin{pmatrix}1&1&1&1&1&1\\1&1&0&0&0&0\\0&0&1&1&0&0\\1&0&0&0&0&0\\0&0&1&0&0&0\\0&0&0&0&1&0\end{pmatrix},\quad U^{-1}=\begin{pmatrix}0&1&0&1&0&0\\0&0&0&-1&0&0\\0&0&1&0&1&0\\0&0&0&0&-1&0\\0&0&0&0&0&1\\1&-1&-1&0&0&-1\end{pmatrix}$$

We mention here that all these matrices are special cases of the class Z of matrices we shall define in section 3.

In [3] and [4], we introduced the discrete RP transform with respect to a class of orthonormal matrices $H(m)$ of order $m\times m$. The particular matrices $H(m)$ may be considered as a generalization of the usual Haar matrices, since their construction was based on dilation and translation operations on matrices and every row of $H(m)$ is an unbalanced Haar function.

Example We present below examples of Haar matrices corresponding to $m=3$ and $m=6$:

$$H(3)=\begin{pmatrix}\frac{1}{\sqrt{3}}&\frac{1}{\sqrt{3}}&\frac{1}{\sqrt{3}}\\\frac{1}{\sqrt{6}}&\frac{1}{\sqrt{6}}&-\frac{\sqrt{2}}{\sqrt{3}}\\\frac{1}{\sqrt{2}}&-\frac{1}{\sqrt{2}}&0\end{pmatrix}H(6)=\begin{pmatrix}\frac{1}{\sqrt{6}}&\frac{1}{\sqrt{6}}&\frac{1}{\sqrt{6}}&\frac{1}{\sqrt{6}}&\frac{1}{\sqrt{6}}&\frac{1}{\sqrt{6}}\\\frac{1}{2\sqrt{3}}&\frac{1}{2\sqrt{3}}&\frac{1}{2\sqrt{3}}&\frac{1}{2\sqrt{3}}&-\frac{1}{\sqrt{3}}&-\frac{1}{\sqrt{3}}\\\frac{1}{2}&\frac{1}{2}&-\frac{1}{2}&-\frac{1}{2}&0&0\\\frac{1}{\sqrt{2}}&-\frac{1}{\sqrt{2}}&0&0&0&0\\0&0&\frac{1}{\sqrt{2}}&-\frac{1}{\sqrt{2}}&0&0\\0&0&0&0&\frac{1}{\sqrt{2}}&-\frac{1}{\sqrt{2}}\end{pmatrix}.$$

We proved that the resulting Haar RP transform is invertible and the coefficients $\{a_n : n=1,...,m\}$ are computed via the following:

$$a_n=\begin{cases}\langle t,h_1\rangle-\sqrt{m}, & n=1\\ \frac{\langle t,h_n\rangle}{\prod_{k=1}^{n-1}(1+a_k h_{k,n_0})}, & n=2,...,m\end{cases}$$

where $\langle\ ,\ \rangle$ is the usual inner product and h_n are the rows of the corresponding Haar matrix H.

Our first attempt to construct a boolean non linear discrete transform was based on the well known Walsh system. More general we proved:

Theorem 2. *(See [5]) Let $\{a_k : k=1,...,m\}$ be a boolean sequence and let $\Theta(m)=\{\theta_{n,j} : |\theta_{n,j}|<\pi,\ j=1,...,m\}$ be an invertible matrix whose columns satisfy the*

following:

$$-\pi \leq \sum_{n=1}^{m} \theta_{n,j} \leq \pi,\ j = 1,...,m.$$

If $t = \{t_j = |t_j| e^{i \arg t_j},\ j = 1,...,m\}$ *is a sequence of complex numbers, then there is a unique sequence of boolean coefficients* $\{a_n : n = 1,...,m\}$*, such that:*

$$t_j = \prod_{n=1}^{m} (1 + a_n e^{i\theta_{n,j}}).$$

Moreover, the coefficients $\{a_n : n = 1,...,m\}$ *are computed via the following matrix equation:*

$$a = 2\Theta^{-1} C(t)$$

where $a = [a_n]$ *and* $C(t) = [\arg t_n]$ *are column matrices of order* $m \times 1$.

Example: Walsh-type Riesz Products

Since Walsh orthogonal matrices $W(2k),\ k = 1,...,$ produced from the Walsh system $\{w_0, w_1, ..., w_{2^k}\}$ (see [5]) have rows with zero mean, except for the first row which is the constant row $(1,...,1)$, orthogonal matrices of the form

$$\Theta(2^k) = \frac{\pi}{2^k} W(2^k)$$

satisfy Theorem 2. We present below two examples:

$$\Theta(2) = \frac{\pi}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \Theta(4) = \frac{\pi}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

3 A Class of Boolean Matrices Determined by Two Permutations

Let $\rho = \{\rho_1, ..., \rho_m\}$ be a permutation of the set of the first m natural numbers and let ρ^{-1} is the inverse permutation of ρ, e.g. if $\rho = \{3,1,2,4\}$, then $\rho^{-1} = \{2,3,1,4\}$.

We call **restricted order of a permutation** $\rho = \{\rho_1, ..., \rho_m\}$ the vector $F(\rho) = \{\sigma_1, ..., \sigma_m\}$, where $\sigma_m = r_m$ whenever $k = m$, whereas for $k = 1,2,...,m-1$, σ_k is the position of the number k of the permutation of the first k natural numbers derived from ρ by erasing all numbers $k+1,...,m$. Clearly, $\sigma_k \leq k,\ k = 1,2,...,m$. The set of all images of F can be considered as a tree, such that from each node in k generation we have exactly $k+1$ branches $k = 0,1,..,m-1$. We call this tree m-**natural tree**. This tree is shown in Figure 1.

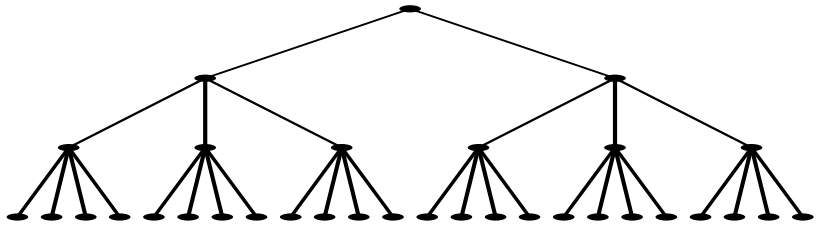

Fig. 1. *m*-natural tree.

Example: $F(\{2,5,4,3,1\}) = \{1,1,2,2,2\}$ and $F(\{2,4,3,1,5\}) = \{1,1,2,2,5\}$.

Theorem 3. *The map F from the set of all permutations* $\rho = \{\rho_1,...,\rho_m\}$ *to the m natural tree is one to one. Moreover there is a one to one correspondence between any leaf of the m-natural tree and all integers* $0 \leq k < m!$.

Let $\rho = \{\rho_1,...,\rho_m\}$ and $r = \{r_1,...,r_m\}$ be two permutations and let $F(r) = \{\sigma_1,...,\sigma_m\}$, we call **Z matrix determined by** ρ **and** r the matrix determined by the following two conditions:

If we denote the support of the k-row of the matrix Z by $supp\{Z_k\} = \{j \in \{1,...,m\} : Z_{k,j} \neq 0\}$ then:

1. a) whenever $\sigma_k < k$: $\text{supp}\{Z_k\} \subset \text{supp}\{Z_{\sigma_k}\}$ and $\text{supp}\{Z_k\} \cap \text{supp}\{Z_j\} = \varnothing,\ \sigma_k < j < k,\ k = 2,...,m$.

   b) whenever $\sigma_k = k$: $\text{supp}\{Z_k\} \cap \text{supp}\{Z_j\} = \varnothing$,for any $j \neq k$.

2. $\rho_k \in supp\{Z_k\}$ and$Z_{j,\rho_k} = 0$ for any $j > k,\ k = 1,...,m-1$.

Examples of matrices Z satisfying conditions (1) and (2):

$$Z = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, ...$$

The first matrix Z of order 3×3 is determined by the permutation $\rho = \{3,1,2\}$ and the restricted order $F(r) = \{1,1,1\}$, where $r = \{3,2,1\}$.

The second matrix matrix Z of order 6x6 is determined by the permutation $\rho = \{5,2,4,3,1,6\}$ and the restricted order $F(r) = \{1,1,1,3,2,2\}$ where $r = \{3,6,5,2,4,1\}$.

From now on we call the class of matrices satisfying (1) and (2) class Z of matrices.

Theorem 4. *Each matrix in the class Z is invertible.*

Corollary 1. *Any pair of numbers less than m! corresponds to a unique Z matrix.*

4 Examples of RP Transforms and Random Generators

By Theorem 1, the main advantage of RP coding is the fact that any boolean invertible matrix provides RP decoding. Since all Z matrices are invertible, their associated RP codings are invertible.

Example

$$Z = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad Z^{-1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 1 & -1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Corollary 2. *The composition of RP transforms associated to Z matrices is also an invertible transform.*

A fast algorithm to compute RP transform of a Z matrix is given by the following:

Theorem 5. *The RP transform $t_n = \prod_{k=1}^{m}(1 + a_k Z_{k,n})$ of a Z matrix determined from two permutations $\rho = \{\rho_1, ..., \rho_m\}$ and $r = \{r_1, ..., r_m\}$ satisfies the following:*

$$t_n = \prod_{k=1}^{\rho_n^{-1}} (1 + a_k)^{b(n,k)},\ n = 1, ..., m$$

where

$$b(n,k) = \begin{cases} 1 & \text{whenever} \quad \text{supp}(Z_{\rho_n^{-1}}) \cap \text{supp}(Z_k) \neq \emptyset \\ 0 & \text{otherwise} \end{cases}.$$

Compositions of RP transforms create boolean random generators based on the following:

Theorem 6. *Let $t = \{t_n,\ n = 1,...,m\}$ be a boolean vector, then the inverse RP transform associated to a Z-matrix:*

$$\{t_n + 1,\ n = 1,...,m\} \to \{a_n,\ n = 1,...,m\} :$$
$$t_n + 1 = \prod_{k=1}^{m} (1 + a_k Z_{k,n}),\ n = 1,...,m$$

satisfies:

(i) $a_n \in \{0, 1, -\frac{1}{2}\},\ n = 1,...,m$

(ii) The map $t \to \{t_n + 1,\ n = 1,...,m\} \to \{a_n,\ n = 1,...,m\} \to$
$\to \{\mathrm{sgn}(a_n - \frac{1}{2}),\ n = 1,...,m\}$ *is a boolean map.*

Application Let t be any boolean vector of length m, then the inverse boolean RP transform sends $t + 1$ to a vector with entries $\{0, -\frac{1}{2}, 1\}$. We observe that the sign of the absolute value of this provides random permutation of the 2^m numbers. The Figure 2 is created by the inverse of composition of RP transform for $m = 9$ and provides a random permutation of the first 512 numbers.

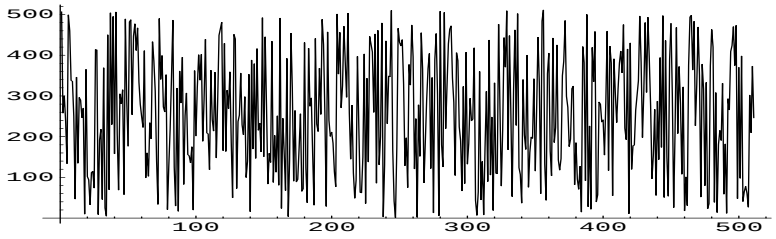

Fig. 2. The inverse of composition of RP transform for $m = 9$ which provides a random permutation of the first 512 numbers.

Appendix

In this section we sketch some of the proofs of our theorems.

Proof of Theorem 1 Since $h_{k,n}$ are binary, we may write:

$$t_n = \prod_{k=1}^{m} (1 + a_k h_{k,n}) = \prod_{k=1}^{m} (1 + a_k)^{h_{k,n}}$$

and so

$$\log(t_n) = \sum_{k=1}^{m} \log(1+a_k) h_{k,n}, \quad n = 1, \ldots, m.$$

Let $H^{-1} = \{h_{k,n}^{-1}\}$ be the inverse matrix of H, then it is easy to see that

$$\log(1+a_k) = \sum_{n=1}^{m} h_{n,k}^{-1} \log(t_n), \quad k = 1, \ldots, m,$$

and so this RP transform is invertible.

Proof of Theorem 4 It is not difficult to see that conditions (1) and (2) determine a unique matrix. To show that the determinant of this matrix is non-zero, we observe that any matrix Z determined by the permutations ρ and r can by reduced by row operations to the identity matrix.

Proof of Theorem 5 Since the inverse matrix $Z^{-1} = \{Z_{k,n}^{-1}\}$ satisfies $Z_{k,n}^{-1} \in \{0, 1, -1\}$, $k, n = 1, ...m$, (i) and (ii) are obtained from the proof of Theorem 1.

References

[1] N. Atreas, C. Karanikas, and P. Polychronidou, "A class of sparse unimodular matrices generating multiresolution and sampling analysis for data of any length," *SIAM J. Matrix Anal. Appl.*, vol. 30, no. 1, pp. 312–323, 2008.

[2] N. Atreas and P. Polychronidou, "A class of sparse invertible matrices and their use for non-linear prediction of nearly periodic time series with fixed period," *Numer. Funct. Anal. Optim.*, vol. 29, no. 1 & 2, pp. 66–87, 2008.

[3] N. Atreas and C. Karanikas, "Multiscale haar unitary matrices with the corresponding Riesz products and a characterization of Cantor - type languages," *Fourier Anal. Appl.*, vol. 13, no. 2, pp. 197–210, 2007.

[4] ——, "Haar-type orthonormal systems, data presentation as riesz products and a recognition on symbolic sequences," in *Proc. Frames and Operator Theory in Analysis and Signal Processing*, ser. Contemporary Mathematics (CONM), 2008, vol. 451, pp. 1–9.

[5] ——, "Discrete type riesz products," in *Proc. of the workshop on Walsh and Dyadic Analysis*, R. Stankovic, Ed. Nis, Serbia: Faculty of Electronic Enfineering, 2007, pp. 137–143.