JOURNAL OF COMBINATORIAL THEORY, Series A **60**, 123–130 (1992)

Note

On the Regularity of Certain 1-Additive Sequences

STEVEN R. FINCH

6 Foster Street, Wakefield, Massachusetts 01880

Communicated by the Managing Editors

Received February 10, 1990

Queneau observed that certain 1-additive sequences (defined by Ulam) are regular in the sense that differences between adjacent terms are eventually periodic. Formulas for the period in one case are herein derived, based on Niederreiter's work on the distribution properties of linear recurring sequences and subject to the truth of a highly plausible conjecture.

INTRODUCTION

Given two positive integers $u < v$, the 1-*additive sequence* with *base* $\{u, v\}$ is the infinite sequence

$$(u, v) = a_1, a_2, a_3, a_4, \ldots$$

defined by $a_1 = u$, $a_2 = v$, and, for $n > 2$,

$$a_n = \text{the smallest integer which exceeds } a_{n-1} \text{ and}$$
$$\text{which has a unique representation } a_i + a_j,\ i < j$$

(Ulam [1]). To illustrate, when $u = 1$ and $v = 2$, the next 25 terms of the sequence are 3, 4, 6, 8, 11, 13, 16, 18, 26, 28, 36, 38, 47, 48, 53, 57, 62, 69, 72, 77, 82, 87, 97, 99, 102. Note the erratic juxtaposition of short and long gaps between adjacent terms. Computer evidence (based on thousands of terms) indicates that gaps of arbitrary length exist but also that most adjacent terms differ by only 2 (see [2–4]). Such behavior contrasts with that of a related sequence: if the word "smallest" in the definition of a_n is replaced by the word "largest," then the Fibonacci sequence 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ... emerges (whose properties are well understood). Erratic behavior is likewise found in 1-additive sequences $(1, v)$ for any $v > 1$ and (2, 3).

0097-3165/92 $3.00

It comes as a surprise, therefore, that when $u=2$ and $v=5$, a pattern appears and the sequence breaks naturally into segments of 32 terms each (except for two extra terms in the initial segment shown in boldface):

2, 5, 7, 9, 11, **12**, 13, 15, 19, 23, 27, 29, 35, 37, 41, 43, 45, 49, 51, 55, 61, 67, 69, 71, 79, 83, 85, 87, 89, 95, 99, 107, 109, 119

131, 133, 135, 137, 139, 141, 145, 149, 153, 155, 161, 163, 167, 169, 171, 175, 177, 181, 187, 193, 195, 197, 205, 209, 211, 213, 215, 221, 225, 233, 235, 245

257, 259, 261, ... (Queneau [5]).

A 1-additive sequence is *regular* if successive differences $a_{n+1}-a_n$ are eventually periodic; i.e., there is a positive integer N such that $a_{N+n+1}-a_{N+n}=a_{n+1}-a_n$ for all sufficiently large n. The smallest such N is called the *period* and the value $D=a_{N+n}-a_n$ for large n is called the *fundamental difference*. Note that the asymptotic density of a regular 1-additive sequence (relative to the positive integers) is clearly N/D. Hence,

TABLE I

Parameters for the 1-Additive Sequence $(2, v)$

v	Fundamental difference D	Period N
5	$126=2(2^6-1)$	32
$7=2^3-1$	$126=2(2^6-1)$	$26=3^3-1$
9	$1778=2(2^3-1)(2^7-1)$	444
11	$6510=2(2^3-1)(2^4-1)(2^5-1)$	1628
13	$23{,}622=2(2^2-1)(2^5-1)(2^7-1)$	5906
$15=2^4-1$	$510=2(2^8-1)$	$80=3^4-1$
17	$507{,}842=2(2^5-1)(2^{13}-1)$	126,960
19	$1{,}523{,}526=2(2^2-1)(2^5-1)(2^{13}-1)$	380,882
21	$8{,}388{,}606=2(2^{22}-1)$	2,097,152
23	$4{,}194{,}302=2(2^{21}-1)$	1,047,588
25	$597{,}870=2(2^9-1)(2^{12}-1)/7$	148,814
27	$35{,}791{,}394=2(2^{28}-1)/15$	8,951,040
29	$21{,}691{,}754=2(2^{30}-1)/99$	5,406,720
$31=2^5-1$	$2046=2(2^{10}-1)$	$242=3^5-1$
33	$511{,}305{,}630=2(2^4-1)(2^{30}-1)/63$	127,842,440
35	$45{,}678{,}505{,}642=2(2^9-1)(2^{10}-1)(2^{17}-1)/3$	11,419,626,400
$63=2^6-1$	$8190=2(2^{12}-1)$	$728=3^6-1$
$127=2^7-1$	$32{,}766=2(2^{14}-1)$	$2186=3^7-1$
$255=2^8-1$	$131{,}070=2(2^{16}-1)$	$6560=3^8-1$
$511=2^9-1$	$524{,}286=2(2^{18}-1)$	$19{,}682=3^9-1$
$1023=2^{10}-1$	$2{,}097{,}150=2(2^{20}-1)$	$59{,}048=3^{10}-1$

the sequence (2, 5) is regular with $N = 32$, $D = 126$, and asymptotic density equal to $16/63 \approx 0.25397$.

Queneau [5] ascertained that the sequences (2, 7) and (2, 9) are also regular. Table I lists periods N and fundamental differences D for sequences $(2, v)$ with odd v satisfying $3 < v < 37$ and with v of the form $2^m - 1$ up to $m = 10$. (These parameters are computed using the *definition* of $(2, v)$ for only small v; computations for large v rest on the truth of Conjecture 1.) Several questions arise. Is the sequence $(2, v)$ always regular, for any odd $v > 3$? Why do N and D vary so intricately as functions of v? Are there procedures for computing N and D which are quicker than actually grinding out the terms of $(2, v)$? We can provide only partial answers to the first two questions. The answer to the third question turns out to involve linear recurring sequences and polynomial orders over finite fields.

Regularity

We wish to find conditions sufficient for an arbitrary 1-additive sequence to be regular. The fact that the regular sequence (2, 5) examined above has only two even terms is no coincidence, as first noted by Finch [6].

Theorem 1. *If a 1-additive sequence has only finitely many even terms, then the sequence is regular.*

Suppose $2c$ is the largest even term in $a_1, a_2, \ldots$. For each integer $n \geq c$, define

$$b_n = \text{the number of representations } a_i + a_j = 2n + 1, \qquad i < j$$

and, for $n \geq 2c$,

$$\beta_n = (b_{n-c}\ b_{n-c+1}\ b_{n-c+2}\ \cdots\ b_{n-1})^{\mathrm{T}},$$

a vector of c components. A formula for b_n in terms of β_n, based on the fact that a sum of two integers is odd iff precisely one of the integers is even, was derived in [6]. The sequence $\beta_{2c}, \beta_{2c+1}, \ldots$ is bounded and hence eventually periodic, from which regularity of $a_1, a_2, \ldots$ follows.

A large class of 1-additive sequences (u, v) appear to have only finitely many even terms [6]. We focus on $(2, v)$ for now in the interest of simplicity.

Conjecture 1. The sequence $(2, v)$ has precisely two even terms (specifically $a_1 = 2$ and $a_{(v+7)/2} = 2v + 2$) for odd $v > 3$.

A formula in [5] for the first $2v + 5$ terms of $(2, v)$ verifies that there are no even terms between $2v + 2$ and $7v + 7$. Substantial computer work also supports Conjecture 1, but rigorous proof seems impossible. We will *assume* it to be true for the rest of the paper.

LINEAR RECURRENCE

On the basis of the formula for b_n in [6] and Conjecture 1, we obtain

$$b_n = \delta(b_{n-1} - 1) + \delta(b_{n-v-1} - 1), \tag{1}$$

where $\delta(0) = 1$ and $\delta(r) = 0$ for $r \neq 0$. Setting $2 = 0$, i.e., immersing formula (1) not in the ring $\mathbb{Z}$ of integers but in the field $\mathbb{Z}_2$ of two elements 0, 1, clearly will not affect computation of the period N or the fundamental difference D. Formula (1) then becomes

$$b_n = b_{n-1} + b_{n-v-1} \qquad \text{(addition modulo 2)}, \tag{2}$$

a *homogeneous linear recurring sequence* [7, 8], with initial data

$$\begin{aligned}\beta_{(v+1)/2} &= (b_{-(v+1)/2} \quad b_{-(v-1)/2} \quad \cdots \quad b_{(v-3)/2} \quad b_{(v-1)/2})^{\mathrm{T}} \\ &= (0 \quad 0 \quad \cdots \quad 0 \quad 1)^{\mathrm{T}}.\end{aligned}$$

This is a very fast way to determine N and D. By formula (2), β_n must at some time return to its initial state β_p, where $p = (v+1)/2$. Suppose that this occurs for the first time when $n = q > p$, i.e., that the length of the cycle of vectors containing β_p is $q - p$. Then

$$N = \sum_{k=p-1}^{q-2} b_k \tag{3}$$

$$D = 2(q-p), \tag{4}$$

where summation of the indicator (0 or 1) variables b_k is here ordinary addition over $\mathbb{Z}$.

An alternative approach for computing N and D is based on the *characteristic polynomial* $f(x) = \det(xI + A) = x^{v+1} + x^v + 1$ associated with the linear recurrence (2), where A is the $(v+1) \times (v+1)$ *companion matrix*

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & & 0 & 0 \\ \vdots & & & & & \ddots & & \vdots \\ 0 & 0 & 0 & 0 & 0 & & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

with entries in $\mathbb{Z}_2$. The *connection* between $f(x)$ and the 1-additive sequence $(2, v)$ is the fact that

$$\beta_{n+1} = A\ \beta_n$$

for all n. The *advantage* of working with $f(x)$ is that results concerning linear feedback shift registers (which have application to random number generation and cryptography) are then available for use.

Polynomial Orders

Note that the sequence $x, x^2, x^3, x^4, \ldots$ modulo $f(x)$ is never zero and contains repetitions; hence it includes the polynomial 1. (Remember that the setting is the field $\mathbb{Z}_2$.) Thus there exists a positive integer k such that $f(x)$ divides $x^k + 1$. The least such integer k is called the *order* of $f(x)$ and is denoted by $o(v)$. Proof [7, 8] of the following result involves the fact that $f(x)$ is the *minimal* polynomial of A [9], the (obvious) linear independence of the initial vector set $\{\beta_p, \beta_{p+1}, \ldots, \beta_{p+v}\}$, and formula (4).

Theorem 2. *The fundamental difference of the* 1*-additive sequence* $(2, v)$ *is equal to twice the order of the characteristic polynomial* $f(x) = x^{v+1} + x^v + 1$; *i.e.*,

$$D(v) = 2\ o(v).$$

Tables of selected trinomial factorizations and orders over $\mathbb{Z}_2$ appear in [8, 10]. The factorizations of D found in Table I are based on the irreducible polynomial factorizations of $f(x)$. Note that $f(x)$ is square-free; i.e., it has no repeated factors, and thus its order can be shown to be equal to the least common multiple of the orders of its (pairwise relatively prime) irreducible factors [8]. Note also, from Table I, that $D(2^m - 1) = 2(2^{2m} - 1)$ for (apparently) all $m > 2$. John Riordan showed that $o(2^m - 1)$ is a *divisor* of $2^{2m} - 1$ (see [8]); proof that $o(2^m - 1)$ is in fact *equal* to $2^{2m} - 1$ is not known. More will be said about this special case $(v = 2^m - 1)$ shortly.

Period Estimates

Theorem 2 demonstrates how to compute the fundamental difference D for the 1-additive sequence $(2, v)$ with odd $v > 3$. An exact formula for the period N, short of actually implementing the linear recurrence (2) for b_n and then invoking formula (3), does not seem to be generally available.

Recent work [7] on the distribution properties of linear recurring sequences is, however, applicable. Using exponential sums in finite fields, Niederreiter [11] obtained bounds on the deviation between the *actual* count N of 1's in the sequence $b_{p-1}, b_p, \ldots, b_{q-2}$ and the obvious *estimated* count $(q-p)/2 = D/4$. (By "obvious" we mean unquestionable to a person who believes the sequence to be uniformly random.)

THEOREM 3. *The deviation between the period of the* 1*-additive sequence* $(2, v)$ *and one-fourth of its fundamental difference is bounded by* $2^{(v-1)/2}$; *i.e.*,

$$\left| N(v) - \frac{D(v)}{4} \right| \leqslant 2^{(v-1)/2}.$$

More elaborate arguments in [12] lead to a revised estimate with a tighter bound. The fact that $f(x)$ is square-free is critical here.

THEOREM 3′. *Suppose that* $f(x) = f_1(x) f_2(x) \cdots f_t(x)$, *where* $f_1(x), f_2(x), \ldots, f_t(x)$ *are* distinct *irreducible factors of degrees* $d_1, d_2, \ldots, d_t$. *Then*

$$\left| N(v) - \frac{D(v)}{4} + \frac{(-1)^t D(v)}{4(2^{d_1}-1)\cdots(2^{d_t}-1)} \right| \leqslant \left(1 - \frac{D(v)}{2(2^{d_1}-1)\cdots(2^{d_t}-1)} \right) 2^{(v-1)/2}.$$

The bound in Theorem 3′ is so tight that under some circumstances it *vanishes* and hence an exact expression for N is available. An irreducible polynomial of degree d is said to be *primitive* [7] if it has order equal to $2^d - 1$ (the maximum possible).

COROLLARY. *Under the conditions of Theorem* 3′, *if the integers* $d_1, d_2, \ldots, d_t$ *are pairwise relatively prime and if each polynomial factor* $f_i(x)$ *is primitive, then*

$$D = 2(2^{d_1}-1)\cdots(2^{d_t}-1)$$

$$N = \frac{D}{4} + \frac{(-1)^{t-1}}{2}.$$

(The fact that $2^{d_1}-1, 2^{d_2}-1, \ldots, 2^{d_t}-1$ are also pairwise relatively prime follows from [13].)

In the special case $(v = 2^m - 1)$ mentioned earlier, the conditions of the

corollary appear never to be met. In fact, from Table I, we conjecture that $N(2^m-1)=3^m-1$ for all $m>2$. Note that

$$\lim_{m\to\infty}\frac{N(2^m-1)}{D(2^m-1)}=\lim_{m\to\infty}\frac{3^m-1}{2(4^m-1)}=0;$$

i.e., belief in the uniform randomness of the recurrence (2) is certainly unwarranted for this special case when m is large. Under all other circumstances apparently $N(v)/D(v)\approx\frac{1}{4}$ to close approximation.

Closing Words

The use of tools from finite field theory to compute the period N and the fundamental difference D of a given 1-additive sequence is conditional on the number of even terms in the sequence. For a 1-additive sequence of the form $(2, v)$ with $v>3$ odd, the number of even terms is apparently two (Conjecture 1), which gives rise to the linear recurrence (2) in $\mathbb{Z}_2$. Many other 1-additive sequences likewise have only finitely many even terms [6]. We wish to provide another concrete example and a possible direction for further study.

Conjecture 2. Assume $v>3$ is odd and $v\neq 2^m-1$ for any integer m. The sequence $(4, v)$ has precisely three even terms, specifically $a_1=4$, $a_g=2v+4$, and $a_h=4v+4$, where

$$g=\begin{cases}\dfrac{v+15}{4} & \text{if } v\equiv 1 \bmod 4\\[2ex] \dfrac{v+13}{4} & \text{if } v\equiv 3 \bmod 4\end{cases}$$

$$h=\begin{cases}\dfrac{7v+41}{8} & \text{if } v\equiv 1 \bmod 8\\[2ex] \dfrac{7v+43}{8} & \text{if } v\equiv 3 \bmod 8\\[2ex] \dfrac{7v+37}{8} & \text{if } v\equiv 5 \bmod 8\\[2ex] \dfrac{7v+39}{8} & \text{if } v\equiv 7 \bmod 8\end{cases}$$

(As an aside, if $v=2^{m-1}$ for some integer $m>2$, then $(4, v)$ has one

additional even term: $a_{4\cdot 3^{m-1}+2} = 4^{m+1} - 3\cdot 2^{m+1} - 2$.) The formula for b_n (see [6]) here is

$$b_n = \delta(b_{n-2} - 1) + \delta(b_{n-v-2} - 1) + \delta(b_{n-2v-2} - 1)$$

which, when setting $3 = 0$, becomes

$$b_n = 2\{b_{n-2}(b_{n-2} + 1) + b_{n-v-2}(b_{n-v-2} + 1) + b_{n-2v-2}(b_{n-2v-2} + 1)\} \quad \text{(addition and multiplication modulo 3)},$$

a *nonlinear* recurring sequence in the field $\mathbb{Z}_3$ of three elements 0, 1, 2. Therefore, to develop a theory for $u = 4$ analogous to that for $u = 2$, one will require an understanding of nonlinear recurring sequences akin to that for the linear case.

REFERENCES

1. S. M. ULAM, "Problems in Modern Mathematics," Interscience, New York, 1964.
2. M. C. WUNDERLICH, The improbable behaviour of Ulam's summation sequence, *in* "Computers and Number Theory," pp. 249–257 (A. O. L. Atkin and B. J. Birch, Eds.), Academic Press, New York, 1971.
3. B. RECAMAN, Questions on a sequence of Ulam, *Amer. Math. Monthly* **80** (1973), 919–920.
4. R. K. GUY, "Unsolved Problems in Number Theory," Problem C4, Springer-Verlag, New York, 1981.
5. R. QUENEAU, Sur les suites s-additives, *J. Combin. Theory Ser. A* **12** (1972), 31–71, MR 46, 1741.
6. S. R. FINCH, Conjectures about s-additive sequences, *Fibonacci Quart.* **29** (1991), 209–214.
7. R. LIDL AND H. NIEDERREITER, "Finite Fields," Vol. 20, Encyclopedia of Mathematics and Its Applications, Addison-Wesley, Reading, MA, 1983.
8. S. W. GOLOMB, "Shift Register Sequences," Holden–Day, San Francisco, 1967.
9. K. HOFFMAN AND R. KUNZE, "Linear Algebra," Prentice–Hall, Englewood Cliffs, NJ, 1971.
10. N. ZIERLER, On $x^n + x + 1$ over GF(2), *Inform. and Control* **16** (1970), 502–505.
11. H. NIEDERREITER, On the cycle structure of linear recurring sequences, *Math. Scand.* **38** (1976), 53–77.
12. H. NIEDERREITER, Weights of cyclic codes, *Inform. and Control* **34** (1977), 130–140.
13. D. SHANKS, "Solved and Unsolved Problems in Number Theory," Chelsea, New York, 1978.