A MIXING OF PROUHET-THUE-MORSE SEQUENCES AND RADEMACHER FUNCTIONS

Hieu D. Nguyen
Department of Mathematics, Rowan University, Glassboro, New Jersey
nguyen@rowan.edu

Received: 3/8/14, Revised: 2/17/15, Accepted: 3/29/15, Published: 4/3/15

Abstract

We present a novel generalization of the Prouhet-Thue-Morse sequence to binary ± 1-weight sequences. Derived from Rademacher functions, these weight sequences are shown to satisfy interesting orthogonality and recurrence relations. In addition, we establish a result useful in radar by describing these weight sequences as sidelobes of Doppler tolerant waveforms.

1. Introduction

Let $u(n)$ denote the binary sum-of-digits residue function, i.e., the sum of the digits in the binary expansion of n modulo 2. For example, $u(7) = u(111_2) = 3 \bmod 2 = 1$. The sequence $u(n)$ is known as the Prouhet-Thue-Morse (PTM) integer sequence. It can easily be shown to satisfy the recurrence

$$\begin{aligned} u(0) &= 0 \\ u(2n) &= u(n) \\ u(2n+1) &= 1 - u(n). \end{aligned}$$

The first few terms of $u(n)$ are $0, 1, 1, 0, 1, 0, 0, 1$. Observe that the PTM sequence can also be generated by starting with the value 0 and recursively appending a negated copy of itself (bitwise):

$$0 \to 01 \to 0110 \to 01101001 \to \cdots$$

Another approach to defining the PTM sequence is to iterate the morphism μ defined on the alphabet $\{0, 1\}$ using the substitution rules $\mu(0) = 01$ and $\mu(1) = 10$

(see [1]). Beginning with $x_0 = 0$, we obtain

$$
\begin{aligned}
&x_1 = \mu(x_0) = 01\\
&x_2 = \mu^2(x_0) = \mu(x_1) = 0110\\
&x_3 = \mu^3(x_0) = \mu(x_2) = 01101001\\
&\dots
\end{aligned}
$$

This *ubiquitous* sequence, coined as such by Allouche and Shallit [1], first arose in the works of three mathematicians: Prouhet [22] involving equal sums of like powers in 1851, Thue [28] on combinatorics of words in 1906, and Morse [18] in differential geometry in 1921. It has found interesting applications in many areas of mathematics, physics, and engineering: combinatorial game theory (see, e.g., [20] on fair division and [9] on infinite play in chess, and [1], p. 3), fractals (see, e.g., [3, 15]), quasicrystals (see, e.g., [17, 25]) and more recently Dopper tolerant waveforms in radar (see, e.g., [6, 19, 21]).

Suppose we now replace the 0's and 1's in the PTM sequence with 1's and -1's, respectively. This yields the ± 1-sequence $w(n)$, a sequence that clearly satisfies the recurrence

$$
\begin{aligned}
w(0) &= 1\\
w(2n) &= w(n)\\
w(2n+1) &= -w(n).
\end{aligned}
$$

Here, $w(n)$ and $u(n)$ are related by

$$w(n) = 1 - 2u(n). \tag{1}$$

It is easy to verify that (1) is equivalent to

$$w(n) = (-1)^{u(n)}. \tag{2}$$

Of course, $u(n)$ can be generalized to any modulus $p \geq 2$. Towards this end, we define $u_p(n)$ to be the sum of the digits in the base-p expansion of n modulo p. We shall call $u_p(n)$ the mod-p PTM integer sequence. Then $u_p(n)$ satisfies the recurrence

$$
\begin{aligned}
u_p(0) &= 0\\
u_p(pn+r) &= (u(n)+r)_p,
\end{aligned}
$$

where $(m)_p \equiv m \bmod p$ and $(m)_p \in [0, p-1]$. More interestingly, it is well known that $u_p(n)$ provides a solution to the famous Prouhet-Tarry-Escott (PTS) problem ([14, 22, 30]): given a positive integer M, find p mutually disjoint sets of non-negative integers $S_0, S_1, \dots, S_{p-1}$ so that

$$\sum_{n\in S_0} n^m = \sum_{n\in S_1} n^m = \cdots = \sum_{n\in S_{p-1}} n^m$$

for $m = 1, \ldots, M$. The solution, first given by Prouhet [22] and later proven by Lehmer [14] (see also Wright [30]), is to partition the integers $\{0, 1, \ldots, p^{M+1} - 1\}$ so that $n \in S_{u_p(n)}$. For example, if $M = 3$ and $p = 2$, then the two sets $S_0 = \{0, 3, 5, 6, 9, 10, 12, 15\}$ and $S_1 = \{1, 2, 4, 7, 8, 11, 13, 14\}$ given by Prouhet's result solve the PTS problem, namely,

$$\begin{aligned} 60 &= 0 + 3 + 5 + 6 + 9 + 10 + 12 + 15 \\ &= 1 + 2 + 4 + 7 + 8 + 11 + 13 + 14 \\ 620 &= 0^2 + 3^2 + 5^2 + 6^2 + 9^2 + 10^2 + 12^2 + 15^2 \\ &= 1^2 + 2^2 + 4^2 + 7^2 + 8^2 + 11^2 + 13^2 + 14^2 \\ 7200 &= 0^3 + 3^3 + 5^3 + 6^3 + 9^3 + 10^3 + 12^3 + 15^3 \\ &= 1^3 + 2^3 + 4^3 + 7^3 + 8^3 + 11^3 + 13^3 + 14^3. \end{aligned}$$

In this paper, we address the following question: what is the natural generalization of $w(n)$ to modulus $p \geq 2$? Which formula should we look to extend, (1) or (2)? Is there any intuition behind our generalization? One answer is to define $w_p(n)$ by merely replacing $u(n)$ with $u_p(n)$ in say (2). However, to discover a more satisfying answer, we consider a modified form of (2):

$$w(n) = (-1)^{d_{1-u(n)}}. \tag{3}$$

Here, $d_{1-u(n)}$ takes on one of two possible values, $d_0 = 1$ or $d_1 = 0$, which we view as the first two digits in the binary expansion (base 2) of the number 1, i.e., $1 = d_1 2^1 + d_0 2^0$. Thus, formula (3) involves the digit opposite in position to $u(n)$.

To explain how this formula naturally generalizes to any positive modulus $p \geq 2$, we begin our story with two arbitrary elements a_0 and a_1. Define $A = (a_n) = (a_0, a_1, \ldots)$ to be what we call a mod-2 PTM sequence generated from a_0 and a_1, where the elements of A satisfy the aperiodic condition

$$a_n = a_{u(n)}.$$

Thus, $A = (a_0, a_1, a_1, a_0, a_1, a_0, a_0, a_1, \ldots)$. Since formula (3) holds, it follows that a_n can be decomposed as

$$a_n = \frac{1}{2}(a_0 + a_1) + \frac{1}{2}w(n)(a_0 - a_1). \tag{4}$$

In some sense, $w(n)$ plays the same role as $u(n)$ in defining the sequence A, but through the decomposition (4). We argue that formula (4) leads to a natural generalization of $w(n)$. For example, suppose $p = 3$ and consider the mod-3 PTM sequence $A = (a_0, a_1, a_2, \ldots)$ generated by three elements a_0, a_1, a_2 so that $a_n = a_{u_3(n)}$. The following decomposition generalizes (4):

$$a_n = \frac{1}{4}w_0(n)(a_0 + a_1 + a_2) + \frac{1}{4}w_1(n)(a_0 + a_1 - a_2) + \frac{1}{4}w_2(n)(a_0 - a_1 + a_2) + \frac{1}{4}w_3(n)(a_0 - a_1 - a_2).$$

Here, $w_0(n), w_1(n), w_2(n), w_3(n)$ are ± 1-sequences that we shall call the weights of a_n. Since $a_n = a_{u_3(n)}$, these weights are fully specified once their values are known for $n = 0, 1, 2$. It is straightforward to verify in this case that $W(n) = (w_0(n), \ldots, w_3(n))$ takes on the values

$$W(0) = (1, 1, 1, 1)$$
$$W(1) = (1, 1, -1, -1)$$
$$W(2) = (1, -1, 1, -1).$$

Thus, the weights $w_i(n)$ are a natural generalization of $w(n)$.

More generally, if $p \geq 2$ is a positive integer and $A = (a_n)$ is a mod-p PTM sequence generated from $a_0, a_1, \ldots, a_{p-1}$, i.e., $a_n = a_{u_p(n)}$, then the following decomposition holds:

$$a_n = \frac{1}{2^{p-1}} \sum_{i=0}^{2^{p-1}-1} w_i^{(p)}(n) B_i. \tag{5}$$

Here, the weights $w_i^{(p)}$ are given by

$$w_i(n) := w_i^{(p)}(n) = (-1)^{d^{(i)}_{p-1-u_p(n)}}, \tag{6}$$

where $0 \leq i \leq 2^{p-1} - 1$ and $i = d^{(i)}_{p-2} 2^{p-2} + \cdots + d^{(i)}_1 2^1 + d^{(i)}_0 2^0$ denotes its binary expansion. Moreover, B_i is calculated by the formula

$$B_i = \sum_{n=0}^{p-1} w_i(n) a_n. \tag{7}$$

Observe that we can extend the range for i to $2^p - 1$ (and will do so), effectively doubling the number of weights w_i. In that case we find that

$$w_i(n) = -w_{2^p-1-i}(n).$$

With this extension, we demonstrate in Theorem 16 that each $w_i(n)$ satisfies the recurrence

$$w_i(pn + r) = w_{x_r(i)}(n) w_i(n),$$

where $x_r(i)$ denotes a quantity that we define in Section 4 as the *xor-shift* of i by r, where $0 \leq x_r(i) \leq 2^p - 1$. For example, if $p = 2$, we find that

$$w_1(2n) = w_0(n) w_1(n)$$
$$w_1(2n + 1) = w_3(n) w_1(n).$$

Since $w_0(n) = 1$ and $w_3(n) = -1$ for all n, this yields the same recurrence satisfied by $w(n) = w_1(n)$ as described in the beginning of this section.

Next, we note that the set of values $R(n) = (w_0(n), \ldots, w_{2^p-1}(n))$ represent those given by the Rademacher functions $\phi_n(x)$, $n = 0, 1, 2, \ldots$, defined by (see [11, 23])

$$\phi_0(x) = 1 \quad (0 \le x < 1/2), \qquad \phi_0(x+1, = \phi_0(x);$$
$$\phi_0(x) = -1 \quad (1/2 \le x < 1), \qquad \phi_n(x) = \phi_0(2^n x).$$

In particular,

$$w_i(n) = \phi_n(i/2^p)$$

so that the right-hand side of (5) can be thought of as a discrete *Rademacher* transform of $(B_0, B_1, \ldots, B_{2^{p-1}-1})$. Moreover, formula (7) can be viewed as the inverse transform, which follows from the fact that the Rademacher functions form an orthogonal set. Thus, weight sequences can be viewed as a mixing of Prouhet-Thue-Morse sequences and Rademacher functions.

It is known that the Rademacher functions generate the Walsh functions, which have important applications in communications and coding theory (see [4, 27]). Walsh functions are those of the form (see, e.g., [11, 29])

$$\psi_m(x) = \phi_{n_k}(x)\phi_{n_{k-1}}(x) \cdots \phi_{n_1}(x),$$

where $m = 2^{n_k} + 2^{n_{k-1}} + \cdots + 2^{n_1}$ with $n_i < n_{i+1}$ for all $i = 1, \ldots, k-1$. This allows us to generalize our weights $w_i(n)$ to sequences

$$\tilde{w}_i(m) = w_i(n_k) \cdots w_i(n_1),$$

which we view as a discrete version of the Walsh functions in the variable i. In that case, we prove in Section 3 that if $0 \le m \le 2^p - 1$ for some fixed non-negative integer p, then

$$\sum_{i=0}^{2^p-1} \tilde{w}_i(m) B_i = \begin{cases} a_n, & \text{if } m = 2^n, 0 \le n \le p-1; \\ 0, & \text{otherwise.} \end{cases}$$

We also prove in the same section a result that was used in [19] to characterize these weight sequences as sidelobes of Doppler tolerant radar waveforms (motivated by [6] and [21]).

Lastly, we note that that the literature contains many generalizations of the PTM sequence (see, e.g., [2, 13, 26] and more recently, [5, 8, 16]). However, a search of the literature did not reveal any work similar to this article.

2. The Prouhet-Thue-Morse Sequence

Let $S(L)$ denote the set consisting of the first L non-negative integers $0, 1, \ldots, L-1$.

Definition 1. Let $n = n_1 n_2 \cdots n_k$ be the base-p representation of a non-negative integer n. We define the *mod-p sum-of-digits function* $u_p(n) \in \mathbb{Z}_p$ to be the sum of the digits n_i modulo p, i.e.,

$$u_p(n) \equiv \sum_{i=1}^{k} n_i \mod p.$$

Observe that $u_p(n) = n$ if $0 \leq n < p$.

Definition 2. We define a sequence $A = (a_0, a_1, \ldots)$ to be a *mod-p Prouhet-Thue-Morse (PTM)* sequence if it satisfies the aperiodic condition

$$a_n = a_{u_p(n)}.$$

Definition 3. Let p and M be positive integers and set $L = p^{M+1}$. We define $\{S_0, S_1, \ldots, S_{p-1}\}$ to be a *Prouhet-Thue-Morse* (PTM) *p-block partition* of $S(L) = \{0, 1, \ldots, L-1\}$ as follows: if $u_p(n) = i$, then

$$n \in S_i.$$

The next theorem solves the famous Prouhet-Tarry-Escott problem.

Theorem 4 ([22], [14], [30]). *Let p and M be positive integers and set $L = p^{M+1}$. Suppose $\{S_0, S_1, \ldots, S_{p-1}\}$ is a PTM p-block partition of $S(L) = \{0, 1, \ldots, L-1\}$. Then*

$$P_m := \sum_{n \in S_0} n^m = \sum_{n \in S_1} n^m = \cdots = \sum_{n \in S_{p-1}} n^m$$

for $m = 1, \ldots, M$. We shall refer to P_m as the m-th Prouhet sum corresponding to p and M.

Corollary 1. *Let $A = (a_0, a_1, \ldots, a_{L-1})$ be a mod-p PTM sequence of length $L = p^{M+1}$, where M is a non-negative integer. Then*

$$\sum_{n=0}^{L-1} n^m a_n = P_m(a_0 + a_1 + \cdots + a_{p-1}) \tag{8}$$

for $m = 0, \ldots, M$.

Proof. We have

$$
\begin{aligned}
\sum_{n=0}^{L-1} n^m a_n &= \sum_{n\in S_0} n^m a_{u_p(n)} + \sum_{n\in S_1} n^m a_{u_p(n)} + \cdots + \sum_{n\in S_{p-1}} n^m a_{u_p(n)} \\
&= a_0 \sum_{n\in S_0} n^m + a_1 \sum_{n\in S_1} n^m + \cdots + a_{p-1} \sum_{n\in S_{p-1}} n^m \\
&= P_m(a_0 + a_1 + \cdots + a_{p-1}).
\end{aligned}
$$

□

3. Weight Sequences

In this section we develop a generalization of the PTM ±1-sequence $w(n)$ and derive orthogonality and recurrence relations for these generalized sequences that we refer to as *weight* sequences.

Definition 5. Let $i = d_{p-1}^{(i)} 2^{p-1} + d_{p-2}^{(i)} 2^{p-2} + \cdots + d_1^{(i)} 2^1 + d_0^{(i)} 2^0$ be the binary expansion of i, where i is a non-negative integer with $0 \le i \le 2^p - 1$. Define $w_0^{(p)}(n), w_1^{(p)}(n), \ldots w_{2^p-1}^{(p)}(n)$ be binary ±1-sequences defined by

$$w_i^{(p)}(n) := w_i(n) = (-1)^{d_{p-1-u_p(n)}^{(i)}}.$$

Example 6. Let $p = 3$. Then

$$
\begin{aligned}
w_0(n) &= (\mathbf{1}, \mathbf{1}, \mathbf{1}, 1, 1, 1, 1, 1, 1, \ldots) \\
w_1(n) &= (\mathbf{1}, \mathbf{1}, -\mathbf{1}, 1, -1, 1, -1, 1, 1, \ldots) \\
w_2(n) &= (\mathbf{1}, -\mathbf{1}, \mathbf{1}, -1, 1, 1, 1, 1, -1, \ldots) \\
w_3(n) &= (\mathbf{1}, -\mathbf{1}, -\mathbf{1}, -1, -1, 1, -1, 1, -1, \ldots) \\
w_4(n) &= (-\mathbf{1}, \mathbf{1}, \mathbf{1}, 1, 1, -1, 1, -1, 1, \ldots) \\
w_5(n) &= (-\mathbf{1}, \mathbf{1}, -\mathbf{1}, 1, -1, -1, -1, -1, 1, \ldots) \\
w_6(n) &= (-\mathbf{1}, -\mathbf{1}, \mathbf{1}, -1, 1, -1, 1, -1, -1, \ldots) \\
w_7(n) &= (-\mathbf{1}, -\mathbf{1}, -\mathbf{1}, -1, -1, -1, -1, -1, -1, \ldots).
\end{aligned}
$$

Observe that the first three values of each weight $w_i(n)$ (displayed in bold) represent the binary value of i if we replace 1 and -1 with 0 and 1, respectively. Morever, we have the following symmetry:

Lemma 1. *For $i = 0, 1, \ldots, 2^p - 1$, we have*

$$w_i(n) = -w_{2^p-1-i}(n).$$

Proof. If $i = d_{p-1}^{(i)} 2^{p-1} + d_{p-2}^{(i)} 2^{p-2} + \cdots + d_0^{(i)} 2^0$, then $j = 2^p - 1 - i$ has expansion

$$j = \bar{d}_{p-1}^{(j)} 2^{p-1} + \bar{d}_{p-2}^{(j)} 2^{p-2} + \cdots + \bar{d}_0^{(j)} 2^0,$$

where $\bar{d}_k^{(j)} = 1 - d_k^{(i)}$. It follows that

$$w_i(n) = (-1)^{d_{p-1-u_p(n)}^{(i)}} = (-1)^{1-d_{p-1-u_p(n)}^{(j)}} = -w_{2^p-1-i}(n).$$

□

Theorem 7. *Let $p \geq 2$ be a positive integer. Then the vectors $W_p(0), W_p(1), .., W_p(p-1)$ defined by*

$$W_p(n) = (w_0^{(p)}(n), w_1^{(p)}(n), \ldots, w_{2^{p-1}-1}^{(p)}(n))$$

form an orthogonal set, i.e., for $0 \leq n, m \leq p-1$, we have

$$W_p(n) \cdot W_p(m) = \sum_{i=0}^{2^{p-1}-1} w_i(n) w_i(m) = 2^{p-1} \delta_{n-m} = \begin{cases} 2^{p-1}, & n = m; \\ 0, & n \neq m. \end{cases}$$

Here, δ_n is the Kronecker delta function.

Proof. It is straightforward to check that the lemma is true for $p = 2$. Thus, we assume $p \geq 3$ and define $k(n) = p - 1 - n$ so that

$$W_p(n) \cdot W_p(m) = \sum_{i=0}^{2^{p-1}-1} (-1)^{d_{k(n)}^{(i)} + d_{k(m)}^{(i)}}.$$

Assume $n \neq m$ and without loss of generality, take $n < m$ so that $k(n) > k(m)$. Assume $0 \leq i \leq 2^{p-1} - 1$ and expand i in binary so that

$$i = d_{p-1}^{(i)} 2^{p-1} + \cdots + d_{k(n)}^{(i)} 2^{k(n)} + \cdots + d_{k(m)}^{(i)} 2^{k(m)} + \cdots + d_0^{(i)} 2^0,$$

where $d_{p-1}^{(i)} = 0$. Suppose in specifying i we fix the choice of values for all binary digits except for $d_{k(n)}^{(i)}$ and $d_{k(m)}^{(i)}$. Then the set $S = \{(0,0), (0,1), (1,0), (1,1)\}$ consists of the four possibilities for choosing these two remaining digits, which we express as the ordered pair $d = (d_{k(n)}^{(i)}, d_{k(m)}^{(i)})$. But then the contribution from this set of four such values for i sums to zero in the dot product $W_p(n) \cdot W_p(m)$, namely

$$\sum_{d \in S} (-1)^{d_{k(n)}^{(i)} + d_{k(m)}^{(i)}} = 0.$$

Since this holds for all cases in specifying i, it follows that $W_p(n) \cdot W_p(m) = 0$ as desired. On the other hand, if $n = m$, then $k(n) = k(m)$ and so $d_{k(n)}^{(i)} = d_{k(m)}^{(i)}$ for all i. It follows that

$$W_p(n) \cdot W_p(m) = \sum_{i=0}^{2^{p-1}-1} (-1)^{2 d_{k(n)}^{(i)}} = \sum_{i=0}^{2^{p-1}-1} 1 = 2^{p-1}.$$

□

In fact, we have the more general result, which states a discrete version of the fact that the Walsh functions form an orthogonal set.

Theorem 8. *Let m be an integer and expand $m = 2^{n_k} + 2^{n_{k-1}} + \cdots + 2^{n_1}$ in binary with $n_i < n_{i+1}$ and $0 \le m \le 2^p - 1$. Define*

$$\tilde{w}_i(m) = w_i(n_k) \cdots w_i(n_1)$$

for $i = 0, 1, \ldots, 2^p - 1$. Then

$$\sum_{i=0}^{2^{p-1}-1} \tilde{w}_i(m) = 0 \tag{9}$$

for all $m = 0, 1, \ldots, 2^p - 1$.

Proof. Let $m = 2^{n_k} + 2^{n_{k-1}} + \cdots + 2^{n_1}$. We argue by induction on k, i.e., the number of distinct powers of 2 in the binary expansion of m. Suppose $k = 1$ and define $q = p - 1 - u_p(n_1)$. Then given any value of i where the binary digit $d_q^{(i)} = 0$, there exists a corresponding value j whose binary digit $d_q^{(j)} = 1$. It follows that

$$\begin{aligned}
\sum_{i=0}^{2^{p-1}-1} \tilde{w}_i(m) &= \sum_{\substack{i=0 \\ d_q^{(i)}=0}}^{2^{p-1}-1} (-1)^{d_q^{(i)}} + \sum_{\substack{i=0 \\ d_q^{(i)}=1}}^{2^{p-1}-1} (-1)^{d_q^{(i)}} \\
&= 2^{p-2} - 2^{p-2} = 0.
\end{aligned}$$

Next, assume that (9) holds for all m consisting of $k-1$ distinct powers of 2. Define $q_k = p - 1 - u_p(n_k)$. Then for m consisting of k distinct powers of 2, we have

$$\begin{aligned}
\sum_{i=0}^{2^{p-1}-1} \tilde{w}_i(m) &= \sum_{i=0}^{2^{p-1}-1} (-1)^{d_{q_k}^{(i)} + d_{q_{k-1}}^{(i)} + \cdots + d_{q_1}^{(i)}} \\
&= (-1)^0 \sum_{\substack{i=0 \\ d_{q_k}^{(i)}=0}}^{2^{p-1}-1} (-1)^{d_{q_{k-1}}^{(i)} + \cdots + d_{q_1}^{(i)}} + (-1)^1 \sum_{\substack{i=0 \\ d_{q_k}^{(i)}=1}}^{2^{p-1}-1} (-1)^{d_{q_k}^{(i)} + d_{q_{k-1}}^{(i)} + \cdots + d_{q_1}^{(i)}} \\
&= \frac{1}{2} \sum_{i=0}^{2^{p-1}-1} (-1)^{d_{q_{k-1}}^{(i)} + \cdots + d_{q_1}^{(i)}} - \frac{1}{2} \sum_{i=0}^{2^{p-1}-1} (-1)^{d_{q_k}^{(i)} + d_{q_{k-1}}^{(i)} + \cdots + d_{q_1}^{(i)}} \\
&= \frac{1}{2} \cdot 0 - \frac{1}{2} \cdot 0 = 0.
\end{aligned}$$

□

In [24], Richman observed that the classical PTM sequence $u(i)$ (although he did not recognize it by name in his paper) can be constructed from the product of all

Radamacher functions up to order $p-1$, where $0 \le i \le 2^p - 1$. This result easily follows from our formulation of weight sequences since

$$\begin{aligned}\tilde{w}_i^{(p)}(2^p-1) &= w_i^{(p)}(0)w_i^{(p)}(1)\cdots w_i^{(p)}(p-1)\\ &= (-1)^{d_{p-1}^{(i)}+d_{p-2}^{(i)}+\cdots+d_0^{(i)}}\\ &= (-1)^{u(i)}\\ &= w(i).\end{aligned}$$

Moreover, in the same paper Richman defines a set of difference (DIF) functions given by

$$\mathrm{DIF}(n,j) = (-1)^{s(j)},$$

where $0 \le j < 2^n$, $j = \sum_{i=0}^{n} j_i 2^i$ is the binary expansion of j and $s(j) = \sum_{i=0}^{n-1} j_i$ is the sum-of-digits function. Since $(-1)^{s(j)} = (-1)^{u(j)}$, this shows that $\mathrm{DIF}(n,j) = w(j)$.

Next, we relate weight sequences with PTM sequences. Since $w_i(n) = -w_{p-1-i}(n)$ from Lemma 1, the following lemma is immediate.

Lemma 2. *Let $A = (a_0, a_1, \ldots)$ be a mod-p PTM sequence. Define*

$$B_i = \sum_{n=0}^{p-1} w_i(n) a_n$$

for $i = 0, 1, \ldots, 2^p - 1$. Then

$$B_i(n) = -B_{2^p-1-i}(n).$$

Theorem 9. *The following equation holds for all $n \in \mathbb{N}$:*

$$a_n = \frac{1}{2^{p-1}} \sum_{i=0}^{2^{p-1}-1} w_i(n) B_i. \tag{10}$$

Proof. Since $a_n = a_{u_p(n)}$ for a PTM sequence and $w_i(n) = w_i(u_p(n))$, it suffices to prove (10) for $n = 0, 1, \ldots, p-1$. It follows from Theorem 7 that

$$\begin{aligned}\frac{1}{2^{p-1}} \sum_{i=0}^{2^{p-1}-1} w_i(n) B_i &= \frac{1}{2^{p-1}} \sum_{i=0}^{2^{p-1}-1} w_i(n) \left(\sum_{m=0}^{p-1} w_i(m) a_m \right)\\ &= \frac{1}{2^{p-1}} \sum_{m=0}^{p-1} \left(\sum_{i=0}^{2^{p-1}-1} w_i(n) w_i(m) \right) a_m\\ &= \frac{1}{2^{p-1}} \sum_{m=0}^{p-1} 2^{p-1} \delta_{n-m} a_m\\ &= a_n.\end{aligned}$$

$\square$

Remark. Because of the lemma above, we will refer to $w_0(n), w_1(n), \ldots, w_{2^{p-1}-1}(n)$ as the PTM weights of a_n with respect to the basis of sums $(B_0, B_1, \ldots, B_{2^{p-1}-1})$.

Example 10.
1. $p = 2$:

$$B_0 = a_0 + a_1$$
$$B_1 = a_0 - a_1.$$

2. $p = 3$:

$$B_0 = a_0 + a_1 + a_2, \qquad B_2 = a_0 - a_1 + a_2,$$
$$B_1 = a_0 + a_1 - a_2, \qquad B_3 = a_0 - a_1 - a_2.$$

Theorem 11. *For $0 \le m \le 2^p - 1$, we have*

$$\sum_{i=0}^{2^p-1} \tilde{w}_i(m) B_i = \begin{cases} a_n, & \text{if } m = 2^n, 0 \le n \le p-1; \\ 0, & \text{otherwise.} \end{cases} \tag{11}$$

Proof. If $m = 2^n$, then $\tilde{w}_i(n) = w_i(n)$ and thus formula (11) reduces to (10). Therefore, assume $m = 2^{n_k} + \cdots + 2^{n_1}$ where $k > 1$. Define $S_m = \{0, 1, \ldots, p-1\} - \{n_1, n_2, \ldots, n_k\}$. Then

$$\begin{aligned} \sum_{i=0}^{2^{p-1}-1} \tilde{w}_i(m) B_i &= \sum_{i=0}^{2^{p-1}-1} w_i(n_k) \cdots w_i(n_1) \left(\sum_{j=0}^{p-1} w_i(j) a_j \right) \\ &= \sum_{j=0}^{p-1} \left(\sum_{i=0}^{2^{p-1}-1} w_i(n_k) \cdots w_i(n_1) w_i(j) \right) a_j. \end{aligned}$$

Next, isolate the terms in the outer summation above corresponding to S_m:

$$\begin{aligned} \sum_{i=0}^{2^{p-1}-1} \tilde{w}_i(m) B_i = a_{n_1} & \sum_{i=0}^{2^{p-1}-1} w_i(n_k) \cdots w_i(n_2) w_i(n_1)^2 + \cdots \\ & + a_{n_k} \sum_{i=0}^{2^{p-1}-1} w_i(n_k)^2 w_i(n_{k-1}) \cdots w_i(n_1) \\ & + \sum_{j \in S_m} \left(\sum_{i=0}^{2^{p-1}-1} w_i(n_k) \cdots w_i(n_1) w_i(j) \right) a_k \\ &= a_{n_1} \sum_{i=0}^{2^{p-1}-1} \tilde{w}_i(m_1^-) + \cdots + a_{n_k} \sum_{i=0}^{2^{p-1}-1} \tilde{w}_i(m_k^-) \\ & + \sum_{j \in S_m} \left(\sum_{i=0}^{2^{p-1}-1} \tilde{w}_i(m_j^+) \right) a_k, \end{aligned}$$

where $m_j^- = m - 2^j$ and $m_j^+ = m + 2^j$. Now observe that all three summations above with index i must vanish because of Theorem 8. Hence,

$$\sum_{i=0}^{2^{p-1}-1} \tilde{w}_i(m)B_i = 0$$

as desired. □

We end this section by presenting a result that is useful in characterizing sidelobes of Doppler tolerant waveforms in radar ([21],[6],[19]).

Theorem 12. *Let $A = (a_0, a_1, \ldots, a_{L-1})$ be a mod-p PTM sequence of length $L = p^{M+1}$, where M is a non-negative integer. Write*

$$a_n = \frac{1}{2^{p-1}} w_0(n)B_0 + \frac{1}{2^{p-1}} S_p(n), \tag{12}$$

where

$$S_p(n) = \sum_{i=1}^{2^{p-1}-1} w_i(n)B_i.$$

Then

$$\sum_{n=0}^{L-1} n^m S_p(n) = N_m(L)B_0 \tag{13}$$

for $m = 1, \ldots, M$, where

$$N_m(L) = 2^{p-1}P_m - \sum_{n=0}^{L-1} n^m.$$

Proof. We apply (8):

$$\begin{aligned}
\sum_{n=0}^{L-1} n^m S_p(n) &= 2^{p-1} \sum_{n=0}^{L-1} n^m a_n - B_0 \sum_{n=0}^{L-1} n^m w_0(n) \\
&= 2^{p-1}P_m(a_0 + a_1 + \cdots + a_{p-1}) - B_0 \sum_{n=0}^{L-1} n^m \\
&= (2^{p-1}P_m - \sum_{n=0}^{L-1} n^m)B_0 \\
&= N_m(L)B_0.
\end{aligned}$$

□

4. XOR-Shift Recurrence

In this section we develop a recurrence formula for our weight sequences. Towards this end, we introduce the notion of an *xor-shift* of a binary integer.

Definition 13. Let $a, b \in \mathbb{Z}/2\mathbb{Z}$, where $\mathbb{Z}/2\mathbb{Z}$ denotes the integers modulo 2. We define $a \oplus b$ to be the exclusive OR (XOR) operation given by the following Boolean truth table:

$$\begin{aligned} 0 \oplus 0 &= 0 \\ 0 \oplus 1 &= 1 \\ 1 \oplus 0 &= 1 \\ 1 \oplus 1 &= 0. \end{aligned}$$

More generally, let $x = a_k \cdots a_0$ and $y = b_k \cdots b_0$ be two non-negative integers expressed in binary. We define $z = x \oplus y = c_k..c_0$ to be the *xor bit-sum* of x and y, where

$$c_k = a_k \oplus b_k.$$

In what follows we shall write $a \equiv b$ to mean $a \equiv b \bmod 2$. Observe then that if $a, b \in \mathbb{Z}/2\mathbb{Z}$, then $a \pm b \equiv a \oplus b$.

Definition 14. Let p be a positive integer and i a non-negative integer with $0 \leq i \leq 2^p - 1$. Expand i in binary so that

$$i = d_{p-1}2^{p-1} + \cdots + d_0 2^0.$$

We define the *degree-p xor-shift* of i by $r \geq 0$ to be the value (in decimal) given by the xor bit-sum

$$x_r(i) := x_r^{(p)}(i) = d_{p-1} \cdots d_r d_{r-1} \cdots d_0 \oplus d_{p-1-r} \cdots d_0 d_{p-1} \cdots d_{p-r},$$

i.e.,

$$x_r(i) = e_{p-1}2^{p-1} + \cdots + e_0 2^0,$$

where for $k = 0, 1, \ldots, p-1$, we have

$$e_k = \begin{cases} d_k \oplus d_{k-r}, & k \geq r; \\ d_k \oplus d_{d+(p-r)}, & k < r. \end{cases}$$

Example 15. Here are some values of $x_i^{(p)}(n)$ for $p = 3$:

$$\begin{aligned} x_1^{(3)}(0) &= 000_2 \oplus 000_2 = 000_2 = 0, & x_2^{(3)}(0) &= 000_2 \oplus 000_2 = 000_2 = 0, \\ x_1^{(3)}(1) &= 001_2 \oplus 010_2 = 011_2 = 3, & x_2^{(3)}(1) &= 001_2 \oplus 100_2 = 101_2 = 5, \\ x_1^{(3)}(2) &= 010_2 \oplus 100_2 = 110_2 = 6, & x_2^{(3)}(2) &= 010_2 \oplus 001_2 = 011_2 = 3, \\ x_1^{(3)}(3) &= 011_2 \oplus 110_2 = 101_2 = 5, & x_2^{(3)}(3) &= 011_2 \oplus 101_2 = 110_2 = 6. \end{aligned}$$

In fact, when $n = p - 1$, the sequence

$$x_1^{(n+1)}(n) = (0, 3, 6, 5, 12, 15, 10, 9, 24, 27, \ldots)$$

generates the xor bit-sum of n and $2n$ (sequence A048724 in the Online Encyclopedia of Integer Sequences (OEIS) database: http://oeis.org).

Lemma 3. *Define*

$$E_p(i, n) := d^{(i)}_{p-1-u_p(n)}$$

so that $w_i(n) = (-1)^{E_p(i,n)}$. Then for $0 \leq r < p$, we have

$$E_p(i, pn + r) = \begin{cases} d_{p-1-u_p(n)-r}, & \text{if } u_p(n) + r < p; \\ d_{p-1-s}, & \text{if } u_p(n) + r \geq p, \end{cases}$$

where $s = u_p(n) + r - p$. Moreover,

$$E_p(i, pn + r) - E_p(i, n) \equiv E_p(x_r(i), n). \tag{14}$$

Proof. Since $u_p(pn + r) = (u_p(n) + r)_p$, we have

$$E_p(i, pn + r) = d_{p-1-(u_p(n)+r)_p}.$$

Now consider two cases: either $u(n) + r < p$ or $u(n) + p \geq p$. If $u(n) + r < p$, then

$$E_p(i, pn + r) = d_{p-1-u_p(n)-r}.$$

On the other hand, if $u(n)+r \geq p$, then set $s = u_p(n)+r-p$ so that $(u_p(n)+r)_p = s$. It follows that

$$E_p(i, pn + r) = d_{p-1-s}$$

To prove (14), we again consider two cases. First, assume $u_p(n) + r < p$ so that $p - 1 - u_p(n) \geq r$. Then

$$\begin{aligned} E_p(i, pn + r) - E_p(i, n) &= d_{p-1-u_p(n)-r} - d_{p-1-u_p(n)} \\ &\equiv d_{p-1-u_p(n)} \oplus d_{p-1-u_p(n)-r} \\ &\equiv E_p(x_r(i), n). \end{aligned}$$

On the other hand, if $u_p(n)+r \geq p$, then set $s = u_p(n)+r-p$ so that $(u_p(n)+r)_p = s$. Since $p - 1 - u_p(n) < r$, we have

$$\begin{aligned} E_p(i, pn + r) - E_p(i, n) &= d_{p-1-s} - d_{p-1-u_p(n)} \\ &\equiv d_{p-1-u_p(n)} \oplus d_{p-1-s} \\ &\equiv d_{p-1-u_p(n)} \oplus d_{p-1-u_p(n)+(p-r)} \\ &\equiv E_p(x_r(i), n). \end{aligned}$$

$\square$

Theorem 16. *Let p be a positive integer. The weight sequences $w_i(n)$, $0 \le i \le 2^p - 1$, satisfy the recurrence*

$$w_i(pn + r) = w_{x_r(i)}(n)w_i(n), \tag{15}$$

where $n \in \mathbb{N}$ and $r \in \mathbb{Z}/p\mathbb{Z}$.

Proof. The recurrence follows easily from formula (14):

$$\begin{aligned}\frac{w_i(pn + r)}{w_i(n)} &= (-1)^{E_p(i,pn+r)-E_p(i,n)} \\ &= (-1)^{E_p(x_r(i),n)} \\ &= w_{x_r(i)}(n).\end{aligned}$$

□

Example 17. Let $p = 3$. Then $w_0(n) = 1$ for all $n \in \mathbb{N}$ and the other weight sequences, $w_1(n)$, $w_2(n)$, $w_3(n)$, satisfy the following recurrences:

$$\begin{aligned}&w_1(3n) = w_0(n)w_1(n),\ w_1(3n+1) = w_3(n)w_1(n),\ w_1(3n+2) = w_5(n)w_1(n);\\ &w_2(3n) = w_0(n)w_2(n),\ w_2(3n+1) = w_6(n)w_2(n),\ w_2(3n+2) = w_3(n)w_2(n);\\ &w_3(3n) = w_0(n)w_3(n),\ w_3(3n+1) = w_5(n)w_3(n),\ w_3(3n+2) = w_6(n)w_3(n).\end{aligned}$$

Acknowledgment. The author wishes to thank Greg E. Coxson for many useful discussions on radar and complementary code matrices. He also wishes to thank the reviewer for his editorial suggestions to improve this article.

References

[1] J.-P. Allouche and J. Shallit, *The ubiquitous Prouhet-Thue-Morse sequence*, Sequences and Their applications, Proc. SETA'98 (Ed. C. Ding, T. Helleseth, and H. Niederreiter). New York: Springer-Verlag, pp. 1-16, 1999.

[2] J.-P. Allouche and J. Shallit, Automatic Sequences: Theory, Applications, Generalizations, Cambridge University Press, New York, 2013.

[3] J.-P. Allouche and G. Skordev, *Von Koch and Thue-Morse revisited*, Fractals **15** (2007), 405-409.

[4] K. G. Beauchamp, Walsh Functions and Their Applications, Academic Press, London, 1975.

[5] E. D. Bolker, C. Offner, R. Richman, C. Zara, *The Prouhet-Tarry-Escott Problem and Generalized Thue-Morse Sequences*, 2013. arXiv:1304.6756 [math.CO]

[6] Y. C. Chi, A. Pezeshki, and A. R. Howard, *Complementary waveforms for sidelobe suppression and radar polarimetry*, Principles of Waveform Diversity and Design, M. Wicks, E. Mokole, S. Blunt, R. Schneible and V. Amuso (editors), SciTech Publishing, Raleigh, NC, 2011.

[7] G. E. Coxson and W. Haloupek, *Construction of complementary code matrices for waveform design*, IEEE Trans. Aerospace and Electr. Systems **49** (2013), 1806-1816.

[8] M. Drmota and J. F. Morgenbesser, *Generalized Thue-Morse sequences of squares*, Israel J. of Math. **190**, 157-193.

[9] M. Euwe, *Mengentheoretische Betrachtungen ü das Schachspiel*, Proc. Konin. Akad. Wetenschappen, Amsterdam **32** (1929), 633-642.

[10] Emmanuel Ferrand, *An Analogue of the Thue-Morse Sequence*, Electron. J. Combin. **14** (2007), #R30.

[11] N. J. Fine, *On the Walsh functions*, Trans. Amer. Math. Soc. **65** (1949), 372-414.

[12] M. J. E. Golay, *Multislit spectroscopy*, J. Opt. Soc. Amer. **39** (1949), 437-444.

[13] L. Kennard, M. Zaremsky, and J. Holdener, *Generalized Thue-Morse sequences and the Von Koch curve*, Int. J. Pure Appl. Math. **47** (2008), 397-403.

[14] D. H. Lehmer, *The Tarry-Escott problem*, Scripta Math. **13** (1947), 37-41.

[15] J. Ma and J. Holdener, *When Thue-Morse meets Koch*, Fractals **13** (2005), 191-206.

[16] Eiji Miyanohara, *Study on the non-periodicity of the generalized Thue-Morse sequences generated by cyclic permutations*, 2013. arXiv:1305.2274 [math.NT]

[17] L. Moretti L and V. Mocella, *Two-dimensional photonic aperiodic crystals based on Thue-Morse sequence*, Optics Express **15** (2007),15314-15323.

[18] M. Morse, *Recurrent geodesics on a surface of negative curvature*, Trans. Amer. Math. Soc. **22** (1921), 84-100.

[19] H. D. Nguyen and G. E. Coxson, *Doppler tolerance, complementary code sets, and the generalized Thue-Morse sequence*, 2014. arXiv:1406.2076v2 [cs.IT]

[20] I. Palacios-Huerta, *Tournaments, fairness and the Prouhet-Thue-Morse sequence*, Economic Inquiry **50** (12012), 848-849.

[21] A. Pezeshki, A. R. Calderbank, W. Moran, and S. D. Howard, *Doppler resilient Golay complementary waveforms*, IEEE Trans. Inform. Theory **54** (2008), no. 9, 4254-4266.

[22] E. Prouhet, *Mémoire sur quelques relations entre les puissances des nombres*, C. R. Acad. Sci., Paris **33** (1851), 225.

[23] H. Rademacher, *Einige Sätze über Reihen von allgemeinen Orthogonalfunktionen*, Math. Ann. **87** (1922), 112-138.

[24] R. M. Richman, *Recursive binary sequences of differences*, Complex Systems 13 (2001), 381-392.

[25] R. Riklund, M. Severin, and Y. Liu, *The Thue-Morse aperiodic crystal: a link between the Fibonacci quasicrytal and the periodic crystal*, Int. J. Mod. Phys. B **1** (1987), 121-132.

[26] P. Séébold, *On some generalizations of the Thue-Morse morphism*, Theoret. Comput. Sci. **292** (2003), 283-298.

[27] S. G. Tzafestas, Walsh functions in signal and systems analysis and design (Benchmark Papers in Electrical Engineering and Computer Science, Vol 31), Springer, 1985.

[28] A. Thue, *Über unendliche Zeichenreihen*, Norske vid. Selsk. Skr. Mat. Nat. Kl. **7** (1906), 1-22. (Reprinted in Selected Mathematical Papers of Axel Thue, edited by T. Nagell. Oslo: Universitetsforlaget, 1977, 139-158).

[29] J. L. Walsh, *A closed set of normal orthogonal functions*, Amer. J. Math. **45** (1923), 5-24.

[30] E. M. Wright, *Prouhet's 1851 solution of the Tarry-Escott problem of 1910*, Amer. Math. Monthly **102** (1959), 199-210.