ABSOLUTE TYPE SHAFT ENCODING USING LFSR SEQUENCES WITH PRESCRIBED LENGTH

J.M. FUERTES, B. BALLE AND E. VENTURA

Abstract. Maximal-length binary sequences have been known for a long time. They have many interesting properties, one of them is that when taken in blocks of n consecutive positions they form $2^n - 1$ different codes in a closed circular sequence. This property can be used for measuring absolute angular positions as the circle can be divided in as many parts as different codes can be retrieved. This paper describes how can a closed binary sequence with arbitrary length be effectively designed with the minimal possible block-length, using *linear feedback shift registers* (LFSR). Such sequences can be used for measuring a specified exact number of angular positions, using the minimal possible number of sensors that linear methods allow.

1. Introduction

Angular absolute position measurement is carried out by transducers that expand a different n-bit code word for each of a finite number of angular positions. One of the common components of such transducers is a marked disk with as many sectors as different angular positions are to be sensed.

Traditional disks use a radial bit sensing method that consists in an arrangement of blacks and whites ("1" and "0") distributed in concentric coronas. Most commercial transducers use the Gray coding bit distribution to reduce the different scanning errors. But such coding has two drawbacks: as the resolution (and so the number of bits) increases, the disk diameter must also increase; and secondly, the number of sectors has to be exactly a power of 2.

For the first drawback, there is a method that uses only one bit code track, based on the window property of pseudo-random binary sequences. Such property states that in a pseudo-random cyclic code expansion, all the n-bit elements that can be successively taken are different to each other. The result is that once the pseudo-random binary sequence is expanded in the circular corona, there are as many different measurements as the length of the cyclic code expansion. In this case, the sensing elements are not radially but tangentially distributed. There are several papers stating such configuration, see [1], [8], [9] and [10].

Next question is about the number of sectors. We need to produce a pseudo-random cyclic code expansion, all of whose n-bit subwords are different to each other, and having a prescribed length $e \geqslant 2$. An obvious restriction is $2 \leqslant e \leqslant 2^n$. In [4] and using graph theory, A. Lempel proved that such sequences always exist, only under the hypothesis $2 \leqslant e \leqslant 2^n$. The problem is how to explicitly construct them with a fast algorithm (not essentially based on a full search among all exponentially many possibilities).

It is well known that, with a window of n sensing bits and using linear feedback shift registers with *connection polynomial* of degree n, the maximal length can be obtained, that is, one can produce cyclic binary sequences of length 2^n-1 such that all windows of n consecutive bits are different to each other (see [6] and [2]). In [8] the author introduces a truncation of these maximal length sequences in order to obtain the desired exact number of sectors (not necessarily being a power of 2). To detect the truncation point it was proposed to include an additional corona where an additional bit shows the discontinuity and allows the correct recovery of the measure in the area of such discontinuity.

Another approach to solve this problem is to try to generate (non-maximal) feedback shift registers expanding circular sequences of a previously given length e (from an appropriate initial *seed*). Although less studied in the literature, this is also possible i.e., there always exist such (non-necessarily linear) feedback shift registers (see [2] and [12] for the binary case, and [4] for a generalization to m-ary sequences).

In this paper, we consider again this problem and we provide another solution having the following two additional advantages. We present an algorithm such that, given a natural number $e \geqslant 2$, it produces a *linear* feedback shift register with connection polynomial of the *smallest* possible degree, and a seed, expanding a circular sequence of length exactly e. In general, the fact of being *linear* makes it easier to implement in hardware. And the fact that the output is a circular sequence of length e expanded by a linear feedback shift register of the *smallest* possible degree ensures us that we are going to use the smallest possible number of sensors. Finally, the algorithm is fast for the typical values of e that can be useful in particular applications. The techniques and arguments used here are inspired on those contained in [11].

We point out that, with the techniques in this paper, we minimize the number of sensors needed, among all possible *linear* feedback shift registers expanding circular sequences of a prefixed length. It is not clear how to systematically achieve the absolute minimum among non necessarily linear ones. In Section 5 we show an example where these two minimums do not agree.

The structure of the paper is as follows. Section 2 contains the preliminaries needed about linear feedback shift registers, and about polynomials over finite fields, stating the notation that will be used along the paper. Section 3 is the central part of the article, where we discuss the cyclic structure of polynomials, and we construct and justify the algorithm. Then, in Section 4, we make the algorithm explicit and particularized to the binary case. Finally, we develop an example and write down the conclusions.

We point out to the reader that (although for the engineering applications one will only make use of the results here particularized to the binary case), we do all the discussions in an arbitrary finite field $\mathbb{F}_q$, (with $q = p^m$, and p being a prime number). The reason for working with more generality than the one strictly needed for the applications, is that the arguments given are general and work exactly in the same manner for the binary field $\mathbb{F}_2$ than for an arbitrary $\mathbb{F}_q$. At any time the reader can particularize any result to the binary case by just declaring everywhere $p = q = 2$ and $m = 1$.

2. Preliminaries

2.1. **Focusing the problem.** Linear feedback shift registers are well known electronic digital circuits used to expand periodic sequences over finite fields (over $\mathbb{F}_2$ for binary sequences). See [2] or [7] for generalities about them.

For the rest of the paper, let p be a prime number, $q = p^m$, and $\mathbb{F}_q$ be the field with q elements (which has characteristic p). As pointed out in the introduction, read $p = q = 2$ (and $m = 1$) for a binary version of this article.

Let $n \geqslant 1$ be a natural number and let $a(x) = -(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) + x^n \in \mathbb{F}_q[X]$ be a monic polynomial of degree n over $\mathbb{F}_q$ with $a(0) = -a_0 \neq 0$. Consider the $n \times n$ invertible matrix

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & a_{n-2} \\ 0 & 0 & \cdots & 1 & a_{n-1} \end{pmatrix} \in GL_n(\mathbb{F}_q),$$

usually called the *companion* matrix of $a(x)$. It is well known that the characteristic polynomial of M is $a(x)$; in particular, $a(M) = 0$. Take now an arbitrary column vector, $u = (u_0, u_1, \ldots, u_{n-1})^T \in \mathbb{F}_q^n$, let u^T be the same vector but written as a row, and let us consider the sequences of

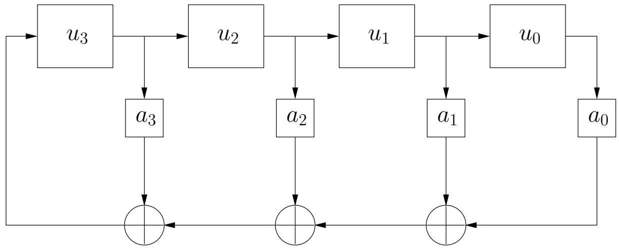

FIGURE 1. LFSR with Fibonacci architecture

vectors $M^i u$ and $u^T M^i$, $i = 0, 1, 2, \ldots$. First of all, since the set $\mathbb{F}_q^n$ is finite, there must be eventual repetitions, say $M^i u = M^j u$ for $i < j$. And, since M is invertible, we have $u = M^{j-i}u$, meaning that the first repetition is always against the very first vector u. In other words, the sequence $M^i u$ (and similarly $u^T M^i$), $i = 0, 1, 2, \ldots$, is *periodic*.

Note that, by the special shape of M, the vector $u^T M^{i+1}$ is the same as the vector $u^T M^i$ with all the coordinates shifted one position to the left (so, loosing the first coordinate), and with the last coordinate computed according to the last column of M. Thus, out of M and u, we can clockwise produce a circular sequence of e elements of $\mathbb{F}_q$ in such a way that the e consecutive n-tuples readable from it are pairwise different, where e is the period of the sequence $u^T M^i$. The generation of such circular sequence is typically carried out by the standard electronic device called *linear feedback shift register* (LFSR for short) with *connection polynomial* $a(x)$, with *seed* u, and with the so-called Fibonacci architecture, see Fig. 1 (where "linear" stands for the linearity of the computation of the last coordinate in terms of the n previous ones). In this terms, the problem addressed in the present paper is the following.

Problem 2.1. *Given a natural number $e \geqslant 2$, construct a LFSR (i.e. a monic $a(x) \in \mathbb{F}_q[X]$) with connection polynomial of the* smallest *possible degree, say n, and a seed $u \in \mathbb{F}_q^n$ such that the sequence $u^T M^i$ has period precisely e.*

Let us reinterpret the problem in terms of the sequence $M^i u$, typically the one expanded by the same LFSR with the same seed, but now with the Galois architecture, see Fig. 2. Identifying $u = (u_0, u_1, \ldots, u_{n-1})^T$ with the polynomial $u(x) = u_0 + u_1 x + \cdots + u_{n-1}x^{n-1} \in \mathbb{F}_q[X]$, it is straightforward to verify that Mu is the polynomial $u(x)x \mod a(x)$. So, the sequence $M^i u$ is the reduction of the sequence of polynomials $u(x)x^i$, modulo $a(x)$. Thus, the period of $M^i u$ is the minimum $j \geqslant 1$ such that $u(x)x^j \equiv u(x)$

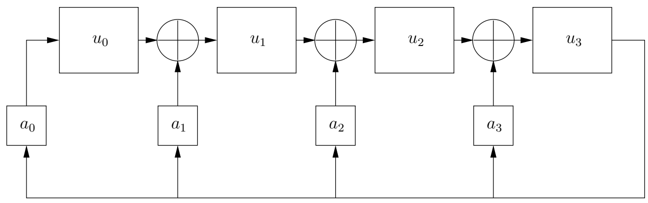

FIGURE 2. LFSR with Galois architecture

mod $a(x)$. This number will be called the *cyclic length of* $u(x)$ *modulo* $a(x)$, and will be closely studied below.

The relation between Problem 2.1 and cyclic lengths modulo polynomials is not immediately obvious since, in general, the sequences $u^T M^i$ and $M^i u$ do not always have the same period. For example, in the binary case consider $a(x) = 1 + x + x^2 + x^3 + x^4 + x^5$ and $u = (0, 1, 1, 0, 1)^T$; $u^T M^i$ has period 3 while $M^i u$ has period 6. However, the following lemma (applied to companion matrices) allows us to restate Problem 2.1 in terms of cyclic lengths.

Lemma 2.2. *Let M be a $n \times n$ matrix over $\mathbb{F}_q$. Then, the set of periods of $u^T M^i$ coincides with that of $M^i u$, while u ranges over all column vectors in $\mathbb{F}_q^n$. Furthermore, for every $P \in GL_n(\mathbb{F}_q)$ such that $PMP^{-1} = M^T$, the map $u \mapsto Pu$ is a bijection of $\mathbb{F}_q^n$* preserving *the period (i.e., $M^i u$ and $(Pu)^T M^i$ have the same period).*

Proof. The first assertion is clearly a consequence of the second one, since it is well-known that M and M^T are always similar matrices (i.e. there does exist $P \in GL_n(\mathbb{F}_q)$ such that $PMP^{-1} = M^T$). For every such matrix P and every integer r we have $PM^r = (M^T)^r P$. Now, for every column vector u, the equation $u = M^r u$ is equivalent to $Pu = PM^r u = (M^T)^r Pu$ and so, to $(Pu)^T = (Pu)^T M^r$. Hence, the periods of the sequences $M^i u$ and $(Pu)^T M^i$ do coincide.

For later use, let us find an easy way of computing such a matrix P, in the case where M is the companion matrix of a monic polynomial $a(x) = -(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) + x^n \in \mathbb{F}_q[X]$. We shall built a matrix P with the upper left triangle full of zeroes, with the contra-diagonal full of ones (and so, invertible) and with each one of the consecutive sub-contra-diagonals having constant values (so, P will be symmetric). One can recursively fill the entries of such a P if we impose the additional condition that PM is also symmetric (note that PM coincides with P removing its first column and adding a last column equal to Pa, where a is the last column of M). This way, we have an invertible matrix P such that both P and PM are symmetric. This P is good enough for our purposes, since $PM = (PM)^T = M^T P^T = M^T P$. $\square$

In view of Lemma 2.2, solving Problem 2.1 reduces to finding a monic polynomial $a(x) \in \mathbb{F}_q[X]$ of the smallest possible degree, and a column vector $u \in \mathbb{F}_q^n$, with prescribed cyclic length for $u(x)$ modulo $a(x)$. In fact, Lemma 2.2 tells that, the same $a(x)$ and an easily computable vector $v = Pu$ solves Problem 2.1. This way, our main goal reduces to solving the following problem, which is completely stated in the language of polynomials over finite fields.

Problem 2.3. *Given a natural number $e \geqslant 2$, construct a monic polynomial $a(x) \in \mathbb{F}_q[X]$ of the* smallest *possible degree, say n, and a seed $u(x) \in \mathbb{F}_q[X]$ (being a polynomial of degree smaller than n), such that the cyclic length of $u(x)$ modulo $a(x)$ is precisely e.*

2.2. **Polynomials over finite fields.** Let us dedicate this section to summarize the elementary facts about polynomials over finite fields that will be needed later.

Let $a(x) \in \mathbb{F}_q[X]$ be a polynomial of degree n and satisfying $a(0) \neq 0$. The ring $\mathbb{F}_q[X]/a(x)\mathbb{F}_q[X]$ contains $q^n - 1$ non-zero elements and so there must be two integers $0 \leqslant s_1 < s_2 \leqslant q^n - 1$ such that $x^{s_1} \equiv x^{s_2}$ modulo $a(x)$. That is, $a(x)$ divides $x^{s_2} - x^{s_1} = x^{s_1}(x^{s_2 - s_1} - 1)$. The fact $a(0) \neq 0$ implies that $a(x)$ also divides $x^{s_2 - s_1} - 1$. It is standard to define the *order* of $a(x)$, denoted $\mathrm{ord}(a(x))$, as the minimum positive integer e such that $a(x)$ divides $x^e - 1$. In general, $\mathrm{ord}(a(x)) \leqslant q^n - 1$. In other words, the order of a given polynomial $a(x) \in \mathbb{F}_q[X]$ is the minimum positive integer e such that $1 \cdot x^e \equiv 1$ modulo $a(x)$. This is, precisely, the cyclic length of 1 modulo $a(x)$.

The following are well-known facts concerning polynomials over finite fields:

- (I) (3.4 in [5]) The order of an irreducible polynomial $a(x) \in \mathbb{F}_q[X]$ with $a(0) \neq 0$ and degree n is always a divisor of $q^n - 1$. In particular, it is not multiple of p.
- (II) (3.6 in [5]) $\gcd(x^r - 1,\, x^s - 1) = x^{\gcd(r,s)} - 1$. Furthermore, an arbitrary polynomial $a(x) \in \mathbb{F}_q[X]$ with $a(0) \neq 0$, divides $x^s - 1$ if and only if $\mathrm{ord}(a(x))$ divides s.

We also quote the following well known result in finite field theory. Recall that, given two coprime integers $a, b \geqslant 2$, one is invertible modulo the other and so it makes sense to define the *order of a modulo b*, denoted $\mathrm{ord}_b(a)$, being the smallest $i \geqslant 1$ such that $a^i \equiv 1 \mod b$.

Theorem 2.4 (3.5 in [5])**.** *Let $e \geqslant 2$ be an integer. Then, there exist irreducible polynomials in $\mathbb{F}_q[X]$ having order e. Furthermore, all of them have the same degree, namely* $\mathrm{ord}_e(q)$. □

A possible method for finding such a polynomial is the following. It has to be a divisor of $x^e - 1$, but not a divisor of $x^d - 1$ for every $d\,|e$, $d \neq e$. So, computing $(x^e - 1)/\,\mathrm{lcm}_{d|e,\, d\neq e}\{x^d - 1\}$ and finding an irreducible factor will be enough (note that, by Theorem 2.4, all such irreducible factors have the same degree, $\mathrm{ord}_e(q)$).

Now, we need the following two lemmas for better understanding of the order of polynomials. We introduce the following notation. Given the prime number p and a positive integer s, we define $\lceil s \rceil_p$ to be the smallest positive integer h such that p^h is not less that s (we will write $\lceil s \rceil$ if there is no risk of confusion). That is, $\lceil 1 \rceil = 0$ and $p^{\lceil s \rceil - 1} < s \leqslant p^{\lceil s \rceil}$ for $s \geqslant 2$.

Lemma 2.5 (3.8 in [5])**.** *Let $a(x) \in \mathbb{F}_q[X]$ be an irreducible polynomial with $a(0) \neq 0$ and order e. Then,* $\mathrm{ord}(a(x)^s) = ep^{\lceil s \rceil}$. □

Lemma 2.6 (3.9 in [5])**.** *Let $a_1(x), \ldots, a_r(x) \in \mathbb{F}_q[X]$ be pairwise coprime polynomials such that $a_i(0) \neq 0$, and let $e_i = \mathrm{ord}(a_i(x))$, $i = 1, \ldots, r$. Then,* $\mathrm{ord}(a_1(x) \cdots a_r(x)) = \mathrm{lcm}\{e_1, \ldots, e_r\}$. □

Finally, the following technical lemma will also be used.

Lemma 2.7. *Let a, b, $q \geqslant 2$ be three integers, a and b coprime with q. Then,*

$$\mathrm{ord}_{\mathrm{lcm}\{a,\, b\}}(q) = \mathrm{lcm}\{\mathrm{ord}_a(q),\, \mathrm{ord}_b(q)\}.$$

In particular,

(i) *if a divides b then* $\mathrm{ord}_a(q)$ *divides* $\mathrm{ord}_b(q)$,

(ii) *if a and b are coprime then* $\mathrm{ord}_{ab}(q) = \mathrm{lcm}\{\mathrm{ord}_a(q),\, \mathrm{ord}_b(q)\}$.

Proof. Let us denote by e_a, e_b and $e_{a,b}$ the orders of q modulo a, b and $\mathrm{lcm}\{a, b\}$, respectively. By definition, a divides $q^{e_a} - 1$, and b divides $q^{e_b} - 1$. So, $\mathrm{lcm}\{a, b\}$ divides $\mathrm{lcm}\{q^{e_a} - 1,\, q^{e_b} - 1\} = q^{\mathrm{lcm}\{e_a, e_b\}} - 1$ and thus, $e_{a,b}$ divides $\mathrm{lcm}\{e_a, e_b\}$ (here, we use fact (II) above). On the other hand, a divides $\mathrm{lcm}\{a, b\}$, which divides $q^{e_{a,b}} - 1$. So, e_a divides $e_{a,b}$. Similarly, e_b divides $e_{a,b}$ and hence $\mathrm{lcm}\{e_a, e_b\}$ also divides $e_{a,b}$. This shows that $\mathrm{ord}_{\mathrm{lcm}\{a,b\}}(q) = e_{a,b} = \mathrm{lcm}\{e_a, e_b\} = \mathrm{lcm}\{\mathrm{ord}_a(q), \mathrm{ord}_b(q)\}$. The statements (i) and (ii) are particular cases. □

3. The construction

As stated in the previous section, our main goal is to solve Problem 2.3. For this purpose, given a polynomial $a(x) \in \mathbb{F}_q[X]$, we have to understand which numbers occur as cyclic length of some seed $u(x)$ modulo $a(x)$. The finite set of all those possible numbers is named *cyclic structure of* $a(x)$, and denoted $\mathcal{CS}(a(x))$. In other words, $\mathcal{CS}(a(x))$ is the finite set of positive integers whose members are precisely the cyclic lengths of all polynomials $u(x)$ (of degree less than that of $a(x)$) modulo $a(x)$. We describe this set in the following two propositions.

Proposition 3.1. *Let $a(x) \in \mathbb{F}_q[X]$, $a(x) \neq x$, be a monic irreducible polynomial of order e. Then, the cycle structure of $a(x)^s$ is $\mathcal{CS}(a(x)^s) = \{1, e, ep, \ldots, ep^{\lceil s \rceil}\}$.*

Proof. Taking $u(x) = 0$ we see that $1 \in \mathcal{CS}(a(x)^s)$. Let $0 \neq u(x) \in \mathbb{F}_q[X]$ be a polynomial of degree less than that of $a(x)^s$, and denote by $k \geqslant 1$ its cyclic length modulo $a(x)^s$. That is, k is the smallest positive integer such that $u(x)x^k \equiv u(x)$ modulo $a(x)^s$ or, in other words, the smallest positive integer such that $a(x)^s$ divides $u(x)(x^k - 1)$. Write $u(x) = u'(x)a(x)^d$ for some $0 \leqslant d < s$ and some $u'(x) \in \mathbb{F}_q[X]$ coprime to $a(x)$. The previous assertion is now equivalent to say that k is the smallest positive integer such that $a(x)^{s-d}$ divides $x^k - 1$, that is, k is the order of $a(x)^{s-d}$. Using Lemma 2.5, this proves that $k = \mathrm{ord}(a(x)^i) = ep^j$ for some $i = 1, \ldots, s$ and some $j = 0, \ldots, \lceil s \rceil$. Furthermore, it is clear that every number of the form ep^j for $j = 0, \ldots, \lceil s \rceil$ occur in $\mathcal{CS}(a(x)^s)$, for example as the cyclic length of $u(x) = a(x)^{s-(p^{j-1}+1)}$ (which makes sense because $j \leqslant \lceil s \rceil$ implies $p^{j-1} + 1 \leqslant p^{\lceil s \rceil - 1} + 1 \leqslant s$; here, we understand $p^{-1} = 0$). □

Proposition 3.2. *Let $a(x) \in \mathbb{F}_q[X]$, be a monic polynomial with $a(0) \neq 0$, and consider its decomposition into different irreducible factors, $a(x) = a_1(x)^{s_1} a_2(x)^{s_2} \cdots a_r(x)^{s_r}$, with increasing exponents, $s_1 \leqslant s_2 \leqslant \cdots \leqslant s_r$. Let $e_i = \mathrm{ord}(a_i(x))$, for $i \in I = \{1, \ldots, r\}$. Then, the cycle structure of $a(x)$ is given by*

$$\mathcal{CS}(a(x)) = \{1\} \cup \{\big(\mathrm{lcm}_{i \in J}\{e_i\}\big)p^t \mid \emptyset \neq J \subseteq I, \\ 0 \leqslant t \leqslant \lceil s_j \rceil,\ \ j = \max J\}.$$

Proof. Taking $u(x) = 0$ we see that $1 \in \mathcal{CS}(a(x))$. Let $u(x) \in \mathbb{F}_q[X]$ be a polynomial of degree less than that of $a(x)$ and cyclic length $k \geqslant 2$ modulo $a(x)$. Denote by k_i the cyclic length of $u(x)$ modulo $a_i(x)^{s_i}$, $i \in I$. That is, k is the smallest positive integer such that $a(x)$ divides $u(x)(x^k - 1)$ and, for every $i \in I$, k_i is the smallest positive integer such that $a_i(x)^{s_i}$ divides $u(x)(x^{k_i} - 1)$. In this situation, it is straightforward to verify that $k = \mathrm{lcm}_{i \in I}\{k_i\}$. Note that, by Proposition 3.1, either $k_i = 1$ or $k_i = e_i p^j$ for some $j = 0, \ldots, \lceil s_i \rceil$, and observe also that, by assumption, $J = \{i \in I \mid k_i \neq 1\} \neq \emptyset$. Then, $k = \mathrm{lcm}_{i \in J}\{k_i\} = \big(\mathrm{lcm}_{i \in J}\{e_i\}\big)p^t$, where $0 \leqslant t \leqslant \lceil s_j \rceil$ and $j = \max J$. Conversely, any positive number of the form $\big(\mathrm{lcm}_{i \in J}\{e_i\}\big)p^t$

with $\emptyset \neq J \subseteq I$, $0 \leqslant t \leqslant \lceil s_j \rceil$ and $j = \max J$, appears in $\mathcal{CS}(a(x))$. In fact, it does as the cyclic length of $u(x) = \big(\prod_{i \in J \setminus \{j\}} a_i(x)^{s_i - 1}\big) \cdot a_j(x)^{s_j - (p^{t-1}+1)} \cdot \big(\prod_{i \notin J} a_i(x)^{s_i}\big)$ modulo $a(x)$ (which makes sense because $t \leqslant \lceil s_j \rceil$ implies $p^{t-1} + 1 \leqslant p^{\lceil s_j \rceil - 1} + 1 \leqslant s_j$; here, we understand $p^{-1} = 0$). □

As an immediate corollary of Proposition 3.2, one can already say that every positive integer occurs as the cyclic length of some polynomial modulo some other. That is, given an exact length, there always exists a linear feedback shift register that expands, with an appropriate seed, a circular sequence of the given required length. The problem now is how to construct one of them (LFSR and seed, i.e. $a(x)$ and $u(x)$) with the minimal possible degree for $a(x)$.

Corollary 3.3. *For every integer $e \geqslant 1$ there exist two polynomials $a(x)$, $u(x) \in \mathbb{F}_q[X]$ such that the cyclic length of $u(x)$ modulo $a(x)$ is precisely e.* □

In order to attack Problem 2.3, we shall make several reductions to simpler ones. Let $a(x) \in \mathbb{F}_q[X]$ be a polynomial with $a(0) \neq 0$, and consider its factorization into different irreducible factors, $a(x) = a_1(x)^{s_1} a_2(x)^{s_2} \cdots a_r(x)^{s_r}$, with increasing exponents $s_1 \leqslant s_2 \leqslant \cdots \leqslant s_r$. Let $e_i = \mathrm{ord}(a_i(x))$, for $i \in I = \{1, \ldots, r\}$.

Lemma 3.4. *With the previous notation, assume $s_r \geqslant 2$ and consider the polynomial $a'(x) = \mathrm{lcm}\{a_1(x) \cdots a_r(x), (x-1)^{s_{r+1}}\}$, where $s_{r+1} = p^{\lceil s_r \rceil - 1} + 1$ is the smallest integer such that $\lceil s_{r+1} \rceil = \lceil s_r \rceil$ (that is, $a_1(x) \cdots a_r(x)(x-1)^{s_{r+1}}$ if $x-1$ was not present in the decomposition of $a(x)$, and $a(x)$ changing all the exponents to 1 except that of $x-1$ to s_{r+1}, otherwise). Then, $\mathcal{CS}(a'(x)) = \mathcal{CS}(a(x))$ and $deg(a'(x)) \leqslant deg(a(x))$.*

Proof. By Proposition 3.2, we have $\mathcal{CS}(a(x)) = \{1\} \cup \{\big(\mathrm{lcm}_{i \in J}\{e_i\}\big) p^t \mid \emptyset \neq J \subseteq I,\ 0 \leqslant t \leqslant \lceil s_j \rceil,\ j = \max J\}$. Also, since the order of $x-1$ is $e_{r+1} = 1$ and $\lceil s_{r+1} \rceil = \lceil s_r \rceil$, we have $\mathcal{CS}(a'(x)) = \mathcal{CS}(a(x))$. The inequality between degrees follows straightforward from the construction of $a'(x)$ and the hypothesis $s_r \geqslant 2$. □

So, in order to solve Problem 2.3, it is enough to consider polynomials whose decomposition into irreducible factors have all the exponents being 1 except, maybe, that of $x-1$.

Consider now such a polynomial, $a(x) = a_*(x)(x-1)^{s_{r+1}}$, where $s_{r+1} \geqslant 0$, $a_*(x) = a_1(x) \cdots a_r(x)$, and $a_1(x), \ldots, a_r(x), (x-1), x$ are pairwise different irreducible polynomials. Since $a_*(x)$ has no multiplicities and, by fact (I) in the previous section, $e_i = \mathrm{ord}(a_i(x))$ is not divisible by p, Proposition 3.2 above tells us that the members of $\mathcal{CS}(a_*(x))$ are also not divisible by p. Again by Proposition 3.2, the unique contribution of the factor $x-1$ to the cyclic structure of $a(x)$ is to add some bounded powers of p as extra factors at the numbers in $\mathcal{CS}(a_*(x))$, which were coprime to p. Hence, Problem 2.3 reduces to the case where e is not multiple of p, and searching only among polynomials without multiplicities and not being multiples of $x-1$ (by then adding the factor $(x-1)^{p^{s-1}+1}$ to gain a possible extra p^s in the factorization of e, $s \geqslant 1$).

With the following obvious lemma, we can do a further reduction.

Lemma 3.5. *Let $a(x) = a_1(x) \cdots a_r(x)$, where $a_1(x), \ldots, a_r(x), x-1, x$ are pairwise different irreducible polynomials. Let $e_i = \mathrm{ord}(a_i(x))$, $i \in I = \{1, \ldots, r\}$ and, for every subset $\emptyset \neq J \subseteq I$, consider $a'(x) = \Pi_{i\in J}\, a_i(x)$. Then, $\mathrm{lcm}_{i\in J}\{e_i\} \in \mathcal{CS}(a'(x))$ and deg$(a'(x)) \leqslant$ deg$(a(x))$.* □

So, according to the description given in Proposition 3.2, we can also think that the unique relevant contribution of a polynomial $a(x) = a_1(x) \cdots a_r(x)$ to the set $\mathcal{CS}(a(x))$ is given by the maximal set of indices $J = I$ (being the other ones also obtainable in cyclic structures of polynomials of smaller degree). In this case, since the $a_i(x)$'s are coprime to each other, Lemma 2.6 tells us that

$$\begin{aligned}\mathrm{lcm}_{i\in I}\{e_i\} = \mathrm{lcm}_{i\in I}\{\mathrm{ord}(a_i(x))\} &= \mathrm{ord}(\Pi_{i\in I}\, a_i(x)) \\ &= \mathrm{ord}(a(x)).\end{aligned}$$

In other words, for solving Problem 2.3, the unique relevant entry in $\mathcal{CS}(a(x))$ is the number $\mathrm{ord}(a(x))$. And, having computed a polynomial $a(x) \in \mathbb{F}_q[X]$ with a given order $\mathrm{ord}(a(x)) = e \geqslant 2$, we have by definition that e is the smallest exponent $i \geqslant 1$ such that $x^i \equiv 1 \mod a(x)$. Hence, the seed $u(x) = 1$ has cyclic length modulo $a(x)$ precisely equal to e, and degree less than that of $a(x)$. So, problem 2.3 reduces to

Problem 3.6. *Given a natural number $e \geqslant 2$ not multiple of p, construct a polynomial $a(x) \in \mathbb{F}_q[X]$ with $a(0) \neq 0$ and of the smallest possible degree (and so, without multiplicities and not being multiple of $x-1$) such that $\mathrm{ord}(a(x)) = e$.*

This is now a problem completely formulated in the area of finite fields. In general, given a natural number $e \geqslant 2$, there are several polynomials of order e, with several degrees. Theorem 2.4 tells us explicitly which is the degree of those being irreducible. However, irreducible polynomials are not always the ones having the smallest possible degree among those of a given order (at the example worked out in Section 5, a binary polynomial of order 45 and degree 10 is shown, while the irreducible polynomials of order 45 all have degree $\mathrm{ord}_{45}(2) = 12$). So, a more detailed search among polynomials of a given order is needed.

Let $e \geqslant 2$ be a natural number not multiple of p, and consider the irreducible factorization, $a(x) = a_1(x) \cdots a_r(x)$, of a possible solution $a(x) \in \mathbb{F}_q[X]$ to the Problem 3.6, $a_i(x) \neq x$. Writing $e_i = \operatorname{ord}(a_i(x))$ and $n_i = \deg(a_i(x))$, $i \in I = \{1, \dots, r\}$, and using Lemma 2.6 and Theorem 2.4, we have

$$e = \operatorname{ord}(a(x)) = \operatorname{ord}(a_1(x) \cdots a_r(x)) = \operatorname{lcm}\{e_1, \dots, e_r\},$$

$$n = \deg(a(x)) = n_1 + \cdots + n_r = \operatorname{ord}_{e_1}(q) + \cdots + \operatorname{ord}_{e_r}(q).$$

So, we can find $a(x)$ by listing all the expressions of the form $e = \operatorname{lcm}\{e_1, \dots, e_r\}$, $e_i \geqslant 2$, and for each of them computing $\operatorname{ord}_{e_1}(q) + \cdots + \operatorname{ord}_{e_r}(q)$. When the minimal possible value of this sum is obtained, we make use of the constructive comment after Theorem 2.4 to obtain irreducible polynomials $a_1(x), \dots, a_r(x)$ of orders $e_1, \dots, e_r$, respectively. Finally, we put $a(x) = a_1(x) \cdots a_r(x)$. This is clearly doable, but let us simplify and shorten the procedure.

Let $e = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ be the prime decomposition of e (p_i being primes all different to each other, and different from p). Note that, generically, there are infinitely many expressions of the form $e = \operatorname{lcm}\{e_1, \dots, e_r\}$, $r \geqslant 1$, $e_i \geqslant 2$. But, obviously, the minimality of the sum of orders will be achieved over an *irredundant* one, i.e. an expression such that $\operatorname{lcm}\{e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_r\} < e$, for every $i \in I$. It is clear that, for every such expression and every $j = 1, \dots, t$, $p_j^{\alpha_j+1}$ divides no e_i, but $p_j^{\alpha_j}$ divides at least one e_i. Choose one such e_i for every j. The irredundancy of the expression implies that we are exhausting all e_i's. So, $r \leqslant t$. In particular, there are finitely many irredundant expressions for e.

Now, using Lemma 2.7, we can simplify even more. Let $e = \operatorname{lcm}\{e_1, \dots, e_r\}$ be an irredundant expression for e corresponding to a solution of the Problem 3.6. As noted above, $p_j^{\alpha_j}$ divides, say, e_i. Suppose that p_j^{α} also divides $e_{i'}$ for some $i' \neq i$ and $0 < \alpha \leqslant \alpha_j$. Then, we can replace $e_{i'}$ by $e_{i'}/p_j^{\alpha}$ in the above irredundant expression for e, and still have an irredundant expression for e. But, by Lemma 2.7 (i), the new expression has sum of orders less than or equal to the original one. Repeating this operation several times, we have proved that there always exists a solution to Problem 3.6 corresponding to an irredundant expression, $e = \operatorname{lcm}\{e_1, \dots, e_r\}$, where each p_j (and hence $p_j^{\alpha_j}$) divides exactly one e_i.

Thus, we only need to consider all expressions of the form $e = \operatorname{lcm}\{e_1, \dots, e_r\}$ where each e_i is a product of some of the $p_j^{\alpha_j}$, in such a way that every $p_j^{\alpha_j}$ appears exactly once. In other words, $\{e_1, \dots, e_r\}$ represents a partition of the set $\{p_1^{\alpha_1}, \dots, p_t^{\alpha_t}\}$. We have to visit all these possible partitions and choose one, say $\{e_1, \ldots, e_r\}$, that has the smallest possible value for $n = \mathrm{ord}_{e_1}(q) + \cdots + \mathrm{ord}_{e_r}(q)$. Then, compute irreducible polynomials $a_1(x), \ldots, a_r(x) \in \mathbb{F}_q[X]$ with orders $e_1, \ldots, e_r$, respectively (following, for example, the comment after Theorem 2.4). And finally, $a(x) = a_1(x) \cdots a_r(x)$ is a polynomial of the smallest possible degree (namely n) among those of order e. This completely solves Problem 3.6 and so achieves our goal.

Theorem 3.7. *There exists an algorithm such that, given an integer $e \geqslant 2$, it constructs a connection polynomial $a(x) \in \mathbb{F}_q[X]$ of the smallest possible degree (say n), and a seed $v \in \mathbb{F}_q^n$, for a linear feedback shift register expanding a circular sequence of length precisely e.*

Proof. According to the previous discussion, let us first factorize $e = p^{\alpha_0} e_*$, where $e_* = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ and $\alpha_0 \geqslant 0$, $t \geqslant 0$, $\alpha_i > 0$ for $i = 1, \ldots, t$, and $p, p_1, \ldots, p_t$ are pairwise different primes. If $e_* \geqslant 2$ (or equivalently $t \neq 0$), follow the above solution to Problem 3.6 for computing a polynomial, say $a_*(x) \in \mathbb{F}_q[X]$, with order e_*, $a_*(0) \neq 0$, and the smallest possible degree; otherwise, put $a_*(x) = 1$. Now, take $a(x) = (x-1)^{p^{\alpha_0 - 1}+1} a_*(x)$ if $\alpha_0 > 0$ and $a(x) = a_*(x)$ otherwise. By Lemmas 2.5 and 2.6, $a(x)$ has order $\mathrm{ord}(a(x)) = \mathrm{lcm}(p^{\alpha_0}, e_*) = p^{\alpha_0} e_* = e$. Thus, the cyclic length of $u(x) = 1$ modulo $a(x)$ is precisely e. And, by construction, $a(x)$ has the smallest possible degree among all such polynomials.

So, we have algorithmically constructed a monic polynomial $a(x) \in \mathbb{F}_q[X]$ (and its companion matrix M) of the smallest possible degree, and a column vector $u \in \mathbb{F}_q^n$ such that the sequence $M^i u$ has period exactly e. Finally, use Lemma 2.2 to realize the same period on the left side of M. That is, compute the matrix P referred to in the proof of Lemma 2.2, and consider $v = Pu$. By Lemma 2.2, $v^T M^i$ has period exactly e. Hence, the LFSR with connection polynomial $a(x)$ and seed v expands a circular sequence of length precisely e and have the minimal possible size. □

We have no detailed analysis of the complexity of this algorithm, but it seems to be polynomial on e. The relevant part is the computation of $a_*(x)$ from e_* (apart from the factorization of e itself, that we assume is easy or given as an input). For doing this, one has to run over all possible partitions of a set of t elements. There are, at most, exponentially many on t^2, but t is at most logarithmic on e. So, in terms of e, the amount of work to do is polynomial.

4. The algorithm

In the present section, let us make explicit the given algorithm. As seen in the previous section, it works in an arbitrary finite field $\mathbb{F}_q$. However, since all the engineering applications involve the binary case, we shall give a particularization to this case taking $p = q = 2$ everywhere (the interested reader can easily follow the algorithm in any other finite field $\mathbb{F}_q$).

The input of the algorithm is an integer $e \geqslant 2$. The output will be the connection polynomial, $a(x) \in \mathbb{F}_2[X]$, and the seed $v \in \mathbb{F}_2^n$ of the desired linear feedback shift register.

Input: an integer $e \geqslant 2$.
Outputs: a polynomial $a(x) \in \mathbb{F}_2[X]$ of degree n, and a vector $v \in \mathbb{F}_2^n$.

Begin

(1) **Factorize** e. Decompose e as a product of prime numbers $e = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, with $\alpha_0 \geqslant 0$, $t \geqslant 0$, $\alpha_i > 0$ for $i = 1, \dots, t$, and $2, p_1, \dots, p_t$ pairwise different primes.
(2) **If** $t = 0$, **put** $a_*(x) = 1$ and **go** to step **(8)**.
(3) **Set** $e_* := p_1^{\alpha_1} \cdots p_t^{\alpha_t} \geqslant 3$ and $nmin := \infty$.
(4) **Enumerate** the set of all partitions $\mathcal{P}_1, \dots, \mathcal{P}_l$ of the set of integers $\{p_1^{\alpha_1}, \dots, p_t^{\alpha_t}\}$. Let $\mathcal{P}_j = \{P_{j,1}, \dots, P_{j,r_j}\}$ be the pairwise disjoint classes of the j-th partition, $P_{j,1} \cup \cdots \cup P_{j,r_j} = \{p_1^{\alpha_1}, \dots, p_t^{\alpha_t}\}$.
(5) **For** j **from 1 to** l **do**:
(5.1) **For** i **from 1 to** r_j **compute** $n_i := \mathrm{lcm}_{d \in P_{j,i}} \{\mathrm{ord}_d(2)\}$ (which equals $\mathrm{ord}_{\prod_{d \in P_{j,i}} d}(2)$ by Lemma 2.7).
(5.2) **Compute** $n := n_1 + \cdots + n_{r_j}$.
(5.3) **If** $n < nmin$ then **let** $nmin := n$, $r := r_j$, and $e_i = \mathrm{lcm}\, P_{j,i} = \prod_{d \in P_{j,i}} d$ for every $i = 1, \dots, r$. We then have $e = \mathrm{lcm}\{e_1, \dots, e_r\} = e_1 \cdots e_r$.
(6) **Compute** irreducible polynomials $a_1(x), \dots, a_r(x) \in \mathbb{F}_2[X]$ of orders $e_1, \dots, e_r$, respectively (follow the comment after Theorem 2.4).
(7) **Set** $a_*(x) := a_1(x) \cdots a_r(x)$.
(8) **Set** $a(x) := (x-1)^s a_*(x)$ for the connection polynomial, where $s = 2^{\alpha_0 - 1} + 1$ if $\alpha_0 > 0$, and $s = 0$ otherwise.
(9) **Set** $u(x) = 1$ (or, alternatively, any polynomial coprime with $a(x)$) thought of as a vector u.
(10) **Compute** the companion matrix M of $a(x)$, and the matrix P referred to in the proof of Lemma 2.2. Then, compute $v = Pu \in \mathbb{F}_2^n$.

End.

For step (4), a possible way of enumerating all partitions of the set $\{p_1^{\alpha_1}, \dots, p_t^{\alpha_t}\}$ is doing it recursively on t. Once we have all partitions of $\{p_1^{\alpha_1}, \dots, p_{t-1}^{\alpha_{t-1}}\}$, it only remains to determine the position of $p_t^{\alpha_t}$, which can join one of the already existing classes, or form a new class alone. The advantage of this method is that one can simultaneously and easily calculate the n_i's of the new partition in terms of the old ones: they are all the same except the one corresponding to the class where $p_t^{\alpha_t}$ belongs. And computing this is as easy as doing the least common multiple between the existing one and $\mathrm{ord}_{p_t^{\alpha_t}}(2)$.

5. Example: a binary sequence of length 360

Let us find a 360 bits binary sequence expanded by a LFSR with connection polynomial of the minimum possible degree. This sequence can then be used to build an angular position encoder with a resolution of exactly one degree, minimizing the number of sensors in use. We will follow the algorithm given above. The desired order is $e = 360 = 2^3 3^2 5$ so, $\alpha_0 = 3$, $t = 2$ and $e_* = 3^2 5 = 45$.

In step (4) we find that the set of integers $\{3^2, 5^1\}$ has only two partitions, namely $\mathcal{P}_1 = \{\{3^2, 5^1\}\}$ and $\mathcal{P}_2 = \{\{3^2\}, \{5^1\}\}$.

When running step (5) for $\mathcal{P}_1$ ($r_1 = 1$), we have $n = n_1 = \mathrm{lcm}\{\mathrm{ord}_9(2), \mathrm{ord}_5(2)\} = \mathrm{lcm}\{6, 4\} = 12$. For $\mathcal{P}_2$ ($r_2 = 2$), we have $n_1 = \mathrm{ord}_9(2) = 6$, $n_2 = \mathrm{ord}_5(2) = 4$ and so, $n = 6 + 4 = 10$. So, the second partition is the best one and we end up with $nmin = 10$, $r = 2$, $e_1 = 9$ and $e_2 = 5$ (of course, $45 = 9 \cdot 5$).

In step (6) we have to compute irreducible polynomials $a_1(x), a_2(x) \in \mathbb{F}_2[X]$ of orders 9 and 5 respectively. Following the comment in the first paragraph after Theorem 2.4, $a_1(x)$ must be an irreducible factor of

$$\frac{x^9 - 1}{\mathrm{lcm}\{x^3 - 1, x - 1\}} = \frac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1,$$

which is itself irreducible. Hence, $a_1(x) = x^6 + x^3 + 1$. Similarly,

$$a_2(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1$$

Thus, in step (7) we have $a_*(x) = x^{10} + x^9 + x^8 + x^5 + x^2 + x + 1$, a polynomial of the minimal possible degree among those of order 45. We point out here that, in this particular example, $a_1(x)$ and $a_2(x)$ are unique because there exist only one irreducible polynomial of order 9, and only one of order 5; in general, there are several and any choice will give raise to different connection polynomials $a(x)$, all of them valid for our purposes.

In step (8), we put $s = 2^{3-1} + 1 = 5$ and compute the desired connection polynomial $a(x) = (x - 1)^s a_*(x) = x^{15} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$. In step (9) we consider the vector $u = (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$.

Finally, in step (10) we compute the matrix P of Lemma 2.2: it is the symmetric 15×15 invertible binary matrix $P = (p_{i,j})$ such that $p_{i,j} = 1$

if $i+j \in \{16,19,20,21,23,26,27,28,29\}$, and $p_{i,j}=0$ otherwise. Then, $v = Pu = (0,0,0,0,0,0,0,0,0,0,0,0,0,0,1)^T$.

This means that the LFSR with connection polynomial $a(x)$ and seed v expands a circular sequence of length $e = 360$, as desired:

```
000000000000001001110100111100100101111001
110011101110111010100000011100001010010100
100000100110011001101111110110101101011100
011111101010001000100011000110000101101100
001101000110111111111111110110001011000011
011010000110001100010001000101011111100011
110101101011011111101100110011001000001001 0
100101000011100000001010111011101110011100 1
111010010011110010111001.
```

That is, the given list of bits, considered circularly, has length 360 and the property that all subwords of 15 consecutive bits are different to each other. Of course, there are 360 such 15-tuples hence, this sequence can be used to measure positions of a circular device with precision exactly equal to one degree, and using 15 sensors. Furthermore, 15 is the smallest possible degree realizing this i.e., no connection polynomial of degree less than 15 has any possible seed expanding a circular sequence of length 360. So, 15 is the minimum number of sensors needed among all *linear* feedback shift registers expanding such sequences.

A totally different question (and out of the scope of the present paper) is how to improve even more, using non-linear methods. An obvious thing to do first, is to check if the obtained sequence works with fewer sensors. As it was constructed, all the 360 consecutive 15-tuples are different to each other, but it turns out that the same is true with the 360 consecutive 14-tuples (and fails for 13-tuples). This way, we can use the same sequence saving one sensor for free. But this phenomenon depends, in a strongly combinatorial way, on the particular sequence analyzed (i.e. on the seed chosen in step (9) of the algorithm). The following table contains the number of initial seeds expanding sequences of length 360, but in such a way that all the 360 consecutive 15-tuples, 14-tuples, 13-tuples, 12-tuples and 11-tuples, respectively, are pairwise different:

# of seeds	-	16	12	6	8	-	-
min # of sensors	15	14	13	12	11	10	9
sensors saved	0	1	2	3	4	5	6

Clearly, an absolute lower bound for the number of sensors needed in this example is 9 (since $2^8 < 360 < 2^9$). And, according to [4], there does exist a circular sequence of length 360 such that all 9-tuples of consecutive bits are pairwise different. However, the method given in [4] to find such a sequence is not effective (it is comparable to brute force searching among all possible 2^{360} sequences), while our method is fast. For completeness, we carried out this brute force search and found the following sequence of 360 bits

```
111110100000000100000010100000100100000110
000000110100001000100001010100001100100001
110000001110100010010100010100100010110000
010110100011000100011010100011100100011110
000011110100100100110000100110100101010100
101100100101110000101110100110010100110110
000110110100111000100111010100111100100111
110000111110101010110001010110101011100101
011110001011110101100111,
```

allowing to measure exact degrees in a rotating disk making use of only 9 sensors, the absolute minimum.

6. Conclusions

This paper presents an extension to previous works in absolute angular position measurement systems. It starts by focusing the problem of searching for linear feedback shift registers being able to expand closed binary sequences of prescribed length. First problem was to demonstrate the existence of solutions for any arbitrary cyclic length. And secondly, to find the smallest size of a LFSR expanding such a sequence. These two problems were already solved in [4], but for arbitrary sequences (not just those linearly generated) and not giving any insights on the way of constructing such cycles (apart from brute force). In the present paper, we show that *all* lengths are also realizable using *linear* feedback shift registers, and provide an efficient algorithm to construct one of the smallest possible size.

For going through the solution, the paper starts by addressing well known facts about finite fields and polynomials over them, which are closely related to cyclic code expansion using linear methods. Then the technical part (results from 3.1 to 3.5) comes, where we analyze the lengths obtainable by a given LFSR when moving the seed. Out of this analysis, we produce an algorithm for constructing a LFSR of the smallest possible size, and a seed expanding a sequence of the prescribed length (Theorem 3.7). The algorithm is explicitly written in section 4, particularized to the binary case. Finally, the paper develops a classical example, namely the design of a connection polynomial and a seed for a LFSR expanding a cyclic sequence of exactly 360 positions in length, and using the minimum possible number of reading sensors. This minimum number is discussed in case of dropping the linearity of the shift register.

Acknowledgments

This work has received partial support by the Spanish Science and Technology Council CICYT project ref. DPI2002-01621 and by DGI (Spain) through grant BFM2003-06613. We thank J.J. Egozcue for originally putting in contact to each other the first and third named authors (resp., an engineer and a mathematician) with respect to the problem addressed here. E. Ventura gratefully acknowledges also the Centre de Recerca Matemàtica (Barcelona) for its warm hospitality during the academic course 2004-2005, while this paper was written.

References

[1] B. Arazi, Position recovery using binary sequences, *IEEE Electronics Letters*, **20** (1984), 61-62.

[2] S.W. Golomb, Shift Register Sequences, Aegean Park Press, 1982.

[3] M. Goresky, A.M. Klapper, Fibonacci and Galois representations of feedback-with-carry shift registers, *IEEE Trans. Inform. Theory*, **48** (2002), no. 11, 2826–2836.

[4] A. Lempel, m-ary closed sequences, *Journal of combinatorial theory*, **10** (1971), 253-258.

[5] R. Lidl, H. Niederreiter, Finite fields, Encyclopedia of mathematics and its applications **20**, Cambridge University Press.

[6] F.J. MacWilliams, N.J.A. Sloane, Pseudo-random sequences and arrays, *Proceedings IEEE*, **64** (1976), 1715-1729.

[7] R.J. McEliece, Finite Fields for Computer Scientists and Engineers, Kluwer Academic Publishers, 1987.

[8] E.M. Petriu, Absolute-type pseudo-random shaft encoder with any desired resolution, *IEEE Electronics Letters*, **21** (1985), 215-216.

[9] E.M. Petriu, Absolute-type position transducers using a pseudo-random encoding, *IEEE Trans. Instrumentation and Measurement*, **IM-36** (1987), 950-955.

[10] E.M. Petriu, Scanning method for absolute pseudorandom position encoders, *IEEE Electronics Letters*, **24** (1988), 1236-1237.

[11] E. Ventura, Dynamic structure of matrices over finite fields, Proceedings of EAMA-97 (Sevilla) (1997), 413-420.

[12] M. Yoeli, Binary ring sequences, *Am. Math. Monthly*, **69** (1962), 852-855.

J.M. Fuertes,
Dept. Enginyeria de Sistemes, Automàtica i Informàtica Industrial,
Universitat Politècnica de Catalunya, Barcelona, Spain.
E-mail: josep.m.fuertes@upc.edu

B. Balle,
Facultat de Matemàtiques i Estadística, Universitat Politècnica
de Catalunya, Barcelona, Spain.
E-mail: borja.balle@gmail.com

E. Ventura,
Dept. Mat. Apl. III, Universitat Politècnica de Catalunya,
Centre de Recerca Matemàtica, Barcelona, Spain.
E-mail: enric.ventura@upc.edu