Application of Sign Hadamard-Haar Transform in Ternary Communication System

Bogdan J. Falkowski   and   Shixing Yan

School of Electrical and Electronic Engineering
Nanyang Technological University
Block S1, 50 Nanyang Avenue, Singapore 639798

Abstract

A recently developed non-linear transform, called 'Sign Hadamard-Haar transform' is discussed. The transform is unique and converts ternary vectors into ternary spectral domain. New transform is extremely effective in terms of computational costs when compared with known Sign Walsh transform in application inside ternary communication system.

1. Introduction

In many applications of computer engineering and science, where logic functions need to be analyzed or synthesized, it is useful to transform such functions to the corresponding spectral domain that provides various new insights into solving some important problems. The most popular ternary transform is Reed-Muller transform over GF(3) [8]. It operates on ternary logic functions and provides 3^n ternary spectra for a given ternary function. Another family of invertible nonlinear transforms, which uniquely map ternary logic functions into ternary transform space, are sign transforms. The first transform under the name of 'sign transform' was based on Walsh functions [5, 7, 8] and is known as Sign Walsh transform [1].

In this paper, a recently developed new transform called Sign Hadamard-Haar transform [2] that is related to rationalized Hadamard-Haar transform [6] is applied in ternary communication system. The basic definitions for this transform have been given here. Besides applications in ternary logic design a new Hadamard-Haar transform can be used when there is a need for a unique coding of ternary vectors into the special domain of the same dimensions. In this article we are showing one such application in the form of ternary communication system and compare computational advantages of our new transform over known Sign Walsh transform. Another area in which our new transform could be used is development of cryptographic functions that need to be immune to input transformations.

The structure of this article is as follows. For comparison purpose, Section 2 covers basic definitions of Sign Walsh as well as Sign Hadamard-Haar transforms. Section 3 shows computational advantages of our new transform over Sign Walsh in ternary communication system while Section 4 concludes the paper.

2. Definitions of Sign Walsh and Sign Hadamard-Haar Transforms

Definition 1: An invertible sign Hadamard-Haar transform hh and its inverse transform hh^{-1} are the mappings hh: $\{+1,0,-1\}^N \rightarrow \{+1,0,-1\}^N_{(hh)}$ and hh^{-1}: $\{+1,0,-1\}^N_{(hh)} \rightarrow$, $\{+1,0,-1\}^N$, where $N = 2^n$. In order to obtain the sign Hadamard-Haar spectrum hh and its inverse, the results of each fast forward or inverse Hadamard-Haar butterfly block are quantized first. In the above equations, the cardinality of the original data set $\{+1,0,-1\}^N$ and its transformed spectrum is equal to 3^N.

The following symbols are used: Let $\vec{x}_n = \{x_n, x_{n-1}, \cdots, x_p, \cdots, x_2, x_1\}$, $\vec{\alpha}_n = \{\alpha_n, \alpha_{n-1}, \cdots, \alpha_p, \cdots, \alpha_2, \alpha_1\}$ and $\vec{\omega}_n = \{\omega_n, \omega_{n-1}, \cdots, \omega_p, \cdots, \omega_2, \omega_1\}$ be n-tuples over GF(2). The symbol x_p stands for a data variable, α_p represents a Sign Walsh transform variable, and ω_p a Sign Hadamard-Haar transform variable, p is an integer and $1 \leq p \leq n$. Let $\vec{F} = [F_0, F_1, ..., F_j, ..., F_{N-2}, F_{N-1}]$ be a ternary vector. For example, it can be the S-coded truth vector of $f:(0,1)^n \rightarrow (-1,0,1)$ where the value of F_j $(1 \leq j < N)$ is given by $F(\vec{x}_n)$ when $\sum_{p=1}^n x_p 2^{p-1} = j$. Let $\vec{W}_F = [w_0, w_1, ..., w_j, ... w_{N-2}, w_{N-1}]$ and $\overrightarrow{HH}_F = [hh_0, hh_1 ..., hh_j, ..., hh_{N-2}, hh_{N-1}]$ be the vector corresponding to Sign Walsh spectrum of $\vec{F}$ and Sign Hadamard-Haar spectrum of $\vec{F}$, accordingly. The value of w_j $(0 \leq j < N)$ is given by $\vec{W}_F(\alpha)$ when $\sum_{p=1}^n \alpha_p 2^{p-1} = j$. The value of hh_j $(0 \leq j < N)$ is given by $\overrightarrow{HH}_F(\omega)$ when $\sum_{p=1}^n \omega_p 2^{p-1} = j$. Let $\vec{O}_i$ represent the vector of i zeros, $1 \leq i \leq n$. Let the symbol $\oplus_c$ represent cyclic addition, the symbol $\oplus_d$ represent dyadic addition, and the symbol $\wedge$ represent bit-by-bit logical AND.

When the above operations are applied to two vectors $\vec{A}_l$ and $\vec{B}_k$, $1 \leq l < k$, l and k are two different integer numbers, they result in the vector $\vec{C}_k$ of the length k. Only l elements of $\vec{B}_k$ and all elements of $\vec{A}_l$ are manipulated on,

remaining (*k-1*) elements of the resulting vector $\vec{C}_k$ are not affected by the applied operation and are simply the same as the elements of the vector $\vec{B}_k$ between positions *k* and *l* + 1 .

Definition 2: An invertible forward Sign Walsh transform w is defined as [1]:

$$w(\vec{\alpha_n}) = \text{sign}\left\{\sum_{x_n=0}^{1}\text{sign}\left[\sum_{x_{n-1}=0}^{1}\text{sign}\left(\ldots\text{sign}\sum_{x_1=0}^{1}f(\vec{x_n})(-1)^{\sum_{p=1}^{n}\alpha_p x_p}\right)\right]\right\} \quad (1)$$

The inverse Sign Walsh transform is [1]:

$$f(\vec{x_n}) = \text{sign}\left\{\sum_{\alpha_1=0}^{1}\text{sign}\left[\sum_{\alpha_2=0}^{1}\text{sign}\left(\ldots\text{sign}\sum_{\alpha_n=0}^{1}w(\vec{\alpha_n})(-1)^{\sum_{p=1}^{n}\alpha_p x_p}\right)\right]\right\} \quad (2)$$

In eqns. 1-2, $1 \le p \le n$.

Definition 3: An invertible forward sign Hadamard-Haar transform hh is [2]:

$$hh\,(\vec{O}_n \oplus_d \omega_1 \oplus_d \omega_n 2^{n-1}) = \text{sign}\sum_{x_n=0}^{1}\big[\,(-1)^{x_n\omega_n}\,[\text{sign}$$

$$\sum_{x_{n-1}=0}^{1}[\text{sign}\sum_{x_{n-2}=0}^{1}[\cdots\text{sign}\sum_{x_1=0}^{1}\{(-1)^{x_{n-1}\omega_1}f(\vec{x_n})\}\cdots]]]] \quad (3)$$

and

$$hh(\vec{O}_n \oplus_d \omega_i \oplus_d 2^i \oplus_d \omega_n 2^{n-1}) = \text{sign}\sum_{x_n=0}^{1}[(-1)^{x_n\omega_n}[\text{sign}$$

$$\sum_{x_{n-i-1}=0}^{1}[\text{sign}\sum_{x_{n-i-2}=0}^{1}[\cdots\text{sign}\sum_{x_1=0}^{1}(-1)^{x_{n-2}}f\{(\vec{O}_{n-1}\oplus_d \vec{\omega_i})$$

$$\oplus_c (n-i-1)\}\oplus_d \vec{x}_{n-i-1}\}]] \quad (4)$$

where $1 \le i < n-1$.

The inverse sign Hadamard-Haar transform is [2]:

$$f(\vec{x_n}) = \text{sign}\{(-1)^{x_1}\{\text{sign}\{hh\{[(\vec{O}_1 \wedge \vec{x}_{n-1})\oplus_c 1]\oplus_d 2^{n-2}\}+$$

$$(-1)^{x_n}hh\{[(\vec{O}_1 \wedge \vec{x}_{n-1})\oplus_c 1]\oplus_d 2^{n-2}\oplus_d 2^{n-1}\}\}\}+$$

$$\text{sign}\{(-1)^{x_2}\{\text{sign}\{hh\{[(\vec{O}_2 \wedge \vec{x}_{n-1})\oplus_c 2]\oplus_d 2^{n-3}\}+$$

$$(-1)^{x_n}hh\{[(\vec{O}_2 \wedge \vec{x}_{n-1})\oplus_c 2]\oplus_d 2^{n-3}\oplus_d 2^{n-1}\}\}\}+\cdots+$$

$$\text{sign}\{(-1)^{x_i}\{\text{sign}\{hh\{[(\vec{O}_i \wedge \vec{x}_{n-1})\oplus_c i]\oplus_d 2^{n-i-1}\}+$$

$$(-1)^{x_n}hh\{[(\vec{O}_i \wedge \vec{x}_{n-1})\oplus_c i]\oplus_d 2^{n-i-1}\oplus_d 2^{n-1}\}\}\}+\cdots+$$

$$\text{sign}\{(-1)^{x_{n-2}}\{\text{sign}\{hh\{[(\vec{O}_{n-2} \wedge \vec{x}_{n-1})\oplus_c (n-2)]\oplus_d 2\}+$$

$$(-1)^{x_n}hh\{[(\vec{O}_{n-2} \wedge \vec{x}_{n-1})\oplus_c (n-2)]\oplus_d 2\oplus_d 2^{n-1}\}\}\}+$$

$$\text{sign}\{\sum_{\omega_1=0}^{1}(-1)^{x_{n-1}\omega_1}\{\text{sign}[h(\vec{O}_{n-1}\oplus_d \omega_1)+$$

$$(-1)^{x_n}h(\vec{O}_{n-1}\oplus_d \omega_1 \oplus_d 2^{n-1})]\}\}\cdots\}\}\} \quad (5)$$

where $1 \le i < n-1$.

In eqns. 1-5,

$$\text{sign}\,z = \begin{cases} -1 & z < 0 \\ 0 & z = 0 \\ +1 & z > 0 \end{cases} \quad (6)$$

3. Application of Sign Hadamard-Haar in Ternary Communication System

In the previous Section, it has been shown that Sign Hadamard-Haar transform similarly to well know Sign Walsh transform exhibit non-linear properties. Though non-linear, these transforms are unique and invertible. With intrinsic coding property, these transforms reveal possible application in secured communication systems [3]. In this Section, the application of Sign Hadamard–Haar as the sequence for ternary communication system will be considered. For comparison the well known Sign Walsh transform will also be used in the same application. In such a system, the incoming binary/ternary data is first encoded by performing Sign Hadamard-Haar transform on it. The digital modulation technique responsible for carrying information in Sign Hadamard-Haar spectra is Ternary Amplitude Frequency Shift Keying (TAFSK) [3, 4]. In this signaling, a ternary +1 is transmitted by a Radio Frequency (RF) pulse of carrier $\cos\omega_1 t$, a ternary -1 is transmitted by an RF pulse of carrier $\cos\omega_2 t$, and a 0 corresponds to no RF pulse. The technique combines Binary Amplitude Shift Keying and Binary Frequency Shift Keying for the ternary case. The Power Spectral Density (PSD) of the resultant signaling is given by

$$S(\omega) = \frac{1}{2}[A_1(\omega+\omega_1)+A_1(\omega-\omega_1)+A_1(\omega+\omega_2)+A_1(\omega-\omega_2)] \quad (7)$$

where

$$A_1(\omega) = \frac{2}{9}T_0\text{sinc}^2\left(\frac{\omega T_0}{2\pi}\right)\left[1+\frac{T_0}{\pi}\sum_{m=-\infty}^{\infty}\delta\left(\omega-\frac{2\pi m}{T_0}\right)\right]$$

Proof. Let Sign Hadamard-Haar transform of binary/ternary data streams be represented by

$$A(t) = \sum_{k=-\infty}^{\infty}a_k p(t-kT_0) = A_1(t)+A_2(t)$$

where $p(t)$ represents a full rectangular pulse which repeats every T_0 seconds, and it is assumed that a_k is equally likely to be +1, 0 or -1, i.e. $P(a_k=1)=P(a_k=-1)=P(a_k=0)$ $=\frac{1}{3}$. Furthermore

$$A_1(t) = \sum_{k=-\infty}^{\infty}a_k^{\langle 1\rangle}p(t-kT_0) \text{ and } A_2(t) = \sum_{k=-\infty}^{\infty}a_k^{\langle -1\rangle}p(t-kT_0)$$

with $P(a_k^{\langle 1\rangle}=1)=P(a_k^{\langle -1\rangle}=-1)=\frac{1}{3}$ and $P(a_k^{\langle 1\rangle}=0)=P(a_k^{\langle -1\rangle}=0)$ $=\frac{2}{3}$. The PSD of ON-OFF signaling [4] is

$$A_0(\omega) = \frac{|P(\omega)|^2}{T_0}\left[\sum_{m=-\infty}^{\infty}R_m e^{-jm\omega T_0}\right]$$

where R_m is the coefficient of the time-autocorrelation function of the signaling and $j=\sqrt{-1}$. Therefore the PSD of $A_1(t)$ is $A_1(\omega)=A_0(\omega)$, with

$$R_0 = \lim_{N_T \to \infty} \frac{1}{N_T} \sum_{k=1}^{N_T} \left(a_k^{\langle 1 \rangle} \right)^2 = \frac{1}{3}$$

and
$$R_m = \lim_{N_T \to \infty} \frac{1}{N_T} \sum_{k=1}^{N_T} a_k^{\langle 1 \rangle} a_{k=m}^{\langle 1 \rangle} = \frac{1}{9}, \text{ if } m \neq 0$$

Since
$$P(\omega) = T_0 \text{sinc}\left(\frac{\omega T_0}{2\pi} \right)$$

and using
$$\sum_{m=-\infty}^{\infty} e^{-jm\omega T_0} = \frac{T_0}{2\pi} \sum_{m=-\infty}^{\infty} \delta\left(\omega - \frac{2\pi m}{T_0} \right)$$

then
$$A_1(\omega) = \frac{2}{9} T_0 \text{sinc}^2\left(\frac{\omega T_0}{2\pi} \right) \left[1 + \frac{T_0}{\pi} \sum_{m=-\infty}^{\infty} \delta\left(\omega - \frac{2\pi m}{T_0} \right) \right]$$

Since $\left(a_k^{\langle 1 \rangle} \right)^2 = \left(a_k^{\langle -1 \rangle} \right)^2$ and $a_k^{\langle 1 \rangle} a_{k+m}^{\langle 1 \rangle} = a_k^{\langle -1 \rangle} a_{k+m}^{\langle -1 \rangle}$, therefore $A_2(\omega) = A_1(\omega)$. Using the frequency shifting property and since
$$s(t) = A_1(t) \cos \omega_1 t + A_2(t) \cos \omega_2 t$$
the proof of eqn. 7 is complete. □

For $\omega_2 > \omega_1$, if $\omega_2 - \omega_1 = 2\omega_0$ then the transmission bandwidth of TAFSK signaling is $4 f_0$ (where $f_0 = 1/T$ is the clock frequency).

A new recursive transform can also be developed based on Sign Hadamard-Haar transform. As an example, Sign Hadamard-Haar transform can be applied twice onto a ternary truth column vector $\vec{F}$ such that a new transform space is developed. The overall transform is named as Sign Hadamard-Haar-2 transform. In general, there are together 3^N different Sign Hadamard-Haar transform spaces, denoted as Sign Hadamard-Haar-q transforms with $1 \leq q \leq 3^N$, where when $q = 1$, the transform yields the original Sign Hadamard-Haar transform. For comparison purpose, Sign Walsh-q transform can be defined similarly.

Figure 1 shows the block diagram of a TASFK transmitter. The continuous streams of binary/ternary data are converted to parallel words of length N by means of a serial-parallel converter. Sign Hadamard-Haar-q transform is applied to each word before converting back to the format of serial data. The output signal V of the parallel-serial converter controls the output frequency of the voltage-controlled oscillator, and both outputs are fed together into the mixer. The output of the mixer is TAFSK signaling. The output of the oscillator is mathematically given by
$$VCO = V_0 \cos\left[2\pi \left(f_c + V f_m \right) t \right] \tag{8}$$
where $V \in \{-1, 0, 1\}$ and V_0 is an arbitrary amplitude. If $f_m = f_0$, then the resultant transmission bandwidth will be $4 f_0$, and $f_c + f_0 = f_2, f_c - f_0 = f_1$.

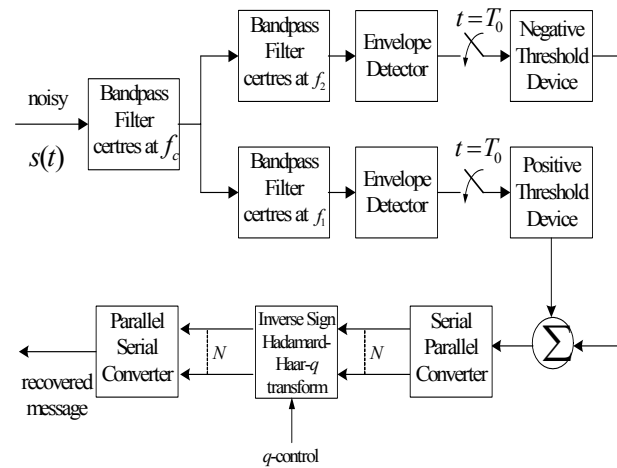Figure 2 shows a block diagram of a TAFSK receiver. The incoming noisy RF signal is bandpass filtered centered at frequency f_c. The bandpass filters centered at f_2 and f_1 are matched to the two RF pulses corresponding to ternary logic of -1 and +1, accordingly. The outputs of the two matched filters are detected by two envelope detectors. The envelope detector is sampled at $t = T_0$ to make the ternary

decision of -1 or 0 and 1 or 0 by negative and positive threshold devices, respectively. The output of summer is ternary, which is fed to a serial-parallel-serial converter, an inverse Sign Hadamard-Haar-q transform block and a parallel-serial converter to extract the original message.
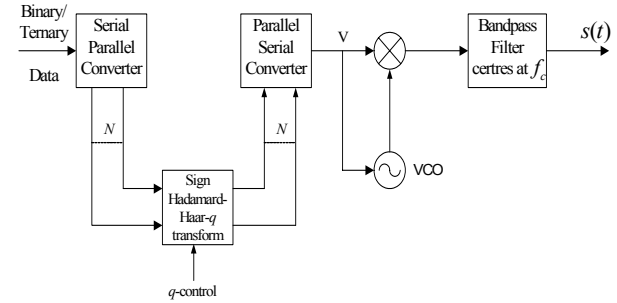
Figure 1 Block diagram of TAFSK transmitter.

The proposed non-coherent system is the simplest implementation of a ternary communication system. Other possibilities include the complicated M-ARY communication systems [3]. The addition of a Sign Hadamard-Haar transform provides security in the digital communication system. The level of security is easily adjustable by controlling q, which corresponds to Sign Hadamard-Haar-q transform applied q times. If q is varied for each word transformed in a manner transparent to a friendly receiver, the level of security in the communication system will be further enhanced. It is obvious that Sign Hadamard-Haar transform provides security to information data, however another possibility to increase the security of the digital communication system is the use of Sign Hadamard-γ-Haar-χ transform described in the conclusion. Though the latter transform is more computationally expensive, it can be also in the form of Sign Hadamard-γ-Haar-χ-q transform, it provides better security properties by its design and is suitable for cryptographic systems.

Figure 2 Block diagram of TAFSK receiver.

Table 1 Comparison of computational costs in ternary communication system

q	n	Sign Hadamard-Haar-q transform $(3 \times 2^{n+1} - 8) \times q$	Sign Walsh-q transform $2qn2^n$
3	1	12	12
	2	48	48
	3	120	144
5	4	440	640
	5	920	1,600
	6	1,880	3,840
8	7	6,080	14,336
	8	12,224	32,768
	9	24,512	73,728
10	10	61,360	204,800
	11	122,800	450,560
	12	245,680	983,040
12	13	589,728	2,555,904
	14	1,179,552	5,505,024
	15	2,359,200	11,796,480

The application of Sign Hadamard-Haar transform in a ternary communication system has been considered. Such application may be used by other quantized transforms as well. When the well known Sign Walsh transform is applied to the ternary communication system, Sign Hadamard-Haar-q transform will be replaced by Sign Walsh-q transform in the Figure 1 and Figure 2. Table 1 shows some results about computational costs of two systems where Sign Hadamard-Haar-q transform and Sign Walsh-q transform are implemented respectively. From Table 1, it is obvious that the system based on Sign Hadamard-Haar-q transform is much more efficient than the one based on Sign Walsh-q transform due to much smaller number of computations especially for higher q and n.

4. Conclusion

A non-linear transform called 'Sign Hadamard-Haar transform' has been applied in ternary communication system. It has been shown that the transform exhibits a non-linear property. Essentially, it transforms ternary data into ternary spectrum. Though non-linear, the transform is unique, and hence invertible. Recursive definition of the transform has been given.

Sign Hadamard-Haar transform is just another representative of a family of quantized transforms based on the usage of sign function as the quantizer and as shown in this article it has advantage over well known Sign Walsh transform in application inside of ternary communication system. In order to further enhance its cryptographic properties, one may develop a new recursive sign transform with just Sign Hadamard-γ-Haar-χ transform as the basis where γ and χ show the number of butterflies in Hadamard and Haar part of the transform. By simply applying Sign Hadamard-γ-Haar-χ transform twice onto a ternary truth column vector $\vec{F}$ such that a new transform space is developed, and name the overall transform as Sign Hadamard-γ-Haar-χ-2 transform. In general, if n is the number of variables of the ternary function, there are altogether 3^n different Sign Hadamard-γ-Haar-χ transform spaces, denoted as Sign Hadamard-γ-Haar-χ-q transforms with $1 \leq q \leq 3^n$ which is well suited to security coding in cryptographic systems and ternary security communication systems, where when $q = 1$, $\gamma = 1$ and $\chi = n - 1$, the transform yields the original Sign Hadamard-Haar transform of size n.

References

[1] Besslich, Ph.W., and Trachtenberg, E.A., 'Three-valued quasi-linear transformation for logic synthesis', IEE Proceedings - Computers and Digital Techniques, 143, (6), pp. 391-400, Nov. 1996.

[2] Falkowski, B.J., and Yan, S., 'Sign Hadamard-Haar transform', Proc. 16th European Conference on Circuit Theory and Design, Krakow, Poland, September 2003, accepted for publication.

[3] Fan, P., and Darnell, M., Sequence Design for Communications Applications, Taunton, Somerset, England: Research Studies Press Ltd. and New York: John Wiley & Sons Inc, 1996.

[4] Filippov, L.I., and Zinoviev, A.L., Methods of Analytic Expression of Radio Communication Signals, Moscow: Vysshaia Shkola, 1966, in Russian.

[5] Karpovsky, M.G., Finite Orthogonal Series in the Design of Digital Devices, New York: John Wiley, 1976.

[6] Rao, K.R., Jalali, A., and Yip, P., 'Rationalized Hadamard-Haar transform', Proc. 11th Annual Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, California, pp. 194-203, Nov. 1977.

[7] Stankovic, R.S. and Astola, J.T., Spectral Interpretation of Decision Diagrams, New York: Springer-Verlag, 2003.

[8] Stankovic, R.S., Stojic, M.R., and Stankovic, M.S., eds., Recent Development in Abstract Harmonic Analysis with Applications in Signal Processing, Belgrade: Science Publisher, 1996.