Codes for spread spectrum applications generated using chaotic dynamical systems

Broomhead, D. S. and Huke, J. P. and Muldoon, M. R.

1999

MIMS EPrint: **2005.14**

Manchester Institute for Mathematical Sciences
School of Mathematics

The University of Manchester

Reports available from: http://eprints.maths.manchester.ac.uk/
And by contacting: The MIMS Secretary
School of Mathematics
The University of Manchester
Manchester, M13 9PL, UK

ISSN 1749-9097

Codes for Spread Spectrum Applications Generated Using Chaotic Dynamical Systems

D. S. Broomhead, J. P. Huke, M. R. Muldoon*
Department of Mathematics
UMIST
P.O. Box 88,
Manchester M60 1QD
United Kingdom

22 November, 1996

Abstract

An approach to finding codes for use in direct sequence spread spectrum communications systems is described. It is based upon an analogy between codes having auto- and cross-correlation properties desirable for spread spectrum systems, and certain dynamical systems encountered in ergodic theory called systems with *Lebesgue spectrum*. Such systems are associated with collections of orthogonal functions and these functions can be used to generate collections of time series with zero cross-correlation functions. To generate codewords we must use truncated versions of these time series, for which the cross-correlations are no longer precisely zero: these truncated sequences correspond to periodic orbits of the dynamical system. The method for finding a code from a suitable periodic orbit is described, and an example, using a simple dynamical system known as the doubling map, is worked through in some detail.

1 Introduction

In areas such as radar, ranging, and spread spectrum communications, it is important to have a set of signals each of which is readily distinguishable from a time-shifted version of itself; for simultaneous ranging to several targets, and in code-division multiple-access (CDMA) communications it is also desirable that each signal should be distinguishable from time shifted versions of the other signals in the set. The technique used to distinguish these signals is usually *correlation*, so that these requirements translate into requirements on the auto- and crosscorrelation properties of the signals in the set.

Considerable effort has gone into devising sets of binary sequences with low auto- and crosscorrelations; this work has been comprehensively reviewed by Sarwate and Pursley [1]. Naturally enough, the approaches generally taken have called on the traditional subjects of linear feedback shift register sequences, and coding theory. These approaches have led to the well-known binary maximal-length sequences (m-sequences) for situations where only low autocorrelations are required, or where the number of signals with small crosscorrelation required is small, and to the 'Gold' and 'Kasami' sequences (and others), where larger

*DSB and JPH would like to acknowledge the support of the Defence Research Agency's Signal Processing Theory Group at Malvern where much of this work was done. MRM was funded by the EPSRC, grant number: GR/H81993.

numbers of signals are required. Lower bounds for the peak auto- and crosscorrelation among a set of binary sequences have also been found, and show that the Gold and Kasami sets are in some sense optimal. But the increasing interest in CDMA systems has maintained a continuing search for codes with good crosscorrelation properties [2], and recently an approach based on chaotic time series has been tried [3].

Here we describe a quite different approach to generating these codes. This is based upon an analogy that can be drawn between the crosscorrelation properties we want the code to have, and the properties of certain dynamical systems encountered in ergodic theory, known as systems with *Lebesgue spectrum* [5]. This analogy will be explained in some detail below. To set the scene, we briefly review dynamical systems and their invariant measures. The set of functions L_2, defined on the state space of the dynamical system is described, and hence systems with Lebesgue spectra are defined. The properties of these systems which might make them useful for the generation of codes are described, and also the way in which, given an appropriate dynamical system, one might generate a code from it. In essence, one identifies an orbit of the system, and generates codewords by evaluating certain specific functions at each point on the orbit. One example of such a dynamical system, known as the *doubling map*, is sufficiently simple to allow quite a lot to be said about the codes that can be generated using it. It turns out that with appropriate choices for the orbit, this system can generate m-sequences, and Gold codes.

2 Ergodic Dynamical Systems

For our purposes, a *dynamical system* consists of two things: a set S, called the *state space* of the system, and a function $\phi : S \to S$ which maps the states of the system (elements of S) to new states. We think of the map ϕ as describing the evolution of the system in one time step. Given a point $x \in S$ the *orbit* of x is the set $\{x, \phi x, \phi^2 x, \ldots\}$: that is, the states visited by the system, starting at x, as time progresses. Usually, the state space S is $\mathbb{R}^n$ or some subset of it. A simple example, which we shall discuss below, is the doubling map; here S is the unit interval $[0, 1]$ and ϕ is given by

$$\phi(x) = \begin{cases} 2x & \text{if } 0 \le x \le 1/2 \\ 2x - 1 & \text{if } 1/2 < x \le 1 \end{cases} \tag{1}$$

That is to say, each number is doubled modulo 1. A similar but slightly more complicated example is the *baker map*, in which S is now the unit square, and

$$\phi(x, y) = \begin{cases} (2x, \frac{1}{2}y) & \text{if } 0 \le x \le 1/2 \\ (2x - 1, \frac{1}{2}y + \frac{1}{2}) & \text{if } 1/2 < x \le 1 \end{cases} \tag{2}$$

Although the state spaces considered are usually subsets of $\mathbb{R}^n$, the branch of dynamical systems theory that interests us here—*ergodic theory*—assumes very little about the system. In technical terms, it assumes S is a *measure space* and that ϕ is *measure preserving*. Physically this means that there is some distribution on S and that the action of ϕ leaves this distribution unaffected. Often enough, this distribution can be described by a probability density function, and is the asymptotic distribution to which the system settles once transients have died away. If $w : S \to \mathbb{R}$ is a probability density function then invariance under ϕ means that

$$\int_B w(x)dx = \int_{\phi^{-1}B} w(x)dx$$

for each $B \subset S$.

The most interesting invariant measures are the *ergodic* ones. For these, averages over time equal averages over the state space in the following sense

$$\lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} f(\phi^i x_0) = \int_S f(x)w(x)dx \tag{3}$$

for almost all x_0, and any reasonable function $f : S \to \mathbb{R}$. (We say something is true for 'almost all' x if the set A for which it is *not* true has zero probability: $\int_A w(x)dx = 0$.) Although property (3) might seem to be very special, it turns out that ergodic systems are quite common. The doubling map is ergodic when supplied with the invariant density $w(x) = 1$ for all x; and the baker map is similarly ergodic with the invariant density $w(x, y) = 1$. An example of an ergodic system whose invariant density is not simply the constant function is the *logistic map*—another function of the interval $[0, 1]$ to itself defined by $\phi(x) = 4x(1 - x)$—with the density $w(x) = 1/\left(\pi\sqrt{x(1-x)}\right)$.

3 L_2 and systems with Lebesgue Spectrum

Apart from the dynamical system with its invariant measure, the other ingredient needed in the definition of systems with Lebesgue spectrum is the collection of functions $f : S \to \mathbb{R}$ for which the integral $\int_S |f(x)|^2 w(x)dx$ exists. This set of functions is called L_2 (or more completely $L_2(S, w)$, since it depends on the state space and the invariant density). It is well known that L_2 is a vector space, and a scalar product can be defined on it by

$$< f, g >= \int_S f(x)g(x)w(x)dx. \tag{4}$$

For the sets S and densities w which we are interested in the dimension of L_2 is infinite, but we can find an orthonormal basis: that is, a collection of functions $f_i, i = 1, \ldots$ such that

$$< f_i, f_j >= \delta_{ij}$$

and for any f in L_2, there is a sequence of real numbers $\{c_i\}_i^\infty$ such that

$$f = \sum_{i=1}^{\infty} c_i f_i. \tag{5}$$

Probably the most well-known example of a basis for an L_2 space is the set of trigonometric functions $\sin(2\pi mx), \cos(2\pi mx)$, $m = 0, 1, \ldots$, which form a basis for the square-integrable functions on the unit interval, $S = [0, 1]$, when $w(x) = 1$ is the density. In that case (5) is the familiar Fourier representation of f. The Walsh functions form another basis for the same L_2; we shall make use of this below.

A different density function on S leads to a different L_2 space. If we choose $w(x) = 1/\left(\pi\sqrt{x(1-x)}\right)$ (the invariant density for the logistic map) then the (shifted) Chebyshev polynomials form a basis for this L_2.

We are now in a position to describe systems with Lebesgue spectrum [5]. These systems not only have an ergodic invariant density, but are also associated with a special basis for L_2. This basis can be split up into classes, each of which has infinitely many functions; the number of these classes varies from system to system: some systems have just one class, but for the cases we are interested in there will usually be an infinite (countable) number of classes. This basis can be thus be written $\{f_{\lambda,j} : \lambda \in \Lambda, j \in \mathcal{Z}\}$: where λ labels the classes

and j labels the functions within each class. One important property that these particular basis functions $f_{\lambda,j}$ have is that for every λ and j

$$f_{\lambda,j} \circ \phi = f_{\lambda,j+1}. \tag{6}$$

(Recall that $f \circ \phi$ is the function defined by $f \circ \phi(x) = f(\phi(x))$.) This means that starting from one of the basis functions, all the others in the same class can be generated from it by compositions with powers of ϕ. Furthermore, this basis for L_2 is orthonormal: each function is orthogonal both to every other function in its class, and to every function in every other class.

For our purposes, it is property (6) and the orthogonality relations that we hope to use later to generate low crosscorrelations between codewords. It is therefore not necessary for the j index to take on all integral values; we shall be satisfied if j runs only over the natural numbers, so long as property (6) holds. This differs slightly from the definition of Lebesgue spectra usually found in ergodic theory. The doubling map furnishes a simple example of the systems we have in mind: the appropriate orthonormal basis is that constituted by the Walsh functions. We shall describe in some detail below how this basis is divided up into classes having the property 6. The bakers map (with $w(x) = 1$) is another example, in which j now does run over all the integers. The basis functions are products of pairs of Walsh functions, one function in each variable x and y.

A rather different example is provided by the so-called 'cat map' [5]: a mapping, ϕ, of the 2-torus to itself:

$$\phi \begin{pmatrix} x \\ y \end{pmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod 1$$

which has Lebesgue spectrum; $w(x, y) = 1$ is the invariant density, and the associated basis functions are the standard basis, $\{\psi_{m,n} = e^{2\pi i(mx+ny)} : (m, n) \in \mathcal{Z}^2\}$, for L_2 on the torus. To see this, consider the composition of ϕ with one of the basis elements:

$$\begin{aligned} (\psi_{m,n} \circ \phi)(x, y) &= e^{2\pi i(m(2x+y)+n(x+y))} \\ &= \psi_{(2m+n),(m+n)}(x, y) \\ &= \psi_{m',n'}(x, y). \end{aligned}$$

That is, composition of $\psi_{m,n}$ with the cat map yields another basis function whose indices (m', n') are given by acting on (m, n) with the matrix of the cat map. To relabel the basis $\{\psi_{m,n}\}$ in accordance with the $f_{\lambda,j}$ notation used in 6 above, one exploits the observation that the quadratic form $m^2 - mn - n^2$ is preserved by the action of the cat map's matrix on the standard indices. The value of this quadratic form essentially determines λ.

4 Sequences from systems with Lebesgue Spectrum

A natural way of deriving time series from a dynamical system is to 'observe' it. We imagine that the dynamical system represents some physical system such as a mechanical or electrical one. We make some sort of measurement on the system at regular intervals, the result of which is a single number (a force or voltage say, measured at some specific point in the system). The value that we measure is assumed to depend only on the state of the system; this means that there is some function $y : S \to \mathbb{R}$ such that for any state x of the system the result of the measurement when the system is in state x is $y(x)$. y is known as the *measurement function*. If at time 0 the system is in state x_0, and subsequently evolves through states $x_1, x_2, \ldots$, (where as we noted above $x_i = \phi^i x_0$)

then the observations form the sequence $y_0, y_1, y_2, \ldots$ where $y_i = y(x_i)$. (If the system is invertible, the sequence can be thought of as extending both forwards and backwards in time, $\ldots, y(x_{-1}), y(x_0), y(x_1), y(x_2), \ldots$.) So each orbit generates a time series of real numbers.

If we consider sequences generated in this way, it turns out that composition of the measurement function with ϕ corresponds to a time shift. To see this, suppose $\{y_i\}$ is a sequence generated using the measurement function y, and with x_0 the state at time 0. Consider what happens if $y \circ \phi$ is used as the measurement function; this generates a different sequence $\{y'_i\}$. However, $y'_i = y \circ \phi(x_i) = y \circ \phi(\phi^i x_0) = y(\phi^{i+1} x_0) = y_{i+1}$. Hence the $\{y'_i\}$ series is the same as the $\{y_i\}$ apart from a shift of one place to the left.

This time shift property forms a connection between integrals of the form (4) and crosscorrelations between time series. Suppose that $\phi : S \to S$ is a system with Lebesgue spectrum, and that $\{f_{\lambda,j}\}$ is the corresponding basis for L_2. Also suppose that $x_0 \in S$ is an initial condition for which the ergodic equality (3) holds. Let $\{y_k^{\lambda,j} : k = 0, 1, \ldots\}$ be the time series generated by using $f_{\lambda,j}$ as a measurement function: (i.e. $y_k^{\lambda,j} = f_{\lambda,j}(x_k)$). What are the auto- and crosscorrelation functions of these sequences?

The autocorrelation is defined by

$$\theta_{y^{\lambda,j}, y^{\lambda,j}}(l) = \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} y_k^{\lambda,j} y_{k+l}^{\lambda,j}$$

Hence

$$\begin{aligned} \theta_{y^{\lambda,j}, y^{\lambda,j}}(l) &= \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} f_{\lambda,j}(x_k) f_{\lambda,j}(x_{k+l}) \\ &= \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} f_{\lambda,j}(x_k) f_{\lambda,j}(\phi^l x_k). \end{aligned}$$

The property of systems with Lebesgue spectrum that $f_{\lambda,j} \circ \phi^l = f_{\lambda,j+l}$ implies that the right hand side is equal to

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} f_{\lambda,j}(x_k) f_{\lambda,j+l}(x_k)$$

and the ergodic property further implies that this is equal to

$$\int_S f_{\lambda,j}(x) f_{\lambda,j+l}(x) w(x) dx.$$

and the orthonormality of the basis functions finally implies that the autocorrelation function is equal to 1 if $l = 0$, and 0 otherwise.

A similar argument shows that more generally the crosscorrelation between sequences is given by

$$\theta_{y^{\lambda,j}, y^{\lambda',j'}}(l) = \delta_{\lambda,\lambda'} \delta_{j,j'+l}.$$

It is these relations that suggest that systems with Lebesgue spectrum may be useful for constructing sequences having the low auto- and crosscorrelations desirable in CDMA communications.

5 Making codes from periodic orbits

The zero crosscorrelation values of the $\{y_k^{\lambda,\,j}\}$ time series result when the limit $N \to \infty$ is taken. In practice of course the set of signals we seek to construct must consist of codewords of some finite length, say p. The sequences transmitted and received by (say) the communications system are strings of codewords concatenated together. A sequence made in this way from a single codeword will naturally be periodic, with period (at most) p. If the dynamical system ϕ is to generate such a sequence by evaluation of a measurement function y along an orbit, then (in the absence of special conditions on y) this will mean that the orbit must itself be periodic. Thus to generate codewords we shall arrange for x_0 to be a periodic point of ϕ, of period p. (That is, $x_p = \phi^p x_0 = x_0$.) It is clear that in that case

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} f_{\lambda,\,j}(x_k) f_{\lambda',\,j'}(x_k) = \frac{1}{p} \sum_{k=0}^{p-1} f_{\lambda,\,j}(x_k) f_{\lambda',\,j'}(x_k)$$

and it might seem that in view of (3) such a choice of orbit could be used to create codewords with the desired correlation properties. Unfortunately, we must recall that equality (3) is not true for *all* x_0, only for almost all. Often, the periodic points are among the points for which it does not hold. So now we must ask if the argument in the previous section is really any use to us, given that one of the steps in it (the use of (3)) is not justifiable for the orbit we have chosen. The reason for believing that it might still be of some relevance is that we will often be able to find, arbitrarily close to our starting x_0, another state x_0' for which the ergodic equality *does* hold. The trajectory of x_0' will initially lie close to that of x_0. If after p time steps x_0 and x_0' are still close together, and if the limit on the left hand side of equation (3) (with initial condition x_0') has been approached closely after p terms, then

$$\frac{1}{p} \sum_{k=0}^{p-1} f_{\lambda,\,j}(x_k) f_{\lambda',\,j'}(x_k) \approx < f_{\lambda,\,j}, f_{\lambda',\,j'} > .$$

In practice, this will mean that our periodic orbit will have to sample the invariant density sufficiently well—we cannot expect this to be possible if the orbit is not long enough.

Thus the scheme for generating codes is, in general terms, as follows. We identify a dynamical system with Lebesgue spectrum, and some suitable periodic orbit $\{x_0, x_1, \ldots, x_{p-1}\}$, where p is the desired length of the codewords. We then compute the (finite) sequences

$$\{f_{\lambda,\,j}(x_0), f_{\lambda,\,j}(x_1), \ldots f_{\lambda,\,j}(x_{p-1})\} \tag{7}$$

for each λ and j. Each such sequence is a codeword. Note that choosing $j \neq 1$ corresponds to a time shift of the $f_{\lambda,\,1}$ sequence—and so in this case gives a cyclic permutation of the $f_{\lambda,\,1}$ codeword.

6 Example: The Doubling Map

We have mentioned the doubling map several times already, and asserted that, when equipped with the ergodic invariant density $w(x) = 1$ it forms a system with Lebesgue spectrum, with the Walsh functions as a basis for L_2. Let us look at this in more detail.

We define the Walsh functions by

$$\begin{aligned} w_1(x) &\equiv 1 \\ w_{k+1}(x) &= \prod_{i=0}^{r-1} \mathrm{sgn}\{\sin^{k_i}(2^{i+1}\pi x)\}, \quad k = 1, 2, \ldots \end{aligned} \tag{8}$$

where the k_i's, (which are all either 0 or 1), are the binary digits of k; $k = \sum_{i=0}^{r-1} k_i 2^i$. (Sometimes slightly different definitions are used.) It is well known [4] that the Walsh functions form an orthonormal basis for L_2. So to show that the system has Lebesgue spectrum it is only necessary to show that property (6) holds. Let us begin this by showing that for every Walsh function $w_{k+1}(x)$ the composition $w_{k+1} \circ \phi(x)$ $(= w_{k+1}(\phi(x)))$ is another Walsh function.

According to the definition of the doubling map given earlier

$$w_{k+1}(\phi(x)) = \begin{cases} w_{k+1}(2x) & \text{if } 0 \le x < 1/2 \\ w_{k+1}(2x-1) & \text{if } 1/2 \le x \le 1. \end{cases}$$

Now if $0 \le x < 1/2$ then

$$\begin{aligned} w_{k+1}(2x) &= \prod_{i=0}^{r-1} \operatorname{sgn}\{\sin^{k_i}(2^{i+1}\pi 2x)\} \\ &= \prod_{i=0}^{r-1} \operatorname{sgn}\{\sin^{k_i}(2^{i+2}\pi x)\} \\ &= w_{2k+1}(x) \end{aligned}$$

and if $1/2 \le x \le 1$ then

$$\begin{aligned} w_{k+1}(2x-1) &= \prod_{i=0}^{r-1} \operatorname{sgn}\{\sin^{k_i}(2^{i+1}\pi(2x-1))\} \\ &= \prod_{i=0}^{r-1} \operatorname{sgn} \begin{cases} \sin^{k_i}(2^{i+1}\pi 2x)\cos^{k_i}(2^{i+1}\pi) \\ -\cos^{k_i}(2^{i+1}\pi 2x)\sin^{k_i}(2^{i+1}\pi) \end{cases} \\ &= \prod_{i=0}^{r-1} \operatorname{sgn}\{\sin^{k_i}(2^{i+1}\pi 2x)\} \\ &= w_{2k+1}(x). \end{aligned}$$

So generally $w_{k+1}(\phi(x)) = w_{2k+1}(x)$. We can arrange the Walsh functions in the following array

$$\begin{array}{cccc} w_2(x) & w_3(x) & w_5 & \dots \\ w_4(x) & w_7(x) & w_{13} & \dots \\ w_6(x) & w_{11}(x) & w_{21} & \dots \\ \vdots & \vdots & \vdots & \\ w_{2m}(x) & w_{4m-1}(x) & w_{8m-3} & \dots \\ \vdots & \vdots & \vdots & \end{array} \tag{9}$$

For each function in the array, the composition of the function with ϕ is the function to its right on the same row. Furthermore, every Walsh function must occur somewhere in the array. To see that this is so, consider the Walsh function $w_n(x)$. If n is even, this function occurs in the left hand column of the array. If it is odd, there is some integer k such that $n = 2k+1$, so now we consider the function with the lower index, $w_{k+1}(x)$. If $k+1$ is even, $w_{k+1}(x)$ lies in the first column, and so $w_n(x)$ lies in the second. If $k+1$ is odd, there is some k' such that $2k'+1 = k+1$, and we repeat the argument. It is clear that whatever n is, by reducing the index of the function in this way we must eventually

end up with a function with an even index, which hence lies in the first column, so that $w_n(x)$ lies somewhere to the right in the corresponding row. This argument not only shows that $w_n(x)$ occurs in the table, but also that it occurs only once. So the table exhibits the division of the Walsh function basis of L_2 into classes having the property (6), which is what we needed to establish that this system has Lebesgue spectrum. (The function w_1, the constant function, lives, as always, in a class on its own.)

Now that we know that the doubling map has the properties we are looking for, let us see what codes we can generate using it. In some respects this task is made simpler by the fact that, despite its nonlinearity, the doubling map has a very convenient representation. For any point x in the interval $[0, 1]$ there is a binary representation of x of the form $0.b_1b_2b_3\ldots$, where the b_i's are binary digits and $x = \sum_{i=1}^{\infty} \frac{b_i}{2^i}$. It is easy to see that mapping x with the doubling map ϕ gives a new point whose binary representation is $\phi(x) = 0.b_2b_3b_4\ldots$; that is, all the digits are shifted one place to the left, and the leftmost one is lost. In particular, if x is a periodic point with period p then the binary sequence representing x is periodic, $x = 0.b_1b_2b_3\ldots b_{p-1}b_pb_1b_2\ldots$. So to specify a *periodic* point, it is only necessary to specify the digit sequence $\{b_1b_2\ldots b_p\}$.

To make codewords, we must evaluate the Walsh functions at points along a periodic orbit. To begin with, we consider the functions w_{k+1} where k is a power of two (say 2^n). From the definition (8) we see that each of these is formed from a single factor $\mathrm{sgn}\{\sin(2^{n+1}\pi x)\}$; these particular functions are sometimes known as *Rademacher* functions. Note that they are the functions on the first row of (9). Let $0.b_1b_2b_3\ldots$ be the binary representation of x, then $2^{n+1}x = b_1b_2b_3\ldots b_nb_{n+1}.b_{n+2}b_{n+3}\ldots = m + r$, where $m = b_1b_2b_3\ldots b_{n+1}$ is an integer and $r = 0.b_{n+2}b_{n+3}\ldots$ lies between 0 and 1. Then

$$\sin(2^{n+1}\pi x) = \sin(m\pi + r\pi) = \cos(m\pi)\sin(r\pi).$$

Since $0 \leq r \leq 1$, $\sin(r\pi)$ is not negative, so the sign of $\sin(2^{n+1}\pi x)$ depends only on that of $\cos(m\pi)$: this will be positive if m is even, and negative if m is odd. From the binary representation of m, we see that m even corresponds to $b_{n+1} = 0$ and m odd corresponds to $b_{n+1} = 1$. These observations can be put succinctly by saying $w_{k+1}(x) = 1 - 2b_{n+1}$ when $k = 2^n$.

We are interested in the case where x is periodic. Recalling the shift property of the doubling map, it is clear that if $w_{k+1}(x) = 1 - 2b_{n+1}$ then $w_{k+1}(\phi x) = 1 - 2b_{n+2}$, $w_{k+1}(\phi^2 x) = 1 - 2b_{n+3}$ and so on. The codeword generated from w_{k+1} evaluated on the orbit of x is, from (7)

$$\{1 - 2b_{n+1}, 1 - 2b_{n+2}, 1 - 2b_{n+3}, \ldots, 1 - 2b_{n+p}\} \tag{10}$$

The digits involved in this codeword are a consecutive set of p digits from the binary representation of x, and so form some cyclic permutation of the digit sequence $\{b_1, b_2, \ldots, b_p\}$. The operation $b_i \to 1 - 2b_i$ is the usual conversion of a unipolar sequence to a bipolar one [6]; it will prove convenient to say $c_i = 1 - 2b_i$. All the Rademacher functions give codewords which are cyclic permutations of the same sequence, so there are at most p different codewords that can be made using these functions.

All the other Walsh functions are products of Rademacher functions. Suppose that w_{l+1} is the product of the two Rademacher functions w_{k+1} and $w_{k'+1}$, where $k = 2^n$ and $k' = 2^{n'}$. Then $w_{l+1}(x) = c_{n+1}c_{n'+1}$ and $w_{l+1}(\phi x) = c_{n+2}c_{n'+2}$, etc.. Thus to find the codeword generated by w_{l+1} we find the codewords generated by w_{k+1} and $w_{k'+1}$ and multiply together corresponding elements. It is clear that this generalises to any number of Rademacher functions: for any Walsh function we can find the codeword it generates

(from x) by decomposing it into Rademacher function factors, finding the codewords given by these factors from (10), and multiplying together all the corresponding elements.

These observations are sufficient to reveal quite a lot about the codes that can be generated using the doubling map. We can start by choosing any length p sequence of binary digits $\{b_1, b_2, b_3, \ldots, b_{p-1}, b_p\}$; then the x whose binary representation is $0.b_1b_2b_3 \ldots b_{p-1}b_pb_1b_2 \ldots$ is a periodic point of ϕ, with period at most p. Using w_2 we generate the codeword $\{1-2b_1, 1-2b_2, 1-2b_3, \ldots, 1-2b_p\}$, and cyclic permutations of this are generated using other Rademacher functions in the first row of (9). (Remember that functions in the same class generate codewords that are cyclic shifts of each other.) We can find a Walsh function that generates the (element by element) product of any selection of these codewords, by choosing the appropriate product of Rademacher functions. Further, as concluded in the previous paragraph, *any* Walsh function will give a codeword that can be expressed as such a product. So these products of $\{1-2b_1, 1-2b_2, 1-2b_3, \ldots, 1-2b_p\}$ and its cyclic shifts exhaust the codewords that we can generate.

There are one or two examples where it is easy to decide what the set of generated codewords looks like. Suppose we take an initial point x whose binary sequence is an m-sequence. Then the Rademacher functions give the cyclic shifts of the bipolar version of the same m-sequence. However, m-sequences have the well-known 'shift-and-add' property: the product of such a sequence with a cyclic shift of itself is another (different) cyclic shift of the same sequence [1]. In this case using Walsh functions other than the Rademacher functions does not yield any new codewords. The totality of codewords we can generate consists simply of the original sequence and its cyclic shifts.

A rather different example is provided by the Gold sequences. If u and v are a *preferred pair* of m-sequences (see [1] for a definition) then the Gold sequences generated by u and v are the products of u with the cyclic shifts of v, together with u and v themselves. (We are taking u and v to be bipolar sequences.) Given any one of these codewords, except u or v, it turns out that we can generate all the others by forming products whose factors are suitably chosen cyclic shifts of the given codeword. (To see this, let $u \otimes v$ be the sequence formed from the element by element multiplication of u and v, and let $T^j v$ be the sequence obtained from v by a cyclic shift of j places to the left. Then the Gold sequences are

$$\{u, v, u \otimes v, u \otimes Tv, u \otimes T^2v, \ldots, u \otimes T^{N-1}v\}$$

where N is the length of the sequences. If we take, for example, $u \otimes v$ and form its product with $T^i(u \otimes v)$ we have

$$\begin{aligned}(u \otimes v) \otimes T^i(u \otimes v) &= (u \otimes v) \otimes (T^i u \otimes T^i v) \\ &= (u \otimes T^i u) \otimes (v \otimes T^i v) \\ &= (T^j u \otimes T^k v)\end{aligned}$$

for some j and k, where we have used the shift-and-add properties of u and v. $T^j u \otimes T^k v$ is clearly a shift of $u \otimes T^{k-j} v$, which is another of the Gold sequences whenever $k \neq j$. To generate u and v we need to take products with three factors. Similar remarks clearly apply to Gold sequences other than $u \otimes v$.)

As we have seen, we can generate these products of shifted codewords by evaluating Walsh functions that are the corresponding products of Rademacher functions. Hence, if our initial condition x has as its binary sequence one of the codewords (other than u or v), evaluating all the Walsh functions will generate the whole Gold code (and its shifts). And since products of Gold sequences with (shifts of) other Gold sequences produce only other sequences in the set, it is clear that making sequences by evaluating Walsh functions does not generate any sequences which are not part of the Gold code.

7 Conclusions

Despite the apparent abstractness of the ergodic theory that leads to the scheme for generating codes, the scheme itself is quite simple, at least in its general principles. Once we have identified a system with Lebesgue spectrum (and we might expect normally to use standard examples from ergodic theory), all we need to do is evaluate functions on a suitable periodic orbit of the system. The examples of the last section, though very simple, do demonstrate that the procedure can generate codes known to have good correlation properties. The most important open question is how to choose an appropriate periodic orbit. The doubling map example illustrates the strong dependence the resulting code can have on the choice of this orbit. We know that the orbit must sample the invariant density sufficiently well; but how well, and where it has to go to do this, depend on the functions whose integrals we want to approximate. We found above that the choice of an m-sequence—which at first sight we might have imagined would sample the constant density on the unit interval rather well—does not lead to the generation of many different codewords. This is reflected in the fact that the orbit based on the m-sequence conspires with the Walsh function basis to produce some very bad estimates for some of the integrals we are interested in. How to choose a good orbit in a particular system, and whether this is easier in some systems than others, are questions needing further investigation.

There are other questions of a more general nature. Although we have tried to construct codes with good auto- and crosscorrelation properties, it is not clear, given a particular system, how good these properties will be. At the moment we can only assess this after generating the code. (Actually, this question is closely bound up with that of the choice of orbit.) But then, of course, the correlation properties of the code are not the sole determinants of its suitability in any particular application, so even codes with known correlations will still have to be tested, usually by simulations. Even in a given application, such as CDMA for cellular telephones, the performance of the code depends on the particular conditions in which it is used.

An interesting possibility is that of using non-binary codes. Several of the systems with Lebesgue spectrum that were mentioned above have real or complex valued, as opposed to integer valued, functions in their L_2 bases. These generate codewords of real or complex numbers rather than binary digits—the cat map is a good illustration. Codes of this kind could be used in at least some applications; whether or not they would be more useful than binary codes in such cases is an open problem.

References

[1] D. V. Sarwate and M. B. Pursley. Crosscorrelation properties of pseudorandom and related sequences. *Proc. IEEE* **68** (1980) 593-619

[2] J.-S. No and P. V. Kumar. A new family of binary pseudorandom sequences having optimal periodic correlation properties and larger linear span. *IEEE Trans. Info. Theory* **35** (1989) 371-379

[3] T. Kohda and A. Tsuneda. Pseudonoise sequences by chaotic nonlinear maps and their correlation properties. *IEICE Trans. Communications* **E76-B** (1993) 855-862

[4] J. R. Higgins. *Completeness and Basis Properties of Sets of Special Functions*, Cambridge University Press, Cambridge, 1977.

[5] V. I. Arnold and A. Avez. *Ergodic Problems of Classical Mechanics*, W. A. Benjamin Inc., New York, 1968.

[6] R. L. Pickholtz, D. L. Schilling and L. B. Milstein. Theory of spread spectrum communications. *IEEE Trans. Communications* **30** (1982) 855-884