Absolute-Type Shaft Encoding Using LFSR Sequences With a Prescribed Length

Josep M. Fuertes, *Senior Member, IEEE*, Borja Balle, and Enric Ventura

***Abstract*—Maximal-length binary sequences have existed for a long time. They have many interesting properties, and 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 to measure absolute angular positions as the circle can be divided into as many parts as different codes can be retrieved. This paper describes how a closed binary sequence with an arbitrary length can be effectively designed with the minimal possible block length using *linear feedback shift registers*. Such sequences can be used to measure a specified exact number of angular positions using the minimal possible number of sensors that linear methods allow.**

***Index Terms*—Absolute angular position sensor, closed circular sequences, linear feedback shift register (LFSR), maximal-length binary sequences, polynomials over finite fields.**

I. Introduction

An angular absolute position measurement system 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 of an arrangement of black and white ("1" and "0," respectively) distributed in concentric coronas. Most commercial transducers use the Gray coding bit distribution to reduce the different scanning errors. However, such coding has two drawbacks: 1) As the resolution (and, thus, the number of bits) increases, the disk diameter also increases, and 2) the number of sectors has to be exactly a power of two.

For the first drawback, there is a method that uses only a one-bit code track based on the window property of pseudorandom binary sequences. This property states that in a pseudorandom cyclic code expansion, all the n-bit elements that can be successively taken are different from each other. The result is that once the pseudorandom 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] and [8]–[10]).

Manuscript received February 2, 2006; revised October 22, 2007. This work was supported in part by the Spanish Science and Technology Council under CICYT Research Projects DPI2007-61527 and DPI2002-01621 and in part by DGI (Spain) under Grant BFM2003-06613.

The authors are with the Technical University of Catalonia, 08034 Barcelona, Spain.

Digital Object Identifier 10.1109/TIM.2007.913811

The second drawback is about the number of sectors. We need to produce a pseudorandom cyclic code expansion, all of whose n-bit subwords are different from each other and have a prescribed length $e \geqslant 2$. An apparent restriction is $2 \leqslant e \leqslant 2^n$. In [4] and using the graph theory, Lempel proved that such sequences always exist only under the hypothesis that $2 \leqslant e \leqslant 2^n$. The problem is how to explicitly construct them with a fast algorithm, which is 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 (LFSRs) with a *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 from each other (see [2] and [6]). In [8], Petriu introduces a truncation of these maximal-length sequences to obtain the desired exact number of sectors, which are not necessarily a power of two. To detect the truncation point, it was proposed to include an additional corona, where an additional bit shows a 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 (nonmaximal) feedback shift registers that expand 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 (unnecessarily linear) feedback shift registers (see [2] and [12] for the binary case and [4] for a generalization to m-ary sequences).

In this paper, this problem is again considered, and another solution is provided, which has the following two additional advantages. Given a natural number $e \geqslant 2$, our algorithm produces an LFSR with a connection polynomial of the *smallest* possible degree and a *seed* that expands a circular sequence of length exactly equal to e. In general, the fact that it is *linear* makes it easier to implement in hardware. Moreover, the fact that the output is a circular sequence of length e expanded by an LFSR of the *smallest* possible degree ensures that the smallest possible number of sensors is to be used. Finally, the algorithm is fast for the typical values of e, which can be useful in particular applications. The techniques and arguments used here are inspired by those contained in [11].

It should be pointed out that with the techniques in this paper, the number of needed sensors is minimized among all possible LFSRs that expand circular sequences of a prefixed length. However, it is unclear how to systematically achieve the absolute minimum among unnecessarily linear LFSRs. In Section V, we will show an example where these two minima do not agree.

This paper is organized as follows: Section II contains the preliminaries needed for LFSRs and for polynomials over finite fields, stating the notation that will be used. Section III is the central part of this paper, where the cyclic structure of polynomials is discussed, and the algorithm is constructed and justified. Then, in Section IV, the algorithm is made explicit and particularized to the binary case. Finally, an example is developed, and conclusions are exposed.

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

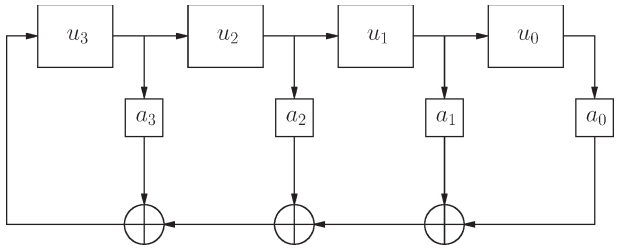

Fig. 1. LFSR with the Fibonacci architecture.

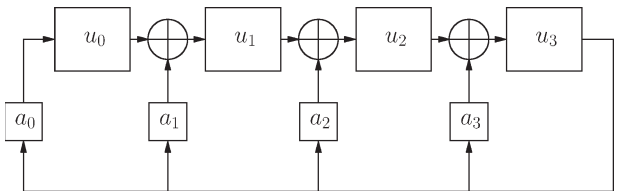

Fig. 2. LFSR with the Galois architecture.

II. Preliminaries

A. Focusing on the Problem

LFSRs are well-known electronic digital circuits that are used to expand periodic sequences over finite fields (over $\mathbb{F}_2$ for binary sequences). See [2] or [7] for generalities about them.

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

Let $n \geqslant 1$ be a natural number, and let $a(x) = -(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) + x^n \in \mathbb{F}_q[X]$ 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

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

which is usually called the *companion* matrix of $a(x)$. It is well known that the characteristic polynomial of M is $a(x)$; in particular, $a(M) = 0$. Now, take 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 consider the sequences of vectors $M^i u$ and $u^T M^i$, $i = 0, 1, 2, \ldots$. First, since the set $\mathbb{F}_q^n$ is finite, there must be eventual repetitions, e.g., $M^i u = M^j u$ for $i < j$. Moreover, since M is invertible, we have $u = M^{j-i}u$, which means 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 (thus losing the first coordinate) and with the last coordinate computed according to the last column of M. Thus, out of M and u, one can produce a clockwise circular sequence of e elements of $\mathbb{F}_q$ in such a way that the e consecutive n-tuples that are readable from it are pairwise different, where e is the period of the sequence $u^T M^i$. The generation of such a circular sequence is typically carried out by the standard electronic device that is called LFSR, with a *connection polynomial* $a(x)$, a *seed* u, and the so-called Fibonacci architecture (see Fig. 1). Note that "linear" stands for the linearity of the computation of the last coordinate in terms of the previous n values). As such, the following problem is addressed in this paper.

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

Let us reinterpret the problem in terms of the sequence $M^i u$, which is 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 represents the polynomial $u(x)x \bmod a(x)$. Thus, 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 $u(x)x^j \equiv u(x) \bmod a(x)$. This number is called the *cyclic length of* $u(x)$ *modulo* $a(x)$ and will be closely studied in the following paragraphs.

The relation between Problem 2.1 and cyclic lengths modulo polynomials is not immediately apparent 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 a period of three, whereas $M^i u$ has a period of six. 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 an $n \times n$ matrix over $\mathbb{F}_q$. Then, the set of periods of $u^T M^i$ coincides with that of $M^i u$, whereas 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 $\mathbb{F}_q^n$ that *preserves* 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 exists $P \in GL_n(\mathbb{F}_q)$ such that $PMP^{-1} = M^T$). For every matrix P and 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, thus, to $(Pu)^T = (Pu)^T M^r$. Hence, the periods of the sequences $M^i u$ and $(Pu)^T M^i$ coincide.

For later use, we remark that there always exists such a matrix P with the upper left triangle full of zeros, with the contradiagonal full of ones (and therefore invertible), and with each of the consecutive subcontradiagonals having constant values (thus, P is symmetric). Given M, i.e., the companion matrix of a monic polynomial $a(x) = -(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) + x^n \in \mathbb{F}_q[X]$, one can recursively fill the entries of such a matrix P by imposing the additional condition that PM is also symmetric (note that PM coincides with P by removing its first column and adding a last column equal to Pa, where a is the last column of M). This way, an invertible matrix P, with both P and PM being symmetric, is obtained. This P is valid for our purposes since $PM = (PM)^T = M^T P^T = M^T P$. ■

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 a prescribed cyclic length for $u(x)$ modulo $a(x)$. In fact, Lemma 2.2 indicates that the same $a(x)$ and an easily computable vector $v = Pu$ solve 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, e.g., n, and a seed $u(x) \in \mathbb{F}_q[X]$, which is a polynomial of degree smaller than n, such that the cyclic length of $u(x)$ modulo $a(x)$ is precisely equal to e.

B. Polynomials Over Finite Fields

This section summarizes the elementary facts about polynomials over finite fields that will be needed later in this paper.

Let $a(x) \in \mathbb{F}_q[X]$ be a polynomial of degree n satisfying $a(0) \neq 0$. The ring $\mathbb{F}_q[X]/a(x)\mathbb{F}_q[X]$ contains $q^n - 1$ nonzero elements, and thus, 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 that $a(0) \neq 0$ implies that $a(x)$ also divides $x^{s_2 - s_1} - 1$. It is standard to define the *order* of $a(x)$, which is 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.

1) Fact 1: 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 a multiple of p [5, Th. 3.4].

2) Fact 2: $\gcd(x^r - 1, x^s - 1) = x^{\gcd(r,s)} - 1$. 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 [5, Th. 3.6].

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

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

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

Now, Lemmas 2.5 and 2.6 are needed to better understand the order of polynomials. The following notation will be convenient: Given the prime number p and a positive integer s, let us define $\lceil s \rceil_p = \lceil \log_p s \rceil$, i.e., the smallest positive integer h such that p^h is not less than s (we will use $\lceil s \rceil$ 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 [5, Lemma 3.8]: 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 [5, Lemma 3.9]: 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, we will also use the following technical lemma.

Lemma 2.7: Let $a, b, q \geqslant 2$ be three integers such that a and b are coprime with q. Then

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

In particular, we have the following.

i) If a divides b, then $\mathrm{ord}_a(q)$ divides $\mathrm{ord}_b(q)$.
ii) If a and b are coprime to each other, 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 $q^{e_b} - 1$. Thus, $\mathrm{lcm}\{a, b\}$ 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, use Fact 2). On the other hand, a divides $\mathrm{lcm}\{a, b\}$, which divides $q^{e_{a,b}} - 1$. Thus, 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 $\mathrm{ord}_{\mathrm{lcm}\{a,b\}}(q) = e_{a,b} = \mathrm{lcm}\{e_a, e_b\} = \mathrm{lcm}\{\mathrm{ord}_a(q), \mathrm{ord}_b(q)\}$. Statements i) and ii) of Lemma 2.7 are particular cases. ■

III. Construction

As stated in the previous section, our main goal is to solve Problem 2.3. For this purpose, given a polynomial $a(x) \in \mathbb{F}_q[X]$, the set of numbers that occurs as a cyclic length of some seed $u(x)$ modulo $a(x)$ must be understood. The finite

set of all those possible numbers is named *cyclic structure of* $a(x)$ and is 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 $a(x)$. The following two propositions describe this set.

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 cyclic 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 can 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 $u(x)(x^k - 1)$. Let $u(x) = u'(x)a(x)^d$ for some $0 \leqslant d < s$ and some $u'(x) \in \mathbb{F}_q[X]$ coprime to $a(x)$. Then, the previous assertion is now equivalent as saying that k is the smallest positive integer such that $a(x)^{s-d}$ divides $x^k - 1$, i.e., k is the order of $a(x)^{s-d}$. Lemma 2.5 proves that $k = \text{ord}(a(x)^i) = ep^j$ 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 $j = 0, \ldots, \lceil s \rceil$ occurs in $\mathcal{CS}(a(x)^s)$, for example, as the cyclic length of $u(x) = a(x)^{s-(p^{j-1}+1)}$. This makes sense because $j \leqslant \lceil s \rceil$ implies that $p^{j-1} + 1 \leqslant p^{\lceil s \rceil - 1} + 1 \leqslant s$ (here, we understand that $p^{-1} = 0$). ■

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 $a(x) = a_1(x)^{s_1} a_2(x)^{s_2}, \ldots, a_r(x)^{s_r}$ with increasing exponents $s_1 \leqslant s_2 \leqslant \cdots \leqslant s_r$. Let $e_i = \text{ord}(a_i(x))$ for $i \in I = \{1, \ldots, r\}$. Then, the cyclic structure of $a(x)$ is given by

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

Proof: Taking $u(x) = 0$, we can 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 $k = \text{lcm}_{i \in I}\{k_i\}$. 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 that by assumption, $J = \{i \in I | k_i \neq 1\} \neq \emptyset$. Then, $k = \text{lcm}_{i \in J}\{k_i\} = (\text{lcm}_{i \in J}\{e_i\})p^t$, where $0 \leqslant t \leqslant \lceil s_j \rceil$ and $j = \max J$. Conversely, any positive number of the form $(\text{lcm}_{i \in J}\{e_i\})p^t$ 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 appears as the cyclic length of $u(x) = (\prod_{i \in J \setminus \{j\}} a_i(x)^{s_i - 1}) \cdot a_j(x)^{s_j - (p^{t-1}+1)} \cdot (\prod_{I \not\ni J} a_i(x)^{s_i})$ modulo $a(x)$. This makes sense because $t \leqslant \lceil s_j \rceil$ implies that $p^{t-1} + 1 \leqslant p^{\lceil s_j \rceil - 1} + 1 \leqslant s_j$ (here, we understand that $p^{-1} = 0$). ■

As an immediate corollary of Theorem 2.4, one can already say that every positive integer e occurs as the cyclic length of some polynomial (even of $u(x) = 1$) modulo some other $a(x)$. That is, given a certain length, there always exists an LFSR that expands, with an appropriate seed, a circular sequence of this 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 equal to e. ■

To attack Problem 2.3, several reductions to simpler problems will be done. Let $a(x) \in \mathbb{F}_q[X]$ be a polynomial with $a(0) \neq 0$, and consider its factorization into different irreducible factors $a(x) = a_1(x)^{s_1} a_2(x)^{s_2}, \ldots, a_r(x)^{s_r}$ with increasing exponents $s_1 \leqslant s_2 \leqslant \cdots \leqslant s_r$. Let $e_i = \text{ord}(a_i(x))$ for $i \in I = \{1, \ldots, r\}$, and consider the new polynomial $a'(x)$ being like $a(x)$ but with the following changes: 1) Reduce all the multiplicities $s_1, \ldots, s_r$ down to 1, and 2) put exponent $s_{r+1} = p^{\lceil s_r \rceil - 1} + 1 \leqslant s_r$ to one of the linear factors if any, or otherwise, 2') add the new factor $(x-1)^{s_{r+1}}$.

Lemma 3.4: With the previous notation, and assuming $s_r \geqslant 2$, we have $\mathcal{CS}(a'(x)) \leq \mathcal{CS}(a(x))$, and $\deg(a'(x)) \leqslant \deg(a(x))$.

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

Thus, to solve Problem 2.3, it is sufficient to consider polynomials whose decomposition into irreducible factors has all the exponents equal to 1, except maybe only one over a linear factor.

Consider now such a polynomial $a(x) = a_*(x)a_i(x)^{s_{r+1}-1}$ or $a(x) = a_*(x)(x-1)^{s_{r+1}}$, where $s_{r+1} \geqslant 0$, $a_*(x) = a_1(x), \ldots, a_r(x)$, and $a_1(x), \ldots, a_r(x), (x-1), x$ are pairwise different irreducible polynomials, and $a_i(x)$ is one of the linear factors. Since $a_*(x)$ has no multiplicities and, by Fact 1 in Section II-B, $e_i = \text{ord}(a_i(x))$ is not divisible by p, Proposition 3.2 states that the members of $\mathcal{CS}(a_*(x))$ are also not divisible by p. Again, by Proposition 3.2, the unique contribution of the exponent s_{r+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 a multiple of p, searching only among polynomials without multiplicities and not being multiples of $x - 1$ (by then increasing to $p^{s-1} + 1$ the exponent of one of its linear factors if any, or otherwise 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 lemma, a further reduction can be done.

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

Thus, according to the description given in Proposition 3.2, the only relevant contribution of a polynomial $a(x) = a_1(x) \ldots a_r(x)$ to the set $\mathcal{CS}(a(x))$ is given by the maximal set of indexes $J = I$ (with the other elements in that set being also

present in the cyclic structure of some polynomial of smaller degree). In this case, since the $a_i(x)$'s are coprime to each other, Lemma 2.6 states that

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

In other words, to solve Problem 2.3, the unique relevant entry in $\mathcal{CS}(a(x))$ is the number $\text{ord}(a(x))$. Moreover, having computed a polynomial $a(x)\in\mathbb{F}_q[X]$ with a given order $\text{ord}(a(x))=e\geqslant 2$, we have by definition that e is the smallest exponent $i\geqslant 1$ such that $x^i\equiv 1 \bmod a(x)$. Hence, the seed $u(x)=1$ has a cyclic length modulo $a(x)$ precisely equal to e and a degree less than that of $a(x)$. Thus, Problem 2.3 reduces to Problem 3.6.

Problem 3.6: Given a natural number $e\geqslant 2$, which is not a 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 therefore without multiplicities and not a multiple of $x-1$) such that $\text{ord}(a(x))=e$.

This is now a problem that is 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 explicitly indicates the degree of the polynomials that are irreducible. However, irreducible polynomials are not always those that have the smallest possible degree among those of a given order. (In the example worked out in Section V, a binary polynomial of order 45 and degree 10 is shown, whereas irreducible polynomials of order 45 all have a degree of $\text{ord}_{45}(2)=12$.) Thus, a more detailed search among polynomials of a given order is needed.

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

$$\begin{aligned}e &= \text{ord}\left(a(x)\right)=\text{ord}\left(a_1(x)\cdots a_r(x)\right)=\text{lcm}\{e_1,\ldots,e_r\}\\ n &= \deg\left(a(x)\right)=n_1+\cdots+n_r=\text{ord}_{e_1}(q)+\cdots+\text{ord}_{e_r}(q).\end{aligned}$$

Thus, $a(x)$ can be found by listing all the expressions of the form $e=\text{lcm}\{e_1,\ldots,e_r\}$, $e_i\geqslant 2$ and, for each of them, by computing $\text{ord}_{e_1}(q)+\cdots+\text{ord}_{e_r}(q)$. When the minimal possible value of this sum is obtained, use the constructive comment after Theorem 2.4 to obtain irreducible polynomials $a_1(x),\ldots,a_r(x)$ of orders $e_1,\ldots,e_r$, respectively. Finally, take $a(x)=a_1(x),\ldots,a_r(x)$. Clearly, this is already an algorithm, but we could still simplify and shorten it.

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

Now, using Lemma 2.7, a further simplification can be done. Let $e=\text{lcm}\{e_1,\ldots,e_r\}$ be an irredundant expression for e corresponding to a solution of Problem 3.6. As previously noted, $p_j^{\alpha_j}$ divides, e.g., 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 aforementioned irredundant expression for e and still have an irredundant expression for e. However, by Lemma 2.7(i), the new expression has sum of degrees less than or equal to the original one. Repeating this operation several times, it has been proven that there always exists a solution to Problem 3.6 corresponding to an irredundant expression $e=\text{lcm}\{e_1,\ldots,e_r\}$, 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 $e=\text{lcm}\{e_1,\ldots,e_r\}$, 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, $\{e_1,\ldots,e_r\}$ represents a partition of the set $\{p_1^{\alpha_1},\ldots,p_t^{\alpha_t}\}$. We have to visit all these possible partitions and choose one that has the smallest possible value for $n=\text{ord}_{e_1}(q)+\cdots+\text{ord}_{e_r}(q)$, e.g., $\{e_1,\ldots,e_r\}$. 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). Finally, $a(x)=a_1(x),\ldots,a_r(x)$ is a polynomial of the smallest possible degree (namely n) among those of order e. This completely solves Problem 3.6, thus achieving 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 (e.g., n) and a seed $v\in\mathbb{F}_q^n$ for an LFSR that expands a circular sequence of length precisely equal to e.

Proof: According to the previous discussion, let us first factorize $e=p^{\alpha_0}e_*$, where $e_*=p_1^{\alpha_1},\ldots,p_t^{\alpha_t}$ and $\alpha_0\geqslant 0, t\geqslant 0$, and $\alpha_i>0$ 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 aforementioned solution to Problem 3.6 for computing a polynomial, e.g., $a_*(x)\in\mathbb{F}_q[X]$, with order e_*, $a_*(0)\neq 0$, and the smallest possible degree; otherwise, put $a_*(x)=1$. Now, take $a(x)=a_*(x)$ if $\alpha_0=0$, and if $\alpha_0>0$, take $a(x)$ to be $a_i(x)^{p^{\alpha_0-1}}a_*(x)$, where $a_i(x)$ is one of the linear factors of $a_*(x)$, or $a(x)=(x-1)^{p^{\alpha_0-1}+1}a_*(x)$ if there are no such linear factors. By Lemmas 2.5 and 2.6, $a(x)$ has order e. Thus, the cyclic length of the seed $u(x)=1$ modulo $a(x)$ is precisely equal to e. Moreover, by construction, $a(x)$ has the smallest possible degree among all such polynomials.

Thus, we have algorithmically constructed a monic polynomial $a(x)\in\mathbb{F}_q[X]$ (and its companion matrix M) of the smallest possible degree such that the sequence M^iu has a period exactly equal to e, where u is the column vector $u=(1,0,\ldots,0)^T\in\mathbb{F}_q^n$. Finally, use Lemma 2.2 to realize the same period on the left side of M. We note here that to do this, the actual matrix P referred to in Lemma 2.2 is unnecessary since Pu is its first column, which is always $v=(0,\ldots,0,1)^T$. By

that result, $v^T M^i$ has a period exactly equal to e. Hence, the LFSR with the Fibonacci architecture, a connection polynomial $a(x)$, and a seed v expands a circular sequence of length precisely equal to e and has the minimal possible size. ■

No detailed analysis of the complexity of this algorithm has been done, 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, which we assume is easy or given as an input). To do this, one has to run over all possible partitions of a set of t elements. Roughly speaking, there are double exponentially many on t, but t is of the order of $\log(\log e)$. Thus, in terms of e, the amount of work to do seems polynomial.

IV. Algorithm

In this section, we make the given algorithm explicit. As seen in the previous section, it works over an arbitrary finite field $\mathbb{F}_q$. However, since most of the engineering applications involve the binary case, we shall give a particularization to this case by taking $p = q = 2$ everywhere (interested readers can easily follow the algorithm in any other finite field $\mathbb{F}_q$). Note that, in this case, the unique valid linear factor is $x - 1$, and so, all the possible powers of 2 involved in e will be obtained by adding a certain power of $x - 1$.

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

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 $e = 2^{\alpha_0} p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$, with $\alpha_0 \geqslant 0$, $t \geqslant 0$, $\alpha_i > 0$ for $i = 1, \ldots, t$, and $2, p_1, \ldots, p_t$ pairwise different primes.
2) If $t = 0$, **put** $a_*(x) = 1$ and **go** to step **8)**.
3) Set $e_* := p_1^{\alpha_1}, \ldots, p_t^{\alpha_t} \geqslant 3$ and $nmin := \infty$.
4) Enumerate the set of all partitions $\mathcal{P}_1, \ldots, \mathcal{P}_l$ of the set of integers $\{p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}\}$. Let $\mathcal{P}_j = \{P_{j,1}, \ldots, P_{j,r_j}\}$ be the pairwise disjoint classes of the jth partition, $P_{j,1} \sqcup \cdots \sqcup P_{j,r_j} = \{p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}\}$.
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 $i = 1, \ldots, r$. We then have $e = \mathrm{lcm}\{e_1, \ldots, e_r\} = e_1 \cdots e_r$.
6) Compute irreducible polynomials $a_1(x), \ldots, a_r(x) \in \mathbb{F}_2[X]$ of orders $e_1, \ldots, e_r$, 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 $v = (0, \ldots, 0, 1)^T \in \mathbb{F}_2^n$.
End.

For step 4), a possible way of enumerating all partitions of the set $\{p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}\}$ is doing it recursively on t. Once we have all partitions of $\{p_1^{\alpha_1}, \ldots, p_{t-1}^{\alpha_{t-1}}\}$, 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 we can simultaneously and easily calculate the n_i's of the new partition in terms of the old n_i's: they are all the same, except for that corresponding to the class where $p_t^{\alpha_t}$ belongs. Moreover, computing the latter is as easy as doing the least common multiple between the existing n_i and $\mathrm{ord}_{p_t^{\alpha_t}}(2)$.

V. Example: Binary Sequence of Length 360

Let us find a 360-bit binary sequence expanded by an LFSR with a connection polynomial of the minimum possible degree. This sequence can then be used to build an angular position encoder with a resolution of exactly 1°, minimizing the number of sensors in use. We will follow the previously given algorithm. The desired order is $e = 360 = 2^3 3^2 5$; thus, $\alpha_0 = 3$, $t = 2$, 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 $n_1 = \mathrm{ord}_9(2) = 6$ and $n_2 = \mathrm{ord}_5(2) = 4$, and thus, $n = 6 + 4 = 10$. Therefore, 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 $a_*(x) = x^{10} + x^9 + x^8 + x^5 + x^2 + x + 1$, which is a polynomial of the minimal possible degree among those of order 45. It should be pointed out here that in this particular example, $a_1(x)$ and $a_2(x)$ are unique because there exists only one irreducible polynomial of order 9 and only one of order 5; in general, there are several polynomials, and any choice will give rise to different connection polynomials $a(x)$, which are all valid for our purposes.

In step 8), we let $s = 2^{3-1} + 1 = 5$ and compute the desired connection polynomial $a(x) = (x-1)^s a_*(x) = x^{15} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$. Finally, in step 9), we take $v = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)^T$.

This means that the LFSR with connection polynomial $a(x)$ and seed v expands the following circular sequence of length

$e = 360$, as desired:

000000000000001001110100111100100101111001110011101110110101000001110000101001010010000010011001100110111101101011010111100011111101010001000100011000100001011011000011010001101111111111111111011000010110000011011010000110001100010001000101011111100011111010110101101111011001100110010000010010100101000011100000010101110111011100111001111010010011110010111001.

That is, the given list of bits, considered circularly, has a length of 360 and the property that all subwords of 15 consecutive bits are different from 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 1° 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 that expands a circular sequence of length 360. Thus, 15 is the minimum number of sensors needed among all LFSRs that expand such sequences.

A totally different question (and out of the scope of this paper) is how to achieve better results using nonlinear methods. Evidently, the first thing to do is to check if the obtained sequence works with fewer sensors. As it was constructed, all 360 consecutive 15-tuples are different from each other, but it turns out that the same is true with the 360 consecutive 14-tuples (and fails for 13-tuples). This way, the same sequence can be used, thus saving one sensor. However, this phenomenon depends, in a strongly combinatorial way, on the particular sequence analyzed.

An absolute lower bound for the number of sensors needed in this example is 9 (since $2^8 < 360 < 2^9$). In addition, according to Lempel [4], there exists 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), whereas the method presented here is fast. For completeness, this brute force search was carried out, and the following sequence of 360 bits was found:

111110100000000100000010100000100100000110000000110100001000010101000011001000011100000011101000100101000101001000101100000101101000110001000110101000011110000011110100100100110000100110101000111001000111100000111101001001001100001001101001011001001011100001011101001100101001101100001101001110001001110101001111001001111100001111101010101100010101101010111001010111100010111101010110001010110101011100101011110001011110101100111.

allowing one to measure exact degrees in a rotating disk by using only nine sensors, which is the absolute minimum.

VI. Conclusion

This paper presents an extension to the previous works on absolute angular position measurement systems. It starts by focusing on the problem of searching for LFSRs that are able to expand closed binary sequences of a prescribed length. The first problem was to demonstrate the existence of solutions for any arbitrary cyclic length. The second problem was to find the smallest size of an LFSR that expands such a sequence. These two problems were already solved in [4] for arbitrary sequences (not only those linearly generated), but [4] did not give any insights in any way of constructing such cycles (apart from brute force). In this paper, we demonstrated that *all* lengths are also realizable using LFSRs, and an *efficient* construction algorithm for the smallest possible size is provided.

Going through the solution, this 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 comes (results from Propositions 3.1 and 3.2, Corollary 3.3, and Lemmas 3.4 and 3.5), where the lengths obtainable by a given LFSR when moving the seed are analyzed. Out of this analysis, we produce an algorithm for constructing an LFSR of the smallest possible size and a seed that expands a sequence of the prescribed length (Theorem 3.7). The algorithm is explicitly written in Section IV, which is particularized to the binary case. Finally, this paper develops a classical example, namely the design of a connection polynomial and a seed for an LFSR expanding a cyclic sequence of exactly 360 positions in length and using the minimum possible number of reading sensors. This is also compared with the result of a brute-force search among non-LFSRs. The implementation of this method in a real sensor is out of the scope of this paper and will be carried out in a future contribution.

Acknowledgment

The authors would like to thank J. J. Egozcue for originally putting into contact J. M. Fuertes and E. Ventura (an engineer and a mathematician, respectively) with regard to the problem addressed here. E. Ventura would like to thank the Centre de Recerca Matemàtica, Barcelona, Spain, for the warm hospitality during the academic course 2004–2005, which is when this paper was written.

References

[1] B. Arazi, "Position recovery using binary sequences," *Electron. Lett.*, vol. 20, no. 2, pp. 61–62, Jan. 1984.

[2] S. W. Golomb, *Shift Register Sequences*. Laguna Hills, CA: Aegean Park, 1982.

[3] M. Goresky and A. M. Klapper, "Fibonacci and Galois representations of feedback-with-carry shift registers," *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2826–2836, Nov. 2002.

[4] A. Lempel, "m-ary closed sequences," *J. Comb. Theory*, vol. 10, pp. 253–258, 1971.

[5] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and Its Applications*, vol. 20. Cambridge, U.K.: Cambridge Univ. Press, 1983.

[6] F. J. MacWilliams and N. J. A. Sloane, "Pseudo-random sequences and arrays," *Proc. IEEE*, vol. 64, no. 12, pp. 1715–1729, Dec. 1976.

[7] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Norwell, MA: Kluwer, 1987.

[8] E. M. Petriu, "Absolute-type pseudo-random shaft encoder with any desired resolution," *Electron. Lett.*, vol. 21, no. 5, pp. 215–216, Feb. 1985.
[9] E. M. Petriu, "Absolute-type position transducers using a pseudo-random encoding," *IEEE Trans. Instrum. Meas.*, vol. IM-36, no. 4, pp. 950–955, Dec. 1987.
[10] E. M. Petriu, "Scanning method for absolute pseudorandom position encoders," *Electron. Lett.*, vol. 24, no. 19, pp. 1236–1237, Sep. 1988.
[11] E. Ventura, "Dynamic structure of matrices over finite fields," in *Proc. EAMA*, Sevilla, Spain, 1997, pp. 413–420.
[12] M. Yoeli, "Binary ring sequences," *Amer. Math. Mon.*, vol. 69, no. 9, pp. 852–855, Nov. 1962.

Josep M. Fuertes (S'75–A'97–SM'05) was born in Barcelona, Spain. He received the degree in industrial engineering and the Ph.D. degree from the Technical University of Catalonia (UPC), Barcelona, in 1976 and 1986, respectively.

From 1975 to 1986, he was a Researcher with the Institut de Cibernètica (Spanish Consejo Superior de Investigaciones Científicas), Barcelona. In 1987, he became a Permanent Professor with the UPC. In 1987, he got a position for a year at the Lawrence Berkeley Laboratory, Berkeley, CA, where he was a Visiting Scientific Fellow for the design of the Active Control System of the W. M. Keck 10-m segmented telescope (Hawaii). From 1992 to 1999, he was the Director of the University Research Line in Advanced Control Systems, UPC, where he was in charge of the Distributed Control Systems Group. From 1996 to 2001, he acted as a Spanish Representative at the Council of the European Union Control Association. His research interests are in the areas of intelligent control systems and distributed control systems and applications. Since 1989, he has been coordinating projects related to the aforementioned areas of expertise, both at the national and international levels.

Dr. Fuertes is a member of the Administrative Committee of the IEEE Industrial Electronics Society and of other scientific and technical societies. He has collaborated as the Organizer (1997 IEEE International Workshop on Factory Communication Systems and 1999 IEEE International Conference on Emerging Technologies and Factory Automation), Chairman, Session Organizer, or member of program committees for several international conferences.

Borja Balle was born in Barcelona, Spain, in 1982. He received the B.S. degrees in mathematics and telecommunication engineering in 2007 from the Technical University of Catalonia (UPC), Barcelona, where he is currently working toward the M.S. degree in applied mathematics.

As an undergraduate student, he collaborated with the Department of Automatic Control and the Department of Signal Theory and Communications, UPC.

Enric Ventura was born in Barcelona, Spain. He received the degree and the Ph.D. degree, both in mathematics, from the Universitat Autònoma de Barcelona in 1988 and 1995, respectively.

In 1998, he became a Permanent Professor with the Technical University of Catalonia (UPC), Barcelona. In 2000, he received a one-year postdoctoral stay with the Mathematics Department, City College of New York. He also had a visiting position with the Mathematics Department, University of Nebraska, Lincoln, during the spring semester of 2004. In recent years, he has actively participated in the organization of several meetings and research activities in his field. He was the main organizer of the conference GAGTA (a satellite activity of the 2006 International Congress of Mathematicians), Manresa, Spain, in August 2006. In particular, he coordinated the research program "The Geometry of the Word Problem," which was developed by the Centre de Recerca Matemàtica, Barcelona, during the academic course 2004–2005 (including a program of more than 25 visitors, an advanced research course, and a conference), and also the CRM research thematic activity "Mathematics and Digital Content Security" running from September 2006 to October 2007. His main research topic is noncommutative algebra, particularly geometric and combinatorial group theory.

Dr. Ventura is a member of the Catalan Mathematical Society and the European Mathematical Society. He is the Editor of the newsletter *SCM/ Notícies* of the Catalan Mathematical Society.