Windmill Generators

A generalization and an observation of how many there are

B.J.M. Smeets¹⁾ W.G. Chambers²⁾

¹⁾ Dept of Inform. Theory
University of Lund

Box 118, S-222 46, Lund, Sweden

²⁾ Dept of Electronic and Electrical Engineering
King's College London
Strand, London, WC2R 2LS, United Kingdom

ABSTRACT

The windmill technique has several practical advantages over other techniques for high-speed generation or blockwise generation of pn-sequences. In this paper we generalize previous results by showing that if $f(t) = \alpha(t^v) - \beta(t^{-v})t^L$ is the minimal polynomial of a pn-sequence, then the sequence can be generated by a windmill generator. For $L = 1, \dots, 127$, and $v = 4, 8, 16$ such that $L \equiv \pm 3 \pmod 8$ no irreducible polynomials $f(t)$ were found. When $L \equiv \pm 1 \pmod 8$ the number of primitive $f(t)$'s was found to be approximately twice the expected number.

I INTRODUCTION

In various crypto systems m-sequence generators are used as building blocks in more complex systems. In such systems like the EBU proposal [1] for the encryption of TV-pictures, the m-sequence generators are used to generate blocks of (pseudo-)random symbols. A straightforward method to generate blocks of v , say, symbols is to operate the m-sequence generator at v times the rate at which the blocks are needed. This method, for instance, is used in the above mentioned EBU proposal. Other methods which do not require this rate increase were described, for instance, in [2], [3], [4], and [5]. The windmill technique is one of such methods. It offers several practical advantages over all the other methods.

Part of this work was supported by the National Swedish Board for Technical Development under grant 85-3759 at the University of Lund.

- No initialization problems as found in the type of generators discussed in [2].
- the generator can produce all the distinct phases of s when s is a maximal-length sequence (m-sequence) unlike the example in [4].
- The generators exhibit a structural parallelism which is useful in VLSI realizations.
- The construction of the generator is easily derived from the feedback polynomial $f(t)$ that corresponds with the generated sequence s . This makes it simple to alter the generator to let it produce a sequence s associated with another feedback polynomial.

The latter fact is very useful for cryptographic purposes because it will make it easy to use the generating polynomial as part of the key information.

In this extended abstract we describe a generalization of the windmill technique for generating m-sequences. The windmill structure is more general than the ones discussed in [3] and [5]. We state a new result that generalizes Theorem 7.4 in [5] and that gives the sufficient and necessary conditions for a feedback polynomial to be a primitive windmill polynomial. With this result it becomes easy to devise a straightforward search for all the primitive windmill polynomials.

Furthermore, we investigate the number of distinct windmill generators that can generate m-sequences of period $2^L - 1$ in blocks of size $v = 4, 8$ and 16 . When $L \equiv \pm 3 \pmod{8}$ no irreducible windmill polynomials for $L = 7, \dots, 127$. When $L \equiv \pm 1 \pmod{8}$ the number of primitive windmill polynomials was found to be approximately twice the expected number which is $2F(L)/L$, where $F(L) = \phi(2^L - 1)$. If the number of primitive windmill polynomials is small then the possibility to change easily the feedback polynomial of the generated sequence has not much value for cryptographic applications. Hence, the latter result, combined with the simple mechanism to change the generating (windmill) polynomial in a windmill generator, shows that it is realistic to use the windmill polynomials as part of the key information.

II THE WINDMILL CONFIGURATION

A windmill consists of a cyclic cascade connection of v , $v \geq 1$, linear feedback shift registers as shown in Figure 1. Each shift register together with its linear feedback polynomial and a linear feedforward network is called a vane of the windmill. The k -th vane has feedback, respectively feedforward connection described by the polynomials $\alpha(t) = 1 - \sum_{j=1}^m \alpha_j t^j$, respectively, the polynomial $\gamma_k(t) = t^{\ell(k)} \beta(t^{-1})$, where¹ $\beta(t^{-1}) = \sum_{j=0}^n \beta_j t^{-j}$ and $\ell(k)$ denotes the number of shift register stages of

¹For convenience we say that $\deg \beta(t^{-1}) = n$

Figure 1: A $[\alpha(t), \beta(t^{-1}), \ell, v, \sigma]$ windmill with v vanes.

the vane. Evidently $\ell(k) \geq \max(m, n)$. Each vane has identical $\alpha(t)$ and $\beta(t^{-1})$. The contents of the first stage of each vane is used to form a v -tuple. The manner in which the v symbols are combined to form the final v -tuple is governed by a permutation σ . The output sequence $\mathbf{z}$ is the sequence

$$\mathbf{z} = x_0^{\sigma^{-1}(0)}, \dots, x_0^{\sigma^{-1}(v-1)}, x_1^{\sigma^{-1}(0)}, \dots, x_1^{\sigma^{-1}(v-1)}, \dots, x_n^{\sigma^{-1}(0)}, \dots, x_n^{\sigma^{-1}(v-1)}, \dots$$

The whole generator is conveniently referred to as a $[\alpha(t), \beta(t^{-1}), \ell, v, \sigma]$ windmill, where

$$\underline{\ell} = (\ell(0), \dots, \ell(v-1)).$$

For each vane k , $k = 0, 1, \dots, v-1$ and $i \in \mathbb{N}$ we have the initial state, $x_0^k, x_{-1}^k, \dots, x_{-\ell(k)+1}^k$ and the recurrence relation $x_{i+1}^k = \sum_{j=1}^m \alpha_j x_{i+1-j}^k + \sum_{j=0}^n \beta_j x_{i+j-\ell(k-1)+1}^{k-1}$. Let $\mathbf{x}^k = \mathbf{x}^k(t)$ be the generating function of the sequence $(x_i^k)_{i \in \mathbb{N}}$, i.e.

$$\mathbf{x}^k = \mathbf{x}^k(t) = \sum_{i=0}^{\infty} x_i^k t^i. \quad (1)$$

The blocks of length v are consecutive blocks from a sequence $\mathbf{z}$ which is given by the expression.

$$\mathbf{z}(t) = \sum_{k=0}^{v-1} t^{\sigma(k)} \mathbf{x}^k(t^v) \quad (2)$$

In general the sequences corresponding to $\mathbf{z}(t)$ is an interleaving of v sequences each generated by LFSR's with feedback polynomial $\phi(t) = (\alpha(t))^v - t^L(\beta(t^{-1}))^v$, so that $\mathbf{z}(t)$ may be expressed as a rational-form with a denominator $\phi(t^v)$ of degree Lv , c.f. [5]. However under the conditions stated in the next theorem the rational-form simplifies considerably.

Theorem Let L, v be integers such that $1 \leq v < L$ and let L and v be relatively prime. Furthermore, let $\alpha(t)$, respectively $\beta(t^{-1})$ be two polynomials over $\text{GF}(q)$ of positive degree $m < L/v$ and $n < L/v$ respectively such that $\alpha(0) = 1$ and $\beta(0) \neq 0$. Suppose $f(t) = \alpha(t^v) - \beta(t^{-v})t^L$ is a primitive feedback polynomial over $\text{GF}(q)$. Then there exist a permutation σ of the numbers $0, 1, \dots, v-1$, and a set ℓ of length parameters given by

$$\begin{aligned}\sigma(k) &= Lk + c \pmod{v}, \\ \ell(k) &= (\sigma(k) - \sigma(k+1) + L)/v,\end{aligned}$$

for $c, k = 0, 1, \dots, v-1$ and c fixed, such that the windmill $[\alpha(t), \beta(t^{-1}), \ell, v, \sigma]$ generates the m -sequence $\mathbf{z}$ with generating function

$$\mathbf{z}(t) = \frac{\sum_{k=0}^{v-1} t^{\sigma(k)} p_k(t^v)}{f(t)},$$

where p_k is defined by equation

$$p_k = p_k(t) = x_0^k + \sum_{j=1}^m \sum_{i=1}^{j-1} \alpha_j x_{i-j}^k t^i + \sum_{j=0}^n \sum_{i=-\ell(k-1)+1}^{-j-1} \beta_j x_{i+j}^{k-1} t^{i+\ell(k-1)}$$

Before we will look at the number of $f(t)$'s of the above type which are primitive we want to make some comments. First, if the polynomial $f(t)$ in the above theorem is a primitive polynomial, then the sequence $\mathbf{z}$ is an m -sequence. Secondly, if $\deg \beta(t^{-1}) = \lfloor L/v \rfloor$ then at least one of the vanes will have its input connected by the feedforward connection to the output of the vane. Such a connection could be source of timing problems in practical applications. Windmill polynomials which do not result in such connections will be called proper windmills. A windmill is certainly proper if it satisfies the additional restriction $v(\deg \beta(t^{-1}) + 1) \leq L$. Thirdly, without loss of generality we may put $c = 0$ and hence the values of $\ell(k)$ and $\sigma(k)$ depend only on L and v . Fourthly, the theorem can easily be generalized to arbitrary polynomials of the type $f(t)$.

III The number of binary windmill polynomials

Let us call a polynomial $f(t)$ a windmill polynomial if it has the form $f(t) = \alpha(t^v) - \beta(t^{-v})t^L$, where $\alpha(t)$ and $\beta(t^{-1})$ satisfy the conditions stated in the above theorem. Those windmill polynomials which are irreducible over $\text{GF}(q)$ we call irreducible windmill polynomials and those that are even primitive we call primitive windmill polynomials, (ML=maximum length). In this section we will investigate the number of binary irreducible (and primitive) windmill polynomials. We present mainly our investigations done for values of v that are powers of 2.

The desired estimates are obtained by assuming that the windmill polynomials form a random subset of all the polynomials of degree L with $f(0) = 1$. Under

this assumption we expect to find the same fraction of windmill-type polynomials to be irreducible respectively to be primitive. We find that the number of binary windmill polynomials of degree L which satisfy the condition $f(0) = 1$ and that are irreducible should be roughly

$$\frac{2^{1+2\lfloor L/v \rfloor}}{L}.$$

For the corresponding number of primitive windmill polynomials we find the estimate

$$\frac{2^{1+2\lfloor L/v \rfloor}}{L} F(L),$$

where $F(L) = \phi(2^L - 1)/2^L = (1 - 1/2^L) \prod_p (1 - \frac{1}{p})$. In the latter formulas the p 's are the distinct prime divisors of $2^L - 1$ and ϕ is Euler's ϕ function.

We counted also the number of polynomials that were proper. The quality of our estimates is investigated by determining the exact counts for $L = 7$ to 127. We obtained the following results. When $L \equiv \pm 3 \pmod{8}$ then there are no windmill polynomials at all!. However if $L \equiv \pm 1 \pmod{8}$ the number of windmill polynomials is about twice the number we predicted by using our probabilistic model.

Recently S.D. Cohen proved that if $L \equiv \pm 3 \pmod{8}$ and L, v co-prime, then every polynomial over $\text{GF}(q^m)$, with m odd is reducible [7]. In his proof the analogue of Stickelberger's theorem over fields with characteristic two plays a similar role as in the derivation of Swan's corollary on the reducibility of binary trinomials [8].

References

- [1] European Broadcasting Union: "Specification of the systems of the MAC/packet family", Tech 3258-E (Brussels: EBU technical centre), 1986.
- [2] A. Lempel, W.L. Eastman, "High speed generation of maximal length sequences", IEEE Trans. on Comput., Vol. C-20, (1971), pp. 227-229.
- [3] A.C. Arvillias, D.G. Maritsas, "Combinational logicfree realisations for high-speed m-sequence generation", Electronics Letters, Vol.13, no.17, (1977), pp. 500-502.
- [4] F. Surböck, H. Weinrichter, "Interlacing properties of shift-register sequences with generator polynomials irreducible over $\text{GF}(p)$ ", IEEE Trans. on Inform. Theory, Vol. IT-24, (1978), pp. 386-389.
- [5] B.J.M. Smeets, *On Linear Recurring Sequences*, PhD dissertation, University of Lund, 1987.

- [6] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Vol. 20, Addison-Wesley, Reading, Mass, 1983.
- [7] S.D. Cohen, "Windmill polynomials over fields of characteristic two", preprint.
- [8] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.