Maximal frequencies of elements in second-order linear recurring sequences over a finite field

Problem

Offen bleibt die Frage, ob ein analoges Verfahren gefunden werden kann, um ähnlich reguläre Codierungen von $\mathbb{Z}^k$ anzugeben.

Mein Dank gilt den Herren J. Schmid und J. Binz, die mich bei der Ausarbeitung mit Rat und Tat unterstützt haben, sowie dem Schweizerischen Nationalfonds.

M. Wymann-Böni, Math. Institut der Universität Bern

LITERATURVERZEICHNIS

1 Cantor G.: *Ein Beitrag zur Mannigfaltigkeitslehre.* Crelles Journal f. Mathematik **84,** (1878) pp. 242–258.
2 Cantor G.: *Gesammelte Abhandlungen.* Georg Olms, Hildesheim, 1962.
3 Blatter C.: *Analysis I.* Springer, Dritte Auflage, 1980.
4 Kirsch A.: *Mathematik wirklich verstehen.* Aulis Verlag, Köln, 1987.
5 Scott D.: *Data types as lattices.* SIAM J. of Comput. **5** (1976) pp. 522–587.

 0013-6018/91/050130-10$1.50 + 0.20/0

Maximal frequencies of elements in second-order linear recurring sequences over a finite field

1. Introduction

Linear recurring sequences form a widely studied class of sequences of elements of a finite field. They have a wealth of special properties such as periodicity properties. A general exposition of the basic properties of linear recurring sequences over a finite field can be found in [2, Chapter 8]. A lot of attention has been devoted to the problem of how the elements of the underlying finite field are distributed over the period of a given linear recurring sequence. Results on the distribution behavior of linear recurring sequences are of interest in various applications, e.g. in algebraic coding theory and in the theory of pseudorandom numbers; see [2, pages 462–464] for a brief survey of the theory and the applications of distribution properties of linear recurring sequences over a finite field. In this paper we are interested in the maximal number of occurrences of a field element in a full period of a linear recurring sequence, and we shall deal mostly with the case of a second-order linear recurring sequence.
Let F_q be a finite field with q elements and characteristic p. Let $w(a,b) = (w)$ be a second-order linear recurring sequence over F_q satisfying the relation

$$w_{n+2} = a\,w_{n+1} - b\,w_n \tag{1}$$

with initial terms w_0, w_1. It is known (see [1, pages 344–345]) that if $b \neq 0$, then $w(a,b)$ is purely periodic. Throughout this paper we shall assume that $b \neq 0$. The sequence $w(a,b)$ is called *regular* if the vectors (w_0, w_1) and (w_1, w_2) are linearly independent over

F_q. If $d \in F_q$, let $A(d)$ denote the number of times that d appears in a full period of the sequence $w(a, b)$. The principal aim of this paper will be to obtain improved upper bounds for $A(d)$.
Let

$$f(x) = x^2 - ax + b \tag{2}$$

be the characteristic polynomial associated with $w(a, b)$ and let ξ_1 and ξ_2 be its characteristic roots. If $w(a, b)$ is regular, it is well-known (see [2, Theorem 8.21 and Remark 8.23]) that for $\xi_1 \neq \xi_2$,

$$w_n = \alpha_1 \xi_1^n + \alpha_2 \xi_2^n, \tag{3}$$

where $\alpha_1, \alpha_2 \in F_q(\xi_1)$ and $\alpha_1 \alpha_2 \neq 0$, and for $\xi_1 = \xi_2$,

$$w_n = (c_1 n + c_2) \xi_1^n, \tag{4}$$

where $c_1, c_2 \in F_q$ and $c_1 \neq 0$.

2. Preliminaries

Let M denote the period of $w(a, b)$. It is easy to see that all regular sequences satisfying the recursion relation (1) have the same period. (See [8, Lemma 9].) The following theorem determines the period of a regular sequence and will be necessary for our later work.

Theorem 1: *Let $w(a, b)$ be a regular sequence with characteristic roots ξ_1, ξ_2, and period M.*
(i) If $\xi_1 \neq \xi_2$, then

$$M = \operatorname{lcm}(\operatorname{ord}(\xi_1), \operatorname{ord}(\xi_2)), \tag{5}$$

where $\operatorname{ord}(\xi_1)$ denotes the multiplicative order of ξ_1 in $F_q(\xi_1)$.
(ii) *If $\xi_1 = \xi_2$, then*

$$M = p \cdot \operatorname{ord}(\xi_1). \tag{6}$$

Proof: Part (i) is proved in [7, page 606]. Part (ii) is proved in [8], Theorem 4].

Niederreiter [3] (see also [2, Theorem 8.82]) has proven the following result regarding $A(d)$ which is specialized to second-order recurrences.

Theorem 2: *Let $w(a, b)$ be a second-order linear recurring sequence over F_q for which $b \neq 0$. Let $d \in F_q$. Then*

$$\left| A(d) - \frac{M}{q} \right| \leq q - 1.$$

3. The Main Theorem

Theorem 3 will sharpen the upper bound given for $A(d)$ in Theorem 2. Note that Theorem 2 guarantees that $A(d) \geq 1$ for all $d \in F_q$ only if $w(a, b)$ has a maximal period of $q^2 - 1$.

Theorem 3: *Let $w(a, b)$ be a second-order linear recurring sequence over F_q for which $b \neq 0$. Then*

$$A(d) \leq \min(q, 2 \cdot \operatorname{ord}(b)) \tag{7}$$

for $d \neq 0$ and

$$A(0) \leq \min(q - 1, 2 \cdot \operatorname{ord}(b)). \tag{8}$$

Proof: Let $d \in F_q$. Let M be the period of $w(a, b)$. If $w(a, b)$ is irregular, then it immediately follows that $A(d) = 0$ or 1. It thus suffices to assume that $w(a, b)$ is regular.
Next we show that $A(d) \leq q$ for $d \neq 0$ and $A(0) \leq q - 1$. Note that the state vectors (w_n, w_{n+1}) are all distinct and non-zero for $0 \leq n \leq M - 1$. Consider those n, $0 \leq n \leq M - 1$, for which $w_n = d$. Then for the corresponding state vectors $(w_n, w_{n+1}) = (d, w_{n+1})$, it follows that the terms w_{n+1} must all be distinct and $w_{n+1} \neq 0$ if $d = 0$. The claim now follows.
Now let $m = \operatorname{ord}(b)$, $m_1 = \operatorname{ord}(\xi_1)$, and $m_2 = \operatorname{ord}(\xi_2)$. We shall show that for every residue $r \pmod m$, there exist at most two integers n satisfying $0 \leqq n < M$ and $n \equiv r \pmod m$ such that $w_n = d$. The theorem will then follow. We consider two cases.

Case 1: Assume that $\xi_1 \neq \xi_2$. Then by (5), $M = \operatorname{lcm}(m_1, m_2)$. If $n \equiv r \pmod m$, we obtain by (3) the equations

$$w_n = \alpha_1 \xi_1^n + \alpha_2 \xi_2^n = d, \quad \xi_1^n \xi_2^n = b^n = b^r,$$

which give for an $\varepsilon = \pm 1$,

$$\xi_1^n = \gamma_\varepsilon / \alpha_1, \quad \xi_2^n = \gamma_{-\varepsilon} / \alpha_2, \tag{9}$$

where

$$(x - \gamma_1)(x - \gamma_{-1}) = x^2 - dx + b^r \alpha_1 \alpha_2.$$

If for a fixed ε, this system of equations (9) has a solution $n_0(\varepsilon)$, then every other solution satisfies $n \equiv n_0(\varepsilon) \pmod{m_i}$ for $i = 1, 2$. Hence, $n \equiv n_0(\varepsilon) \pmod M$. Since there are two possibilities for ε, the claim follows.

Case 2: Assume that $\xi_1 = \xi_2$. Then by (6),

$$M = p m_1.$$

Further, since $\xi_1^2 = b$, we have that

$$m = \frac{m_1}{g\,c\,d(m_1, 2)}.$$

If $n \equiv r \pmod m$, we have $n \equiv r + \varepsilon m \pmod{m_1}$ for $\varepsilon = 0$ or 1. If for a fixed ε, the equation $w_n = d$ has a solution $n_0 \equiv r + \varepsilon m \pmod{m_1}$, then by (4), every other such solution satisfies

$$(c_1 n + c_2)\,\xi_1^{r+\varepsilon m} = (c_1 n_0 + c_2)\,\xi_1^{r+\varepsilon m}.$$

Hence, $n \equiv n_0 \pmod p$ since p is the characteristic of F_q. Thus, $n \equiv n_0 \pmod M$. Since there are at most two possibilities for ε, the claim follows.

Remark 1: Schinzel [4] and Somer [5] and [6] have proven this theorem for the sequences $w(a, 1)$ and $w(a, -1)$ over F_p for the case in which the initial terms are $w_0 = 0$, $w_1 = 1$. Note also that if $2 \mid q$ and $\xi_1 = \xi_2$, it follows from the proof of Theorem 3 that $A(d) \leq \operatorname{ord}(b)$ for all $d \in F_q$.

Remark 2: Let $w(a_1, a_2, \ldots, a_k)$ denote a non-zero kth-order linear recurring sequence over F_q satisfying the relation

$$w_{n+k} = a_1 w_{n+k-1} - a_2 w_{n+k-2} + \ldots + (-1)^{k+1} a_k w_n$$

with $a_k \neq 0$. It follows from an argument similar to that in the proof of Theorem 3 that

$$A(d) \leq q^{k-1}$$

for $d \neq 0$ and

$$A(0) \leq q^{k-1} - 1.$$

Remark 3: The upper bounds for inequalities (7) and (8) in Theorem 3 are the best possible and hold for a wide class of second-order linear recurring sequences. If $w(a, b)$ has a maximal period of $q^2 - 1$, then we have equality in (7) and (8), since

$$\sum_{d \in F_q} A(d) = q^2 - 1 = q(q-1) + (q-1).$$

H. Niederreiter, Institute for Information Processing, Vienna
A. Schinzel, Institute of Mathematics, Polish Acad. of Sciences, Warsaw
L. Somer, Departement of Mathematics, Catholic University of America, Washington

REFERENCES

1 Carmichael R. D.: On Sequences of Integers Defined by Recurrence Relations. Quart. J. Pure Appl. Math. *48* (1920), pp. 343–372.
2 Lidl R. and Niederreiter H.: Finite Fields. Addison-Wesley, Reading, Mass., 1983.

3 Niederreiter H.: On the Cycle Structure of Linear Recurring Sequences. Math. Scand. *38* (1976), pp. 53–77.
4 Schinzel A.: Special Lucas Sequences, Including the Fibonacci Sequence, Modulo a Prime. A Tribute to Paul Erdös (A. Baker, B. Bollobás, and A. Hajnal, eds.), pp. 349–357, Cambridge University Press, Cambridge, 1990.
5 Somer L.: Distribution of Residues of Certain Second-Order Linear Recurrences Modulo p. Applications of Fibonacci Numbers, Vol. 3 (G. E. Bergum, A. N. Philippou and A. F. Horadam, eds.), pp. 311–324, Kluwer Academic Publishers, Dordrecht, The Netherlands, 1990.
6 Somer L.: Distribution of Residues of Certain Second-Order Linear Recurrences Modulo p, II. Fibonacci Quart. *29* (1991), pp. 72–78.
7 Ward M.: The Arithmetical Theory of Linear Recurring Series. Trans. Amer. Math. Soc. *35* (1933), pp. 600–628.
8 Zierler N.: Linear Recurring Sequences. J. Soc. Ind. Appl. Math. *7* (1959), pp. 31–48.

 0013-6018/91/050139-05$1.50 + 0.20/0

Kleine Mitteilungen

Zur Übereinstimmung der Mittelwertstellen von Funktionen und ihren Ableitungen

Sei $f: \mathbb{R} \to \mathbb{R}$ eine zweimal stetig differenzierbare Funktion, für die $\operatorname{sign}(f'(x)) = c_1$ und $\operatorname{sign}(f''(x)) = c_2$ mit $c_1, c_2 \in \{-1, 1\}$ für alle $x \in \mathbb{R}$ gelte. Nach den Mittelwertsätzen der Integral- und Differentialrechnung sind dann die Mittelwertstellen $W(x,a)$ und $w(x,a)$ gemäss (1) und (2) für $x, a \in \mathbb{R}$ wohldefiniert:

$$f(W(x,a)) = \int_a^x f(s)\,ds/(x-a) \tag{1}$$

$$f'(w(x,a)) = (f(x) - f(a))/(x-a). \tag{2}$$

(Für $x = a$ sei $W(x,a) = w(x,a) = x$.)
Im allgemeinen unterscheiden sich beide Mittelwertstellen, für die Exponentialfunktion $f(x) = \exp(x)$ stimmen sie offensichtlich immer überein. Es stellt sich die Frage, für welche Funktionen f diese Stellen für jedes x und a übereinstimmen. Darüber gibt folgender Satz Auskunft:

Satz: *Für jedes $x, a \in \mathbb{R}$ gelte*

$$W(x,a) = w(x,a). \tag{3}$$

Dann gibt es $\alpha, \beta \neq 0$ und $\mu \in \mathbb{R}$ mit

$$f(x) = \alpha \exp(\beta x) + \mu.$$