(around 1990)

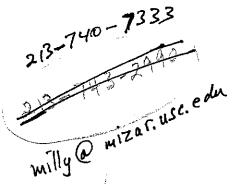
213-140-8729

DISCRETE CHAOS: Property of the property of th

Solomon W. Golomb

Communication Sciences Institute
Dept. of Electrical Engineering Systems
University of Southern California
Los Angeles, CA 90089-0272

2565



1. Historical Summary

Analogous to the Fibonacci Sequence, defined by $f_1 = f_2 = 1$, $f_n = f_{n-1} + f_{n-2}$ $\forall n > 2$, D. Hofstadter (in [1]) defined a sequence $\{q_n\}$ by $q_1 = q_2 = 1$, $q_n = q_{n-q_{n-1}} + q_{n-q_{n-2}}$, which he called a "strange" recursion, in that the subscripts depend on terms in the sequence itself. He asserted that this sequence has no discernable regularities, and this remains very nearly true.

A somewhat better behaved sequence $\{c_n\}$, proposed by J.H. Conway (private communication) is defined by $c_1 = c_2 = 1$, $c_n = c_{n-c_{n-1}} + c_{c_{n-1}}$. Unlike $\{q_n\}$, the sequence $\{c_n\}$ is monotone non-decreasing, and in fact, $d_n = c_n - c_{n-1}$ is restricted to the values 0 and 1. Regularities include: $n \ge c_n \ge \frac{n}{2}$ for all n, with $c_n = \frac{n}{2}$ iff $n = 2^k$, $k \ge 1$. Even so, $\{d_n\}$ is a good "pseudo-random" binary sequence, and appears to approximate "G-randomness" as defined in [2].

Golomb proposed the recursion $a_n = a_{n-a_{n-1}}$, with a choice of initial conditions, as a very simple example of a "strange" recursion. U. Cheng showed [3] that even in this very simple case, some quite unusual and "strange" things can happen.

The design of virtually all modern digital computers makes it easy to perform arithmetic on indices, and hence to carry out the calculation of sequences which are well-defined by a "strange" recursion and appropriate initial conditions. Some of these sequences are likely to be useful in applications where "pseudo-random" sequences of integers are required.

The theory of "strange" recursions may be regarded as the discrete case of the theory of "strange attractors," which has become very fashionable in the last few years, and which is also referred to as the theory of "chaos" [8].

2. Classical Recursions

The archetype of classical recursions is the Fibonacci sequence, defined by

$$f_n = f_{n-1} + f_{n-2}, \quad f_1 = f_2 = 1.$$
 (1)

The first forty terms of this sequence are given in Table 1, together with two different "closed-form" expressions for the n^{th} term of the sequence.

In the nineteenth century, Edouard Lucas in France described the analysis and properties of sequences satisfying any "linear recurrence" of any degree k over the real number field:

$$a_n = \sum_{j=1}^k c_j a_{n-j}.$$
 (2)

The behavior of such linear recursions has also been studied as over finite fields [4], and over polynomial rings [5]. Classes of nonlinear recursions over the real numbers have been studied in [6] and [7], and over finite fields in [4].

f :	=	f _{n-1} +f	2.3	f,	≖ f ₂	= <u>1</u>
'n		n-1	n-2		=	

n	f _n	
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 31 32 33 34 35 36 36 37 37 37 37 37 37 37 37 37 37 37 37 37	1 1 2 3 5 8 13 21 34 55 89 144 233 377 610 987 1,597 2,584 4,181 6,765 10,946 17,711 28,657 46,368 75,025 121,393 196,418 317,811 514,229 832,040 1,346,269 2,178,309 3,524,578 5,702,887 9,227,465 14,930,352	FIBONACCI'S SEQUENCE $f_n = \frac{1}{\sqrt{5}} \left\{ (\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n \right\}.$ $f_n = \sum_{1 \le j \le \left[\frac{n+1}{2}\right]} {\binom{n-j}{j-1}}.$ $I(f_n) = D(f_n) + D^2(f_n),$ $\{D^2 + D - I\} (f_n) = (0).$ $\lambda = \frac{-1 \pm \sqrt{5}}{2}.$ Other initial conditions will produce other sequences with the same characteristic equation, and with the "largest eigenvalue" $(\lambda_1 = \left \frac{-1-\sqrt{5}}{2}\right = 1.618)$
37 38 39	24,157,817 39,088,169 63,245,986	determining the asymptotic rate of growth.
40	102,334,155	defermining one asymptotic

3. Hofstadter's Sequence $\{q_n\}$

The first 280 terms of Hofstadter's sequence $\{q_n\}$ are shown in Table 2. Hofstadter's sequence has the following properties:

- 1. Unless $1 \le q_n \le n$ for all $n \ge 1$, the sequence will not be well-defined. It is almost certainly true that $1 \le q_n \le n$ for all $n \ge 1$, but no proof of this has yet been given.
- 2. The sequence is very sensitive to its initial conditions, and the given sequence is the only one which neither "blows up" (by becoming undefined) nor degenerates into a rather deterministic pattern, for the given recursion. (The subscripts can all be translated a uniform amount without affecting the sequence itself.)
 - 3. With $Q_1 = 3$, $Q_2 = 2$, $Q_3 = 1$, and Hofstadter's recursion, the resulting sequence is quasi-periodic with a quasi-period of 3:

3 2 1
3 2 1 3 5 4 3 8
3 8 7 3
3 11 10

Q _{3k+1}	- 3
Q _{3k+2}	= 3k+2
Q _{3k} -	3k-2

(It is easy to prove that this sequence satisfies the recursion, by induction.)

n.	Qn
13 14 15	3 14
15 16 17 18	13 17 16 3
18 19 20 21	3 20 19
22 23 24	3 23 22

4. If there is a limiting value l such that $\lim_{n\to\infty}\frac{q_n}{n}=l$, then $l=\frac{1}{2}$.

Proof. Assume l exists, $0 \le l \le 1$. Then for very large n, the recursion is arbitrarily well approximated by

$$ln = l(n-l(n-1)) + l(n-l(n-2))$$

$$n = (n-l(n-1)) + l(n-l(n-2))$$

$$l(n-1) + l(n-2) = n, \ 2nl - 3 = n, \ l = \frac{1}{2},$$
and since $n \to \infty$, $l = \frac{1}{2}$.

and since $n \to \infty$, $l = \frac{1}{2}$.

Apparent regularities in Hofstadter's sequence include: 5.

q ₄ =3=2+1	<i>q</i> ₇ =5	$q_3=2$:q ₁₉₂ =128	$q_5=3.$
q ₈ =5=4+1	<i>q</i> ₁₅ =10	q ₆ =4	: :q ₃₈₄ =256	<i>q</i> ₁₀ =6.
q ₁₆ =9=8+1	q ₃₁ =20	<i>q</i> ₁₂ =8	:q ₇₆₈ =512 · BUT	q_{20} =12.
q ₃₂ =17=16+1	q ₆₃ =40	q ₂₄ =16	:q ₁₅₃₆ <1024	BUT
q ₆₄ =33=32+1	BUT	q ₄₈ =32	: :q ₃₀₇₂ <2048	q ₄₀ =22.
BUT: q ₁₂₈ =64.	q ₁₂₇ =68	q ₉₆ =64	:q ₆₁₄₄ <4096	

However, none of these regularities persist!

- Statistical "regularities": $Pr\{|q_n-\frac{n}{2}|>\eta\}\to 0$ in the sense that, for fixed $\eta>0$, the fraction of the set of integers $[10^k, 10^{k+1}]$ for which $|q_n - \frac{n}{2}| > \eta$ appears to go to 0 as $k \to \infty$. Statistics have been studied for $n \le 10^6$. Nothing has been proved.
- Note the swings and oscillations around $n = 3.2^k$. E.g. $q_{186} = q_{187} = \cdots = q_{191} =$ 7. 96, $q_{192} = 128$, $q_{193} = 72$.
- The apparent regularities noted above, which do not persist, are strongly reminiscent of 8. the "chaos" in the theory of "strange attractors" [8].

q _n =	$q_{n-q_{n-1}}$	+ q _{n-q}	,	$n \geq 2$;	q ₁ :	* q ₂ =	· 1.
	.u-1		n-2				

n	q _n	n	q _n	n	q _n	n	qn	п	qn		qn	n	q _n	
1	1	41	23	81	44	121	72	161	82	201	106	241	132	
2	î	42	23	82	43	122	58	162	85	202	124	242	113	
3	2	43	24	83	43	123	61	163	84	203	82	243	133	
4	3	44	24	84	46	124	78	164	84	204	101	244	123	
5	3	45	24	85	44	125	57	165	88	205	111	245	118	
6	4	46	24	86	45	126	71	166	83	206	108	246	. 125	
7	5	47	24	87	47	127	68	167	87	207	118	247	121	
8	5	48	32	88	47	128	64	168	88	208	104	248	129	
9	6	49	24	89	46	129	63	169	87	209	108	249	122	
10	6	50	25	90	48	130	73	170	86	210	106	250	136	
11	6	51	30	91	48	131	63	171	90	211	114	25 l	129	
		52	28	92	48	132	71	172	88	212	104	252	116	
12	8	53	26	93	48	133	72	173	87	213	114	253	149	
13	8	54	30	94	48	134	72	174	92	214	109	254	137	
14 15	8	55	30	95	48	135	80	175	90	215	100	255	120	
16	9	56	28	96	64	136	61	176	91	216	109	256	123	
17	10	57	32	97	41	137	71	177	92	217	120	257	143	
18	11	58	30	98	52	138	77	178	92	218	112	258	146	
19	11	59	32	99	54	139	65	179	94	219	108	.259	107	_
	12	60	32	100	56	140	80	180	92	220	118	260	139	HOFSTADTER'S
20		61	32	101	48	141	71	181	93	221	106	2ól	138	SEQUENCE
21	12		32	102	54	142	69	182	94	222	105	262	139	30000.10.2
22	12	62 63	40	103	54	143	77	183	94	223	130	263	135	
23	12 16	64	33	104	50	144	75	184	96	224	110	264	120	
24	14	65	31	105	60	145	73	185	94	225	114	265	146	<u> </u>
25	14	66	38	106	52	146	77	186	95	226	115	265	135	
26	16	67	35	107	54	147	79	187	96	227	112	267	143	
27		68	33	108	58	148	76	188	96	228	107	268	129	
28	16		39	109	60	149	80	189	96	229	120	269	151	
29	16	69	40	110	53	150	79	190	96	230	114	270	133	i -
30	16	70		111	60	151	75	191	96	231	122	271	135	!
31	20	71	37	112	60	152	82	192	128	232	121	272	136	
32	17	72	38	113	52	153	77	193	72	233	120	273	148	1] }
33	17	73	40	114	62	154	80	194	96	234	114	274	148	
34	20	74	39	115	66	155	80	195	115	235	138	275	136	[!
35	21	75	40	1 1	55	156	78	196	100	236	110	276	144	li
36	19	76	39	116	62	It	83	197	84	237	122	277	143	
37	20	77	42	117	1	157		1	114	238	119	278	152	
38	22	78	40	118	68	158	83	198	110	239	120	279	129	
39	21	79	41	119	62	159	78	199	1	240	130	280	139	
40	22	80	43	120	58	160	85	200	93	1 240	1 , 30	1	1,3,	<u>II</u>

TABLE 2

1

4. Conway's Sequence $\{c_n\}$

The first 160 terms of Conway's sequence $\{c_n\}$ are given in Table 3. This sequence has the following *provable* regularities:

Properties of Conway's Sequence $\{c_n\}$

- 1. $\{c_n\}$ is monotonic non-decreasing.
- 2. In fact, $c_{n+1} c_n = 0$ or 1, for all n.
- 3. Fact 2 is proved by induction, using the further fact that: of the two summands which combine to form c_{n+1} , one of them is one of the two summands for c_n , and the other is the other summand of c_n with its argument advanced by 1. To illustrate:

$$c_{100} = c_{56} + c_{100-56} = c_{56} + c_{44} = 31 + 26 = 57,$$
Hence, $c_{101} = c_{57} + c_{101-57} = c_{57} + c_{44} = 31 + 26 = 57,$
and $c_{102} = c_{57} + c_{102-57} = c_{57} + c_{45} = 31 + 26 = 57.$

- 4. $\{d_n\} = \{c_{n+1} c_n\}$ is a reasonable pseudo-random binary sequence, especially in view of Fact 5.
- 5. $c_n \ge \frac{n}{2}$ for all $n \ge 1$, with $c_n = \frac{n}{2}$ iff $n = 2^k$, k = 1, 2, 3, 4, 5, ...
- 6. $\{d_n\}$ has arbitrarily long runs of 0's (e.g. terminating at the values $n=2^k$, $\{d_n\}$ has $\geq k-1$ consecutive 0's; followed by $\geq k$ consecutive 1's) and of 1's.
- 7. $\lim_{n\to\infty} \frac{c_n}{n}$ exists and equals ½. (The second part follows from Fact 5.)
- 8. Formulas can be given for c_n by relating n to the "nearest" power of 2.

9. The sequence $\{d_n\}$ seems to closely approximate "G-randomness", as defined in [2], based on the "randomness properties" of Chapter 3 of [4].

10. In the terminology of "strange attractor" theory, Conway's sequence $\{c_n\}$ is "tamely

chaotic") while Hofstadter's sequence $\{q_n\}$ is "wildly chaotic".

Reiter furnive in Phis

CONWAY'S SEQUENCE:	c _n = c _{n-c}	+c n-1 n-1	c ₁ =	c ₂ =	l.
--------------------	-----------------------------------	---------------	------------------	------------------	----

n	c _n	ກ	· cn	n	c _n	n	c _n
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 22 23 24 25 26 27 28 29 30 30 30 30 30 30 30 30 30 30 30 30 30	1 1 1 2 2 3 4 4 4 5 6 7 7 8 8 8 9 10 11 12 12 13 14 14 15 15 16 16 16 16 17 18 19 20 21 21 21 21 21 21 21 21 21 21 21 21 21	41 42 43 44 45 46 47 48 49 55 55 55 55 55 55 56 66 67 68 67 77 77 77 77 77 77 78 79 80	24 24 25 26 27 27 28 29 30 30 31 31 32 32 32 32 32 33 34 35 36 37 38 39 40 42 43 44 45 45	81 82 83 84 85 86 87 88 89 91 92 93 94 95 97 98 99 100 101 102 103 104 105 106 107 108 110 111 112 113 114 115 116 117 118 119 120	4677888901123334445566777788889001112222333344456666666666666666666666666666	121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160	63 64 64 64 64 64 64 65 66 70 71 72 73 74 75 76 77 78 80 81 82 83 84 85 86 86 87 89

5. The Recursion $a_n = a_{n-a_{n-1}}$

This simple-looking one-term "strange" recursion hides a great wealth of behaviors, which depend on the initial conditions which are used. Three simple examples are shown below.

I. $\begin{cases}
a_1 & 2 \\
a_2 & 5 \\
a_3 & 2
\end{cases}$ $\begin{array}{c|cccc}
a_4 & 5 \\
a_5 & a_0^{4}
\end{array}$

III. $\begin{array}{|c|c|c|c|c|c|}
\hline
 & a_1 & 2 \\
 & a_2 & 3 \\
 & a_3 & 2 \\
\hline
 & a_4 & 3 \\
 & a_5 & 3 \\
 & a_6 & 2 \\
 & a_7 & 3 \\
 & a_8 & 3 \\
 & a_9 & 2 \\
 & a_{10} & 3 \\
 & a_{12} & 2 \\
\hline
\end{array}$

Observations:

1. Not all initial conditions lead to well-defined sequences.

IĮ.

- 2. If the sequence is well-defined from the initial conditions, it will be <u>ultimately periodic</u>; and it can never have any term which did not already appear as a value among the initial conditions.
- 3. Proof of the "ultimately periodic" property:

Let $\{a_1, a_2, \ldots, a_{n_0}\}$ be a "proper initial condition", so that $\{a_n\}$ is defined for all $n \ge 1$. The possible values for any a_n are the distinct integers (say k of them) in the set

 $\{a_1,a_2,\ldots,a_{n_0}\}$. Let m be the largest of these. Then a_n (for $n>n_0$) is uniquely determined by the m-tuple $(a_{n-m},a_{n-m+1},\ldots,a_{n-1})$. The total number of m-tuples of k distinct integers is m^k . Hence there are integers n_1 and p, $1 \le n_1 \le k^m + m$, and $1 \le p \le k^m$, such that $a_n = a_{n-p}$ for all $n>n_1$.

Constructing Cycles with Long Periods, for $a_n = a_{n-a_{n-1}}$ FIRST EXAMPLES, for p=9.

First Step: (9,9,9,9,9,9,9,9,9). p=1, m=9, k=1.

Second Step: (9,9,3,9,9,9,9,9,9). p=9, m=9, k=2.

Third Step: (6,9,3,6,9,9,9,9,9). p=9, m=9, k=3.

Fourth Step: (6,9,3,6,9,4,3,9,6). p=9, m=9, k=4.

Question: Can the period be bigger than the biggest term in the sequence?

Answer: Yes! (due to Unjeng Cheng [3]).

SECOND EXAMPLES, $p \ge 9$.

- #1. (6,9,3,6,3,3;6,9,6,6,3,6). p=12, m=9, k=3. Compare the "first half" and "second half" of the cycle!
- #2. (8,12,8,12,8,4,8,4;8,12,2,12,8,4,2,4). p=16, m=12, k=4.
- #3. (18,3,3;18,3,3;18,21,18;18,3,18;18,21,18,18,3,18;18,3,18;18,3,18;18,3,18;18,21,3; 18,3,3;18,21,18;18,3,18;18,3,18;18,3,18;18,21,81;18,3,18;18,21,3;18,3,3). p=54, m=21, k=3.

In general, U. Cheng showed [3] that examples exist which make p/m arbitrarily large.

6. "Strange" Recursions with Known Solutions

The simplest "strange" recursion is

$$u_{u_n}=u_n$$
,

Suppose ulassi) = u(n).

for which the most general solution is given as follows:

Let R be any non-empty subset of the positive integers. If $n \in R$, require $u_n = n$. For each $n \notin R$, arbitrarily pick a value r_n from the set R, and define $u_n = r_n$.

It is easy to prove that this is the general solution. As an example, let $R = \{2,7,10\}$, and use these values as the range of u(n) described above. For example, we could set

n	u_n	n	u_n
1.	7	7	7
2	2	8	7
3	10	9	2
4	10	10	10
5	2	11	2
6	7	12	2

We then verify:

$$n = 1, 7 = u_1 = u_{u_1} = u_7 = 7$$

 $n = 2, 2 = u_2 = u_{u_2} = u_2 = 2$
 $n = 3, 10 = u_3 = u_{u_3} = u_{10} = 10$
 $n = 4, 10 = u_4 = u_{u_4} = u_{10} = 10$

etc.

From this starting point, progressively more complicated "strange" recursions can be

$$b(b(n)+kn) = 2b(n) + kn$$

$$-14-$$

$$b(m) = 2b(m-kn) + kn$$
investigated.

For example, for any positive integer k, there is a "strange" recursion

$$2b_n + kn = b_{b_n + kn} . \tag{3}$$

As initial condition, set $b_1 = 1$, and $b_2 = 3$ if k=1 but $b_2 = 2$ for all k > 1. Then the $b_n^{(k)} = [n\alpha^{(k)}]$ The + nign is the problem doesn't sermit upigue identification of term based on preceding ones sequence given by

satisfies the recursion (3), where $\alpha^{(k)}$ is the positive root of $x^2+(k-2)x-k=0$, namely $\alpha^{(k)} = \frac{2-k+\sqrt{k^2+4}}{2}$, and [y] denotes the greatest integer $\leq y$.

Although (4) is a solution of the recursion (3), it is not the only solution. It appears to be the only monotonically increasing solution, however. Conway's sequence, which is monotone non-decreasing, is a close relative of these sequences, but is uniquely specified by its recursion and a simple initial condition. No finite initial condition is sufficient to uniquely specify the solution sequence of (3) for any given k. A. Fraenkel (private communication) suggested the study of the sequences given by (4) in this context. Fine Nie (@ wisdom.weizman

A recursion which has a much simpler solution than one might expect from its "strange" $g_n = g_{n-g_{n-1}} + 1, \quad g_1 = 1.$ appearance is

$$g_n = g_{n-g_{n-1}} + 1, \quad g_1 = 1.$$
 (5)

There is a uniquely determined solution sequence for (5), with $g_1 = 1$, $g_2 = g_3 = 2$, $g_4 = g_5 =$ $g_6 = 3$, and in general each positive integer k occurring successively k times as the value of g_n . (See Table 4.) The transitions occur after each time that n is a "triangular number,"

specifically where

$$n=\frac{g_n^2+g_n}{2}. = \frac{2m\left(3n+1\right)}{2}$$

From this, we have the quadratic equation

$$g_n^2 + g_n - 2n = 0,$$

so that for all "triangular" values of n,

$$g_n = \frac{-1 + \sqrt{8n+1}}{2} ,$$

and it is easy to show that for general n,

$$g_n = \begin{bmatrix} \frac{\sqrt{8n} + 1}{2} \end{bmatrix}, \qquad n = 2 \qquad \frac{\sigma_2}{\sigma^2}$$

where [y] denotes the greatest integer not exceeding y.

This furnishes an important example of a recursion which looks as "strange" as several others we have considered, but where the resulting sequence is completely regular and predictable. It is a challenging unsolved problem to categorize those "strange" recursions which have well-behaved, closed-form solutions.

ń	g(n)	n	g(n)	_	n	g(n)
1	1	16	6		31	8
2	2	. 17	6		32	8
3	2	18	6		33	8
4	3	19	6		34	8
5	3	20	6		35	8
6	3	21	6		36	8
7	4	22	7		37	9
8	4	23	7		38	9
9	4	24	7		39	9
10	4	25	7		40	9
11	5	26	7		41	9
12	5	27	7		42	9
13	5	28	7		43	9
14	5	29	8		44	9
15	5	30	8		45	9

TABLE 4

The Sequence $g_n = g_{n-g_{n-1}} + 1$, $g_1 = 1$

References

- D. Hofstadter, Gödel, Escher, Bach, An Eternal Golden Braid, Random House, New York, 1979.
- [2] H. Beker and F. Piper, Cipher Systems, the Protection of Communications, John Wiley and Sons, 1982.
- [3] U. Cheng, "Properties of Sequences," Ph.D. Dissertation, USC Dept. of Electrical Engineering, 1981.
- / [4] S.W. Golomb, Shift Register Sequences, Holden-Day, Inc., 1967. Revised edition, Aegean Park Press, 1982.
- [5] S.W. Golomb and A. Lempel, "Second Order Polynomial Recursions," SIAM Journal on Applied Mathematics, vol. 33, no. 4, December 1977, pp. 587-592.
- [6] S.W. Golomb, "On Certain Nonlinear Recurring Sequences," American Math. Monthly, vol. 70, no. 4, April 1963.
- [7] J.N. Franklin and S.W. Golomb, "A Function-Theoretic Approach to the Study of Nonlinear Recurring Sequences," Pacific Journal of Mathematics, February 1975.
- [8] J. Gleick, CHAOS, Penguin-Viking, 1988.

Are there measures of "randomness" (like G-random, etc, pseudorandomness)?

of so, can we relate MF sequences, we even portions of them (like blocks) to there measures, so we can eategoise how untial carditions affect their measure of randomness?