# Time-Hopping Patterns derived from Permutation Sequences for Ultra-Wide-Band Impulse-Radio Applications 

TOMASO ERSEGHE<br>Dipartimento di Elettronica ed Informatica<br>Università di Padova<br>Via Gradenigo 6/A, 35131 Padova

ITALY


#### Abstract

Time-hopping (TH) communication techniques have gathered increasing attention since the introduction of ultra-wide-band impulse-radio, by Scholtz, in 1993. In these systems, the design of TH sequences is a critical point, since they constitute the only source of diversity that protects the transmitted signal from the interference caused by multipath and by the presence of other users. Moreover, they represent a reliable source for synchronization and channel estimation. In this paper the author addresses the issue of building TH patterns with very good correlation properties by use of a construction based upon the theory of permutation-sequences (PSs) that was recently proposed in the context of frequency-hopping by Moreno. The paper devotes much care in the analytical evaluation of correlation properties (correcting some mistakes of the literature) and in the identification of the widest possible class of TH patterns based upon PSs.


Key-Words: - Impulse radio, ultra wide band, time hopping, frequency hopping, permutation sequences.

## 1 Introduction

Time-hopping (TH) multi-user-diversity techniques have gathered increasing attention since the introduction, in 1993, of ultra-wide-band impulse-radio (UWB-IR) [1]. UWB-IR is a multi-user modulation technique that employs ultra narrow pulses $w(t)$ of temporal extension of less than a nanosecond (hence of ultra-wide-bandwidth in excess of a few GHz ). The way to encode information is an hybrid modulation that uses TH code division multiple access and binary PPM modulation. The signal associated to user $i$ is thus [3], [4]

$$
\begin{equation*}
s^{(i)}(t)=\sum_{m=-\infty}^{+\infty} w\left(t-m T_{f}-c_{m}^{(i)} T-\delta b_{m}^{(i)}\right) \tag{1}
\end{equation*}
$$

where $T_{f}$ is the frame duration, and we have one pulse per user per frame, $\left\{c_{m}^{(i)}\right\}$ is the TH sequence associated with user $i$, and $\left\{b_{m}^{(i)}\right\}$ is a binary encoded sequence carrying the information to be transmitted ${ }^{1}$.

[^0]

Figure 1: Exemplification of the TH signal $s_{n}^{(i)}$ associated to the TH sequence $c_{m}^{(i)}$ with $N=5$.

The design of TH sequences is a critical point for any communication technique employing TH, and so for UWB-IR, since they constitute the main source of diversity for the system. By inspection of (1), we see that the TH sequence $\left\{c_{m}^{(i)}\right\}$, with elements belonging to the alphabet $\{0,1, \ldots, N-1\}$, is in practice determining the sub-frame of duration $T$ in which datatransmission occurs (and we assume that $T_{f}=N T$ ). Thus, the situation is that depicted in Fig. 1, where it

[^1]is also shown that, for our purposes, it can be convenient to associate to every TH sequence a binary signal where ones indicate the slots available for transmission. According to the above notation, such a binary signal is
\[

$$
\begin{equation*}
s_{n}^{(i)}=\sum_{m=-\infty}^{+\infty} \delta_{n, m N+c_{m}^{(i)}} \tag{2}
\end{equation*}
$$

\]

where $\delta_{n, m}$ is the Kronecker delta function. In each frame interval $N k+[0, N-1]$, of duration $N$, it carries a one and $N-1$ zeros. In other words, $s_{n}^{(i)}$ exhibits a one-pulse-per-frame structure.

It is intuitive to see that, in order to be successfully employed in TH applications, the signals $s_{n}^{(i)}$ must have very good self-correlation and cross-correlation properties, that is, the signal $s_{n}^{(i)}$ associated to user $i$ and the delayed signal $s_{n+u}^{(j)}$ associated to user $j$ (where $i=j$ for self-correlation) must have in common as few positions where transmission occurs as possible. In particular, the request on self-correlation is two-fold. On one side, it guarantees robust synchronization and robust channel estimation, especially with UWB-IR where multipath components can be modeled as distinct arrivals [5], [6]. On the other side, it guarantees to attenuate the inter-symbolinterference due to the propagation delay spread. Instead, the request on cross-correlation clearly guarantees a minimization of the multi-user-interference which, in the presence of multipath, is true both for synchronous and asynchronous transmission.

According to the literature, the construction of TH sequences could be addressed in two ways. The first approach is to make use of frequency-hopping (FH) results, that is to directly employ known FH sequences, since the similarity between TH and FH is evident. Incidentally, this is the approach of the only explicit references found by the author on TH sequences constructions for UWB-IR, [7], [8]. An alternative approach would be to make use of optical orthogonal codes (OOC), typically employed in fiber-optics [9], [10], [11], which have optimal correlation properties but do not guarantee the one-pulse-per-frame structure of Fig. 1.

In this paper we follow the FH approach, guaranteeing the one-pulse-per-frame structure, and investigate the possibility to use, for TH applications, the FH patterns based upon permutation sequences (PSs)
recently proposed by Moreno [12]. The paper is organized as follows. Section II reviews the construction of hopping patterns based upon PSs. Section III proceeds with the analytical evaluation of correlation properties in the context of TH , and underlines the relation to FH . We note that, the analytical evaluation of correlation properties is a central result of this paper, since in the literature this topic was not correctly addressed. For this reason, correlation properties of the hopping sequences (based upon PSs) proposed in the literature are reviewed in an example. Finally, Section IV identifies the widest possible classes of hopping patterns based upon PSs that guarantee noncatastrophic correlation properties.

## 2 Hopping Patterns based upon PSs

### 2.1 Mathematical preliminaries

A Galois field (GF) is a finite field $\boldsymbol{F}_{q}=$ $\{0,1, \ldots, q-1\}$ of $q=p^{m}$ elements where $p$ is a prime (see [13] for an overview on GFs). A projective line $(\mathrm{PL}), \boldsymbol{P}_{q}$, is an generalization of a GF extended to include the element $\infty$, that is

$$
\boldsymbol{P}_{q}=\boldsymbol{F}_{q} \cup\{\infty\}
$$

In PLs the element $\infty$ has the usual properties, namely $x+\infty=\infty, x \cdot \infty=\infty, x / \infty=0$ and $x / 0=\infty$, and also the usual indeterminates $\infty-\infty$, $0 / 0, \infty / \infty$ and $0 \cdot \infty$.

A permutation sequence is a sequence $\left\{a_{m}\right\}$ of period $q+1$ such that the values in a period represent a permutation of the elements of $\boldsymbol{P}_{q}$ and with the further property that each value is determined from the previous by application of a function, that is $a_{m+1}=f\left(a_{m}\right)$ [12]. Moreover, it is customary to set $a_{0}=0$. The existence of functions $f(\cdot)$ that generate a PS is assured by the following theorem [13].

Theorem 1 For every field $\boldsymbol{F}_{q}$ there always exist a primitive element $\alpha$ such that $x^{2}+x+\alpha$ is an irreducible polynomial over the field and the function

$$
\begin{equation*}
f(x)=\frac{-\alpha}{x+1}, \quad x \in \boldsymbol{P}_{q} \tag{3}
\end{equation*}
$$

generates a PS of the elements of $\boldsymbol{P}_{q}$. A period of the resulting sequence is thus of the form $0,-\alpha, \ldots,-1, \infty$

In this context, we define the mapping function $A: Z_{\bmod q+1} \rightarrow \boldsymbol{P}_{q}$ (where $Z_{\bmod q+1}$ is the ring of integers modulo $q+1$ ) that maps $m$ into $a_{m}$, and its inverse $A^{-1}: \boldsymbol{P}_{q} \rightarrow Z_{\bmod q+1}$.
A further concept that needs to be introduced is, according to the language of [12], that of fractional linear transformations (FLTs) in $\boldsymbol{P}_{q}$. We thus recall the following results [13].

## Theorem 2 A fractional linear transformation

$$
\begin{equation*}
g(x)=\frac{a x+b}{c x+d}, \quad x \in \boldsymbol{P}_{q} \quad a, b, c, d \in \boldsymbol{F}_{q} \tag{4}
\end{equation*}
$$

where a $d \neq b c$ (so that numerator and denominator do not simplify), provides a permutation of the elements of $\boldsymbol{P}_{q}$. Two different FLTs $g(x)$ and $h(x)$ have at most two coincidences, that is values of $x$ for which $g(x)=h(x)$, whereas two FLTs with three or more coincidences are equal. The combination of FLTs is an FLT.

### 2.2 Definition and problem formulation

According to the above notation, the most general formulation of a class of hopping patterns (either TH or FH ) based upon PSs is

$$
\begin{equation*}
c_{m}^{(i)}=A^{-1}\left(g_{i}\left(a_{m}\right)\right), \quad i=1, \ldots, N_{u} \tag{5}
\end{equation*}
$$

where we require that each $g_{i}(x)$ is a FLT. Note that, each of the sequences in (5) has period length $L=$ $q+1$ and alphabet width $N=q+1$. Moreover, it is easily seen that $\left\{c_{0}^{(i)}, \ldots, c_{q}^{(i)}\right\}$ is a permutation of the elements $\{0, \ldots, q\}$.
The definition of patterns of the form of (5) that are suitable for TH (or FH ) applications, requires to properly define the FLT family $\left\{g_{i}(\cdot), \quad i=\right.$ $\left.1, \ldots, N_{u}\right\}$. To correctly address the problem of optimally choosing such a FLT family, we first need to investigate methods for the analytical evaluation of correlation properties.

## 3 Correlation Properties

### 3.1 Preliminaries

As we have seen, hopping patterns based upon PSs have the characteristic to be periodic of period $L=$ $q+1$. This is a welcome property, which guarantees
a certain ease in synchronization, and which implies that the TH signal (1) can be written as

$$
\begin{equation*}
s_{n}^{(i)}=\sum_{m=0}^{L-1} \delta_{n, m N+c_{m}^{(i)}}^{(N L)} \tag{6}
\end{equation*}
$$

where $\delta_{n, m}^{(N L)}$ is the Kronecker delta function periodic of period $N L$.
The correlation between user $i$ and user $j$, that is $C_{i, j}(u)=\sum_{n=0}^{N L-1} s_{n}^{(i)} s_{n+u}^{(j)}$, after substutution of (6) becomes

$$
\begin{equation*}
C_{i, j}(u)=\sum_{m, n=0}^{L-1} \delta_{u+m N+c_{m}^{(i)}, n N+c_{n}^{(j)}}^{(N L)} \tag{7}
\end{equation*}
$$

and is a periodic function in $u$ of period $N L$. In a period, (7) consists of $L^{2}$ Kronecker deltas and optimal correlation properties are thus obtained whenever these "deltas" are scattered all-over the period. Note also that, for $i=j$ equation (7) forces $C_{i, i}(0)$, that is the signal energy, to $L$. By further expressing $u$ as $k N+\ell$ where $0 \leq k<L$ and $0 \leq \ell<N$, we have (recall that $0 \leq c_{m}^{\overline{(i)}}<N$ )

$$
\begin{equation*}
C_{i, j}(k N+\ell)=\sum_{m=0}^{L-1} \delta_{c_{m}^{(i)}+\ell, c_{m+k}^{(j)}}+\delta_{c_{m}^{(i)}+\ell, N+c_{m+k+1}^{(j)}} \tag{8}
\end{equation*}
$$

where the modulo operation disappeared.

### 3.2 Quality measures

We now introduce two quantities as quality measures for classes of TH sequences, which will turn very useful for comparison. These are

$$
\begin{equation*}
S_{\max }=\max _{i, k \neq 0} C_{i, i}(k), \quad C_{\max }=\max _{i, j \neq i, k} C_{i, j}(k) \tag{9}
\end{equation*}
$$

where $C_{\text {max }}$ is the maximum value for crosscorrelation, and $S_{\text {max }}$ is the maximum value for selfcorrelation $\left(C_{i, i}(0)=L\right.$ excluded). Evidently, the lower the values $S_{\max }$ and $C_{\text {max }}$ the better the class.

In this context, classes of TH sequences are said having ideal self-correlation properties if $S_{\text {max }}=1$ and ideal cross-correlation properties if $C_{\max }=1$. These evidently require that the Kronecker deltas in (7) are distinct and also that $N \geq L$. We note that, classes of ideal TH sequences with a one-pulse-perframe structure (e.g. those derived from FH patterns)
are, to the author's knowledge, not known ${ }^{2}$. So we will talk of hopping classes suitable for TH whenever both values $S_{\max }$ and $C_{\text {max }}$ are $\ll L$ and as close as possible to 1 . Instead, we will talk of catastrophic classes (i.e. useless for TH applications) whenever $S_{\text {max }}$ or $C_{\text {max }}$ approach $L$, that is as soon as some peak occurs in the correlation functions.

### 3.3 Analytical evaluation

The analytical evaluation of correlation properties for a class of TH sequences can be performed by direct use of (8). This requires to identify, for any $k$ and $\ell$, the maximum number of solutions in $m$ to

$$
\begin{equation*}
c_{m}^{(i)}+\ell=c_{m+k}^{(j)} \quad \text { and } \quad c_{m}^{(i)}+\ell=N+c_{m+k+1}^{(j)} \tag{10}
\end{equation*}
$$

Although finding a solution to (10) is a very hard task, the evaluation of the maximum number of solutions in $m$ to

$$
\begin{equation*}
c_{m}^{(i)}+\ell=c_{m+k}^{(j)} \quad(\bmod N) \tag{11}
\end{equation*}
$$

is a much feasible operation. In addition, by comparison between (10) and (11), we note that twice the maximum number of solutions to (11) is an upper bound to the maximum number of solutions to (10), so we follow this approach. For TH sequences based upon PSs, our bound turns out to be very strict and, in almost all cases, upper bound and maximum coincide.

The particularization of (11) to hopping patterns generated from PSs (5) further gives

$$
\begin{equation*}
f^{\ell}\left(g_{i}(x)\right)=g_{j}\left(f^{k}(x)\right), \quad x=a_{m} \tag{12}
\end{equation*}
$$

with $f^{k}(\cdot)$ the the $k$-fold application of $f(\cdot)$ and where we used the property $A\left(A^{-1}(x)+\ell\right)=f^{\ell}(x)$ whose straightforward derivation is left to the reader.

The possibility to evaluate the maximum number of solutions of (12) in $x$ (or equivalently $a_{m}$, or $m$ ) is a central result of this paper, and is given by the fact that $f^{k}(x)$ is a FLT in $x$. According to Theorem 3, by imposing three values to the generic function (4), we

[^2]then obtain that $f^{k}(x)$ can be written explicitly as ${ }^{3}$
\[

$$
\begin{equation*}
f^{k}(x)=\frac{\alpha a_{k}+x\left(\alpha+a_{k}\right)}{\alpha-x a_{k}} \tag{13}
\end{equation*}
$$

\]

This guarantees that both terms of (12) are FLTs, since the combination of FLTs is an FLT. By application of Theorem 3 we further obtain that (12) has up to 2 solutions once we provide that (12) is not an equivalence. As a direct consequence, a class of hopping sequences generated by the FLT family $\left\{g_{i}(\cdot), \quad i=1, \ldots, N_{u}\right\}$ is suitable for TH whenever the generating FLTs do not make (12) an equivalence for any value of $i, j, k, \ell$ other than $i=j$ and $k=\ell=0$ (that refers to the energy of the TH signal). In this case, we will talk of a non catastrophic class, for which we have $S_{\max }=C_{\max }=4$.

To show how the analytical evaluation works we now give some examples. This is of some interest since the literature did not address this topic correctly.
Example 1 We derive correlation properties for the linear class generated by the FLTs

$$
\begin{equation*}
g_{i}(x)=x \cdot q i, \quad i=1,2, \ldots, q-1 \tag{14}
\end{equation*}
$$

that was proposed in [12]. To this end, we must check whether (12) gives an equivalence for some $i, j, k, \ell$. This is simply done by substitution of (14) and (13) into (12), that gives

$$
\frac{\alpha a_{\ell}+x i\left(\alpha+a_{\ell}\right)}{\alpha-x i a_{\ell}}=\frac{\alpha j a_{k}+x j\left(\alpha+a_{k}\right)}{\alpha-x a_{k}}
$$

where operations are defined on $\boldsymbol{P}_{q}$. From this we derive the equivalent equation system

$$
\left\{\begin{array}{l}
\alpha a_{\ell}=\eta \alpha j a_{k} \\
i\left(\alpha+a_{\ell}\right)=\eta j\left(\alpha+a_{k}\right) \\
\alpha=\eta \alpha \\
i a_{\ell}=\eta a_{k}
\end{array}\right.
$$

where $\eta \neq 0$. After some straightforward algebra, we obtain that solutions to the system are found for some $k$ and $\ell$ whenever (see [14])

$$
\begin{equation*}
i j=1 \tag{15}
\end{equation*}
$$

with the exception, when $q$ is not a power of 2 , of $i=j=-1$.

[^3]Equation (15) indicates that the sequence $i=1$ has catastrophic self-correlation properties, while sequences $i$ and $j=1 / i$ have catastrophic crosscorrelation properties. So, by limiting the choice of $i$ in (14) to

$$
\begin{equation*}
i=\alpha^{1}, \alpha^{2}, \ldots, \alpha^{N_{u}} \quad N_{u}=\lfloor(q-1) / 2\rfloor \tag{16}
\end{equation*}
$$

where $\alpha$ is primitive in $\boldsymbol{F}_{p}$, we obtain a class of $\lfloor(q-$ 1) $/ 2\rfloor$ TH sequences with $S_{\max }=C_{\max }=4$. Note that this is the widest subset of the linear construction that guarantees to be non catastrophic.

Example 2 Following the same procedure, it can be easily found that, the correlation properties of the hyperbolic class generated from the FLT set $g_{i}(x)=$ $\alpha i / x$ leads to (15) and to the choice of $i$ as in (16). Note that, this is a slightly modified, but equivalent, version of the hyperbolic code proposed in [12].

Example 3 The possibility of co-existence between the linear and the hyperbolic class can be instead tested by assuming that, in (12), $g_{i}(x)=i x$ and $g_{j}(x)=\alpha j / x$. In this case, the reference equation turns out to be an equivalence whenever

$$
\begin{equation*}
i+\frac{1}{i}+j+\frac{1}{j}=\frac{1}{\alpha} \quad i=\alpha^{k_{i}}, j=\alpha^{k_{j}} \tag{17}
\end{equation*}
$$

where, according to (16), $k_{i}, k_{j}=1, \ldots, N_{u}$.
Equation (17) constitutes a quick check to individuate whether a sequence of the hyperbolic class can coexist with the linear class. For instance, with $q=2^{4}$, generating polynomial $x^{4}+x+1$ and $\alpha=9$, equation (17) is solved for $k_{i}=1, k_{j}=2$ and for $k_{i}=2, k_{j}=1$ (according to this result, the example above in Fig. 2 shows a catastrophic collision between user $i=\alpha^{1}=9$ and user $j=\alpha^{2}=13$ ). So, the joint class allows for up to $2 N_{u}-2=12$ non catastrophic sequences, that is $k_{j}=1,2$ excluded. For $q=2^{5}$ the maximum number of users is instead $2 N_{u}-8=22$. None of the examples reaches the $q-2$ non catastrophic sequences claimed in [12].

### 3.4 Relation to FH results

Equation (8) is closely related to the correlation measure in FH applications, which reads as

$$
\begin{equation*}
C_{i, j}(k, \ell)=\sum_{m=0}^{L-1} \delta_{c_{m}^{(i)}+\ell, c_{m+k}^{(j)}} \tag{18}
\end{equation*}
$$



Figure 2: Co-existence between linear and hyperbolic TH sequences for $q=2^{4}$ (we used $x^{4}+x+1$ as generating polynomial and $\alpha=9$ ). Recalling that $C_{i, j}(u) \geq 0$, the figure shows an example of catastrophic collision (top half) and one of perfect coexistence (bottom half in upside-down fashion).
where $k$ represents the frame displacement and $\ell$ the presence of a frequency shift. So, (11) is the reference equation for correlation properties in FH applications as well. However, in FH the maximum number of solutions to (11) should be considered once (as opposed to the TH twice), as clarified by inspection of (18). This suggests that use of FH patterns for TH applications give slightly degraded performances. In particular, in the FH context, hopping patterns based upon PSs guarantee $S_{\max }=C_{\max }=2$.

## 4 Wider Classes based upon PSs

### 4.1 General results

The problem to derive the widest possible class of hopping patterns based upon PSs (valid both for TH and FH ) can be addressed exhaustively using the tools developed in this paper. The problem can be reformulated in the following terms. We need to identify an appropriate FLT family $\left\{g_{i}(\cdot), \quad i=\right.$ $\left.1, \ldots, N_{u}\right\}$ for which (12), or equivalently,

$$
\begin{equation*}
g_{i}(x) \neq f^{-\ell}\left(g_{j}\left(f^{k}(x)\right)\right) \tag{19}
\end{equation*}
$$

is satisfied for every choice of $i, j, k$, $\ell$ other than $i=j, k=\ell=0$.

We note that, (19) induces a natural partition of the set $\mathcal{F}$ of all FLTs. In fact, let $g_{i}(x)$ be a FLT, and define the FLT set

$$
\begin{equation*}
\mathcal{J}_{i}=\left\{f^{-\ell}\left(g_{i}\left(f^{k}(x)\right)\right) \mid k, \ell=0, \ldots, q\right\} \subset \mathcal{F} \tag{20}
\end{equation*}
$$

which is close with respect to the operation that generates it,

$$
\begin{equation*}
h(x) \in \mathcal{J}_{i} \quad \Longrightarrow \quad f^{-\ell}\left(h\left(f^{k}(x)\right)\right) \in \mathcal{J}_{i} \tag{21}
\end{equation*}
$$

This assures that there must exist a partition of $\mathcal{F}$ into sets of the form (20), and this partition is unique. In particular, given any two elements belonging to different sets, $g_{i} \in \mathcal{J}_{i}$ and $g_{j} \in \mathcal{J}_{j}$ with $i \neq j$, these always satisfy (19), that is, the hopping sequences they generate have non-catastrophic crosscorrelation properties. Furthermore, (19) assures that sets $I_{i}$ with cardinality $(q+1)^{2}$ (that we call full cardinality sets) generate hopping sequences with noncatastrophic self-correlation properties. In conclusion, the widest possible class of hopping patterns based upon PSs can be obtained by choosing one representative from each of the full-cardinality-sets.

We note that sets with restricted cardinality exist and these are the two sets generated by the FLTs $x$ and $-x-1$, that is ${ }^{4}$

$$
\begin{align*}
\mathcal{J}_{x} & =\left\{f^{k}(x) \mid k=0, \ldots, q\right\}  \tag{23}\\
\mathcal{J}_{-x-1} & =\left\{f^{k}(-x-1) \mid k=0, \ldots, q\right\}
\end{align*}
$$

both with cardinality $(q+1)$, while all the remaining sets have full cardinality. Since the number of different FLTs is $(q+1) q(q-1)$, the number of sets with full cardinality is

$$
\frac{(q+1) q(q-1)-2(q+1)}{(q+1)^{2}}=q-2
$$

and, with the addition of (23), the class of FLTS can be thus partitioned in $q$ sets. So, the following theorem holds.

Theorem 3 There exist at most $N_{u}=q-2$ noncatastrophic hopping patterns derived from PSs, with correlation properties $C_{\max }=S_{\max }=2$ for FH applications and $C_{\max }=S_{\max }=4$ for TH applications.

[^4]

Figure 3: Correlation properties for the TH class (24) with $q=2^{4}$ (we used $x^{4}+x+1$ as generating polynomial and $\alpha=9$ ).

### 4.2 The case of $q$ a power of 2

The identification of a representative for each set is particularly easy when $q$ is a power of 2 . In this case, a suitable FLT class of representatives is

$$
\begin{equation*}
g_{i}(x)=x+{ }_{\left(2^{m}\right)} i, \quad i=0,1, \ldots, 2^{m}-1 \tag{24}
\end{equation*}
$$

Restricted cardinality sets are generated by $g_{0}(x)=$ $x$ and $g_{1}(x)=x+1=-x-1$ (since in $\boldsymbol{F}_{q}, q=2^{m}$ we have the equivalence $x=-x$ ) so, for TH applications, we need to restrict the class to $i=2, \ldots, q-1$. The proof that (24) with $i \neq 0,1$ constitutes a class of $2^{m}-2$ non catastrophic sequences can be derived as in Example 1 (but the interested reader can find a detailed proof in [14]), while an illustrative example of correlation properties is given in Fig. 3 for $q=2^{4}$.

### 4.3 The case of $q$ not a power of 2

For $q$ not a power of 2 , all expressions like (24) seem to generate a restricted number of representatives. We thus proceed by inspection and present an efficient method to obtain exact results.

As can be easily proved, each set $\mathcal{J}_{i}$ contains at least one linear function, say $g_{i}(x)=a x+b$. By application of definition (20) we further derive that each full-cardinality-set contains exactly $q+1$ linear functions of the form $g_{i, k}(x)=a_{k} x+b_{k}$, with
$a_{k}=\frac{k^{2}\left[\frac{1}{a}+\frac{(a-b)(a-b-1)}{a \alpha}\right]+k[2(a-b)-1]+a \alpha}{k^{2}+k+\alpha}$
$b_{k}=\frac{k^{2}(a-b-1)+k\left[\frac{b(a-b-1)}{a}+\frac{\alpha\left(a^{2}-1\right)}{a}\right]+b \alpha}{k^{2}+k+\alpha}$
where $k \in \boldsymbol{P}_{q}$ and where operations are defined on $\boldsymbol{P}_{q}$. Note that, for $k=0$ we obtain $g_{i, 0}(x)=a x+b$.

Equation (25) allows to partition the set of linear functions into subsets belonging to different full-cardinality-sets (which is much more efficient than partitioning the FLTs set $\mathcal{F}$ ), and thus to identify representatives. As a reference example, for $q=3^{3}$, generating polynomial $x^{3}+2 x+1$ and $\alpha=10$, we found the 25 full-cardinality-set representatives

$$
\begin{array}{ccccccc}
x+1 & x+3 & x+4 & x+5 & x+9 & x+10 & x+11 \\
x+12 & x+13 & x+14 & x+15 & x+16 & x+17 & 2 x+3 \\
2 x+4 & 2 x+9 & 2 x+10 & 2 x+12 & 2 x+16 & 3 x+2 & 3 x+9 \\
3 x+10 & 3 x+11 & 4 x+14 & 5 x+1 & & &
\end{array}
$$

## 5 Conclusion

In this paper the author addressed the issue of building TH patterns with very good correlation properties, by use of a construction based upon the theory of PSs recently proposed by Moreno [12]. These have period $L=q+1$ and frame width $N=q+1$ where $q$ is a power of a prime. The paper devoted much care in the analytical evaluation of correlation properties, leading to the identification of the widest possible class of TH patterns based upon PSs that consists of $q-2$ sequences. The expression for the hopping class is straightforward when $q$ is a power of 2 , which suggests use of this class for practical use (also because modulo 2 arithmetics are much more suitable for hardware applications). In conclusion, the present contribution can constitute a valid reference for the upcoming interest in UWB-IR and TH applications.

## References:

[1] R.A. Scholtz, "Multiple Access with TimeHopping Impulse Modulation", MILCOM 1993, pp. 447-450, Bedford, MA, October 11-13, 1993.
[2] P. Withington, "Ultra-Wideband: A Wide Open Opportunity", lst European Ultra Wideband Workshop, Brussels, 13th December 2000.
[3] M.Z. Win, and R.A. Scholtz, "Ultra-Wide Bandwidth Time-Hopping Spread-Spectrum Impulse Radio for Wireless Multiple-Access Communications", IEEE Trans. on Comm., Vol. 48, No. 4, pp. 679-691, April 2000.
[4] F. Ramirez-Mireles, "Performance of Ultra Wideband SSMA Using Time-Hopping and Mary PPM'", IEEE Journal on Selected Areas in

Communications, Vol. 50, No. 1, pp. 244-249, January 2001.
[5] M.Z. Win, R.A. Scholtz, and M.A. Barnes, "Ultra-Wide Bandwidth Signal Propagation for Indoor Wireless Communications", IEEE ICC '97, Vol. 1, pp. 56-60, June 1997.
[6] D. Cassioli, M.Z. Win, and A.F. Molisch, "A Statistical Model for the UWB Indoor Channel", IEEE VTC Spring 2001, Rhodos, Greece, May 6-9, 2001.
[7] C. Corrada-Bravo, R.A. Scholtz, and P.V. Kumar, "Generating TH-SSMA Sequences with Good Correlation and Approximately Flat PSD Level", Ultra Wideband Conference, September 28, 1999.
[8] M.S. Iacobucci, M.G. Di Benedetto,"Time Hopping Codes in Impulse Radio Multiple Access Communication Systems", International Symposium on third generation Infrastructure and Services, Athens, Greece, 2-3 July 2001.
[9] R. Fuji-Hara and Y. Miao, "Optical Orthogonal Codes: Their Bounds and New Optimal Constructions", IEEE Trans. on Information Theory, Vol. 46, No. 7, pp. 2396-2406, November 2000.
[10] P. Fan and M. Darnell, Sequence Design for communications applications, Research Studies Press, John Wiley \& Sons Inc., Exeter, Great Britain, 1996.
[11] H. Chung and P.V. Kumar, "Optical Orthogonal Codes: New Bounds and an Optimal Construction", IEEE Trans. on Information Theory, Vol. 36, No. 4, pp. 866-873, July 1990.
[12] O. Moreno, and S.V. Maric, "A New Family of Frequency-Hop Codes", IEEE Trans. on Communications, Vol. 48, No. 8, pp. 1241-1244, August 2000.
[13] F.J. Mac Williams and N.J. Sloane, "The Theory of Error-Correcting Codes", Amsterdam, The Netherlands: North Holland, 1978.
[14] T. Erseghe, "Ultra Wide Band Pulse Communications", Ph.D. thesis, Universitá degli Studi di Padova, December 2001; available on-line at http://www.dei.unipd.it/~erseghe.


[^0]:    ${ }^{1}$ In the standard UWB-IR format, the encoded sequence $\left\{b_{m}^{(i)}\right\}$ is derived from a source binary sequence $\left\{a_{n}^{(i)}\right\}$ by a simple bit-repetition approach [1], [4]. Equation (1) takes into ac-

[^1]:    count that more efficient methods could be used to encode the

[^2]:    ${ }^{2}$ It is perhaps worth recalling that there exist OOC constructions with ideal correlation properties. However, these require to relax the one-pulse-per-frame constraint.

[^3]:    ${ }^{3} \mathrm{As}$ a check, note that (13) gives $f^{k}(0)=a_{k}$, and is valid for $k=0$ as well giving $f^{0}(x)=x$.

[^4]:    ${ }^{4}$ The proof can be obtained by first proving that each set of the form (20) contains at least one linear function of the form $a x+b$. It is then required to investigate which linear functions belong to sets with restricted cardinality. To do so, we must look for solutions to (12) where $g_{i}(x)=g_{j}(x)=a x+b$, that is

    $$
    \begin{equation*}
    f^{\ell}(a x+b)=a f^{k}(x)+b \tag{22}
    \end{equation*}
    $$

    After some straightforward algebra we get the two results $g(x)=$ $x$ and $g(x)=-x-1$.

