Can. J. Math. Vol. **48** (6), 1996 pp. 1154–1169

THE $3x + 1$ CONJUGACY MAP

DANIEL J. BERNSTEIN AND JEFFREY C. LAGARIAS

ABSTRACT. The $3x+1$ map T and the shift map S are defined by $T(x) = (3x+1)/2$ for x odd, $T(x) = x/2$ for x even, while $S(x) = (x-1)/2$ for x odd, $S(x) = x/2$ for x even. The $3x + 1$ conjugacy map Φ on the 2-adic integers $\mathbf{Z}_2$ conjugates S to T, *i.e.*, $\Phi \circ S \circ \Phi^{-1} = T$. The map Φ mod 2^n induces a permutation Φ_n on $\mathbf{Z}/2^n\mathbf{Z}$. We study the cycle structure of Φ_n. In particular we show that it has order 2^{n-4} for $n \geq 6$. We also count 1-cycles of Φ_n for n up to 1000; the results suggest that Φ has exactly two odd fixed points. The results generalize to the $ax + b$ map, where ab is odd.

1. **Introduction.** The $3x + 1$ problem concerns iteration of the $3x + 1$ function

$$T(x) = \begin{cases} (3x+1)/2 & \text{if } x \equiv 1 \pmod 2 \\ x/2 & \text{if } x \equiv 0 \pmod 2 \end{cases} \tag{1.1}$$

on the integers $\mathbf{Z}$. The well-known $3x+1$ Conjecture asserts that, for each positive integer n, some iterate $T^k(n)$ equals 1, *i.e.*, all orbits on the positive integers eventually reach the cycle $\{1, 2\}$.

The $3x + 1$ function (1.1) is defined on the larger domain $\mathbf{Z}_2$ of 2-adic integers. It is a measure-preserving map on $\mathbf{Z}_2$ with respect to the 2-adic measure, and it is strongly mixing, so it is ergodic; see [8]. More is true. Let $S: \mathbf{Z}_2 \longrightarrow \mathbf{Z}_2$ be the 2*-adic shift map* defined by

$$S(x) = \begin{cases} (x-1)/2 & \text{if } x \equiv 1 \pmod 2 \\ x/2 & \text{if } x \equiv 0 \pmod 2; \end{cases} \tag{1.2}$$

i.e., $S(\sum_{i=0}^{\infty} b_i 2^i) = \sum_{i=0}^{\infty} b_{i+1} 2^i$, if each b_i is 0 or 1. Then T is topologically conjugate to S: there is a homeomorphism $\Phi: \mathbf{Z}_2 \longrightarrow \mathbf{Z}_2$ with

$$\Phi \circ S \circ \Phi^{-1} = T. \tag{1.3}$$

In fact T is metrically conjugate to S: one map Φ satisfying (1.3) preserves the 2-adic measure. Thus T is Bernoulli.

The map Φ is determined by (1.3) up to multiplication on the right by an automorphism of the shift S. It is known that the automorphism group of S is isomorphic to $\mathbf{Z}/2\mathbf{Z}$, with nontrivial element $V(x) = -1 - x$. (See [6, Theorem 6.9] and the introduction to [3].) We obtain a unique function Φ by adding to (1.3) the side condition $\Phi(0) = 0$. We call Φ the $3x + 1$ *conjugacy map*. This function has been constructed several times, apparently first in [8], where Φ^{-1} is denoted Q_∞, and also in [1], [2].

Received by the editors January 26, 1995.
AMS subject classification: 11B75.

https://doi.org/10.4153/CJM-1996-060-x Published online by Cambridge University Press

An important property of Φ is that it is solenoidal. Here we say that a function f on $\mathbf{Z}_2$ is *solenoidal* if, for every n, it induces a function mod 2^n, *i.e.*,

$$x \equiv y \pmod{2^n} \Longrightarrow f(x) \equiv f(y) \pmod{2^n}.$$

This solenoidal property, together with $\Phi(0) = 0$, implies that

$$\Phi(x) \equiv x \pmod 2. \tag{1.4}$$

For completeness, we give a self-contained proof that Φ is unique. Let Φ and Φ' be two invertible functions satisfying (1.3) and (1.4). Write Q and Q' for their inverses. Then $S\circ Q = Q\circ T$ and $S\circ Q' = Q'\circ T$, and (1.4) gives $Q \equiv Q' \pmod 2$. If $Q \equiv Q' \pmod{2^k}$ then $Q\circ T = Q'\circ T \pmod{2^k}$, so $S\circ Q \equiv S\circ Q' \pmod{2^k}$. Now $S\circ Q$ and $S\circ Q'$ agree in the bottom k bits, and Q and Q' agree in the bottom bit, so Q and Q' agree in the bottom $k+1$ bits. Hence $Q \equiv Q' \pmod{2^{k+1}}$. By induction $Q \equiv Q' \pmod{2^k}$ for every k, so $Q = Q'$, so $\Phi = \Phi'$.

There is an explicit formula for Φ^{-1} ([8]). Let T^m denote the m-th iterate of T. Then

$$\Phi^{-1}(x) = \sum_{i=0}^{\infty} \big(T^i(x) \bmod 2\big) 2^i. \tag{1.5}$$

This implies (1.3) and (1.4), and also shows that Φ^{-1} is solenoidal.

There is also an explicit formula for Φ ([2]). For $x \in \mathbf{Z}_2$, expand x as

$$x = \sum_l 2^{d_l},$$

in which $\{d_l\}$ is a finite or infinite sequence with $0 \le d_1 < d_2 < \cdots$. Then

$$\Phi(x) = -\sum_l 3^{-l} 2^{d_l}. \tag{1.6}$$

This also implies (1.3) and (1.4), and shows that Φ is solenoidal.

Various properties of the $3x+1$ map under iteration can be formulated in terms of properties of Φ. The $3x+1$ Conjecture is reformulated as follows ([2], [8]). Here $\mathbf{Z}^+$ denotes the positive integers.

$3x+1$ CONJECTURE. $\mathbf{Z}^+ \subseteq \Phi(\frac{1}{3}\mathbf{Z})$.

Furthermore, it is known that $\Phi(\mathbf{Q}\cap\mathbf{Z}_2) \subseteq \mathbf{Q}\cap\mathbf{Z}_2$. (This is easily proven from (1.6); see [2].) The following conjecture is proposed in [8].

PERIODICITY CONJECTURE. $\Phi(\mathbf{Q}\cap\mathbf{Z}_2) = \mathbf{Q}\cap\mathbf{Z}_2$.

This would imply that the $3x+1$ function T has no divergent trajectories on $\mathbf{Z}$. Recall that a trajectory $\{T^k(n) : k \ge 1\}$ is *divergent* if it contains an infinite number of distinct elements, so that $|T^k(n)| \longrightarrow \infty$ as $k \longrightarrow \infty$. In fact, if

$$T_{3,k}(x) = \begin{cases} (3x+k)/2 & \text{if } x \equiv 1 \pmod 2, \\ x/2 & \text{if } x \equiv 0 \pmod 2, \end{cases}$$

https://doi.org/10.4153/CJM-1996-060-x Published online by Cambridge University Press

then the Periodicity Conjecture is equivalent to the assertion that, for all $k \equiv \pm 1 \pmod 6$, the $3x + k$ function has no divergent trajectories on $\mathbf{Z}$. (This follows from [9, Corollary 2.1b].)

This paper studies the $3x + 1$ conjugacy map Φ for its own sake. The function Φ is a solenoidal bijection; it induces permutations Φ_n of $\mathbf{Z}/2^n\mathbf{Z}$. Our object is to determine properties of the cycle structure of the permutations Φ_n. In effect, our results give information about the iterates Φ^k of Φ. We prove in particular that Φ_n contains three "long" cycles of length 2^{n-4}, for all $n \geq 6$.

We remark that the results we prove are not related to the $3x + 1$ Conjecture in any immediate way; indeed for the iterates T^k the conjugacy (1.3) gives $\Phi \circ S^k \circ \Phi^{-1} = T^k$, a relation which does not involve Φ^k for any $k \geq 2$. We do note that the Periodicity Conjecture is equivalent, for any $k \geq 1$, to the assertion that $\Phi^k(\mathbf{Q} \cap \mathbf{Z}_2) = \mathbf{Q} \cap \mathbf{Z}_2$. Consequently information about Φ^k may conceivably prove useful in resolving the Periodicity Conjecture.

The contents of the paper are as follows. In Section 2 we give a table of the cycle lengths of Φ_n for $n \leq 20$. This table motivated our results. We also give data on 1-cycles of Φ_n for $n \leq 1000$. We conjecture that Φ has exactly two odd fixed points. In Section 3 we formulate results on the progressive stabilization of the "long" cycles of Φ_n. In Section 4 we generalize these results to the conjugacy map for the $ax + b$ function

$$T_{a,b}(x) = \begin{cases} (ax+b)/2 & \text{if } x \equiv 1 \pmod 2 \\ x/2 & \text{if } x \equiv 0 \pmod 2), \end{cases}$$

where ab is odd. We prove all these results in Section 5. The proofs are based on Theorem 5.1, which keeps track of the highest-order significant bit in the orbit of $x \bmod 2^{n+2}$. In Section 6 we reconsider "short" cycles of Φ_n, and present a heuristic argument that relates their asymptotics to the number of global periodic points. This heuristic is consistent with the data on 1-cycles presented in Section 2.

There are two appendices on solenoidal maps. Appendix A shows the equivalence of "solenoidal bijection," "solenoidal homeomorphism," and "2-adic isometry." Appendix B shows that a wide class of functions U generalizing the $3x + 1$ map T are conjugate to the 2-adic shift S by a solenoidal conjugacy map Φ_U.

Finally, we note that, for odd k, the map $Q(x) = kx$ conjugates the $3x+1$ function to the $3x + k$ function; *i.e.*, $Q \circ T \circ Q^{-1} = T_{3,k}$. Thus the cycle structure of the permutations mod 2^n of all the conjugacy maps $\Phi_{3,k}$ are identical. Other properties of the $3x + 1$ conjugacy map appear in [2], [10], [11]. In particular, Φ and Φ^{-1} are nowhere differentiable on $\mathbf{Z}_2$; see [10], [2].

We thank Mike Boyle and Doug Lind for supplying references concerning the automorphism group of the one-sided shift, and the referee for helpful comments.

2. **Empirical Data and Two Conjectures.** By (1.4), Φ_n takes odd numbers to odd numbers. Let $\hat{\Phi}_n \colon (\mathbf{Z}/2^n\mathbf{Z})^* \longrightarrow (\mathbf{Z}/2^n\mathbf{Z})^*$ denote its restriction. The properties of Φ_n are completely determined by $\hat{\Phi}_n$. Indeed, $\Phi(2^j x) = 2^j \Phi(x)$ by (1.6), so the action of $\hat{\Phi}_{n-j}$ describes the action of Φ_n on odd numbers times 2^j.

n	$\hat{\Phi}_n$	order($\hat{\Phi}_n$)
2	identity	1
3	$\{1,5\}$	2
4	$\{1,5\}\{9,13\}$	2
5	$\{1,21\}\{5,17\}\{7,23\}\{9,29,25,13\}$	4
6	$\{1,21\}\{3,35\}\{5,17,37,49\}\{7,23\}\{9,29,25,13\}$ $\{19,51\}\{27,59\}\{33,53\}\{39,55\}\{41,61,57,45\}$	4

Table 2.1. Cycle structure of $\hat{\Phi}_n$, $n \leq 6$. 1-cycles are omitted.

Each $\hat{\Phi}_n$ consists of cycles of various lengths, all of which are powers of 2. (See Section 3 for a proof.) The exact form of $\hat{\Phi}_n$ for $n \leq 6$ appears in Table 2.1.

Table 2.2 below lists the number of cycles of various lengths in $\hat{\Phi}_n$ for $n \leq 20$. Let $X_{n,j}$ denote the set of cycles of $\hat{\Phi}_n$ of period 2^j, and let $|X_{n,j}|$ be the number of such cycles. From Table 2.2 we see, empirically, that

$$\text{order}(\hat{\Phi}_n) = 2^{n-4}, \quad n \geq 6. \tag{2.1}$$

We also see a progressive stabilization of the number of "long" cycles in $\hat{\Phi}_n$. In Sections 3–5 we prove both these facts.

How does $|X_{n,j}|$, the number of cycles of $\hat{\Phi}_n$ of size 2^j, behave as $n \longrightarrow \infty$, for fixed j? We give data for the simplest case $|X_{n,0}|$ of 1-cycles. Table 2.3 gives all values of $|X_{n,0}|$ for $n \leq 100$, and Table 2.4 gives values of $|X_{n,0}|$ at intervals of 10 for $n \leq 1000$. We computed the values $|X_{n,0}|$ recursively for increasing n by tracking each 1-cycle individually.

The tables show that $|X_{n,0}|$ behaves irregularly, but has a general tendency to increase. In Section 6 we present a heuristic model which suggests that

$$|X_{n,0}| \sim F_0 n \quad \text{as } n \longrightarrow \infty, \tag{2.2}$$

where F_0 is the number of odd fixed points of Φ. Comparison with Table 2.4 suggests the following conjecture.

FIXED POINT CONJECTURE. *The* $3x + 1$ *conjugacy map* Φ *has exactly two odd fixed points.*

We searched for odd rational fixed points, and immediately found two: $x = -1$ and $x = 1/3$. The conjecture thus asserts that these are the only odd fixed points of Φ. We do not know of any approach to determine the existence or non-existence of non-rational odd fixed points.

More generally we propose the following conjecture.

(n,j)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2																
3	2	1															
4	4	2															
5	6	3	1														
6	6	7	3														
7	8	10	3	3													
8	14	17	8	0	3												
9	14	21	18	4	0	3											
10	10	35	24	14	2	0	3										
11	12	40	37	18	12	2	0	3									
12	16	48	70	23	16	10	2	0	3								
13	26	53	79	60	24	11	10	2	0	3							
14	22	63	111	98	50	14	11	10	2	0	3						
15	18	81	129	153	84	40	11	11	10	2	0	3					
16	20	96	179	186	137	78	31	11	11	10	2	0	3				
17	18	91	242	236	207	131	61	29	11	11	10	2	0	3			
18	12	104	305	308	312	192	105	56	29	11	11	10	2	0	3		
19	16	86	375	401	432	307	152	99	54	29	11	11	10	2	0	3	
20	26	95	424	573	564	445	281	133	91	54	29	11	11	10	2	0	3

Table 2.2. Number of cycles $|X_{n,j}|$ of $\hat{\Phi}_n$ of order 2^j, $0 \le j \le n$.

3x + 1 CONJUGACY FINITENESS CONJECTURE. *For each $j \ge 0$, the $3x+1$ conjugacy map Φ has finitely many odd periodic points of period 2^j.*

We have no idea whether the $3x+1$ conjugacy map Φ has finitely many odd periodic points in total. There are examples of $ax+b$ conjugacy maps that have no odd periodic points; see Section 4.

3. **Cycle structure of Φ_n: Inert Cycles and Stable Cycles.**

There is a simple relation between the cycles of Φ_n and those of Φ_{n+1}: For $x \in \mathbf{Z}_2$, the cycle $\sigma_{n+1}(x)$ that x belongs to in Φ_{n+1} has length $|\sigma_{n+1}(x)|$ either equal to or double the length of the cycle $\sigma_n(x)$ that x belongs to in Φ_n.

This follows from a more general fact. Call a function $f_{n+1}: \mathbf{Z}/m^{n+1}\mathbf{Z} \to \mathbf{Z}/m^{n+1}\mathbf{Z}$ *consistent mod m^n* if it induces a function f_n from $\mathbf{Z}/m^n\mathbf{Z}$ to $\mathbf{Z}/m^n\mathbf{Z}$, *i.e.*, if

$$x_1 \equiv x_2 \pmod{m^n} \Longrightarrow f_{n+1}(x_1) \equiv f_{n+1}(x_2) \pmod{m^n}. \tag{3.1}$$

LEMMA 3.1. *Let $f_{n+1}: \mathbf{Z}/m^{n+1}\mathbf{Z} \to \mathbf{Z}/m^{n+1}\mathbf{Z}$ be a function which is consistent mod m^n. If x is a purely periodic point of f_{n+1} then x is a purely periodic point of f_n and*

$$|\sigma_{n+1}(x)| = k\,|\sigma_n(x)|$$

for some integer k with $1 \le k \le m$.

(k,j)	0	1	2	3	4	5	6	7	8	9
1		12	32	52	80	116	106	152	124	110
2	2	16	38	54	82	122	112	144	124	108
3	2	26	36	56	96	124	110	120	130	108
4	4	22	38	54	106	124	112	108	128	92
5	6	18	36	54	116	114	106	114	128	96
6	6	20	36	54	90	128	92	132	136	96
7	8	18	50	68	82	118	106	140	124	102
8	14	12	60	68	92	94	116	144	118	108
9	14	16	62	84	102	92	122	144	104	88
10	10	26	50	92	108	100	132	144	98	90

Table 2.3. Number of 1-cycles in $\hat{\Phi}_{10j+k}$.

(k,j)	0	1	2	3	4	5	6	7	8	9
1	10	96	380	700	844	1278	1078	1330	1944	2030
2	26	90	458	788	840	1176	1130	1142	2180	2162
3	50	116	452	916	1134	1000	1212	1170	2194	2230
4	92	156	544	780	942	914	1270	1240	2226	2128
5	108	240	574	678	874	998	1462	1346	2130	2206
6	100	278	588	908	910	1110	1476	1538	2294	2362
7	132	282	628	818	866	1172	1360	1562	2204	2354
8	144	320	634	784	932	1172	1358	1778	2184	2362
9	98	378	784	870	1060	1072	1190	1974	2114	2242
10	90	404	714	892	1150	1086	1208	1808	2056	2308

Table 2.4. Number of 1-cycles in $\hat{\Phi}_{100j+10k}$.

PROOF. The image of $\sigma_{n+1}(x)$ under projection mod m^n consists of k copies of a purely periodic orbit $\sigma_n(x)$, for some $k \geq 1$. The bound $k \leq m$ follows because any element of $\mathbf{Z}/m^n\mathbf{Z}$ has only m distinct preimages in $\mathbf{Z}/m^{n+1}\mathbf{Z}$. ■

Lemma 3.1 applies to Φ_{n+1}, because Φ is solenoidal. Since $m=2$ we have

$$|\sigma_{n+1}(x)| = k\,|\sigma_n(x)| \text{ with } k = 1 \text{ or } 2.$$

We call a cycle $\sigma_{n+1}(x)$ *split* if $|\sigma_{n+1}(x)| = |\sigma_n(x)|$, because $\sigma_n(x)$ lifts to two cycles mod 2^{n+1}, namely $\sigma_{n+1}(x)$ and $\sigma_{n+1}(x)+2^n$. If $|\sigma_{n+1}(x)| = 2\,|\sigma_n(x)|$ we call $\sigma_{n+1}(x)$ *inert*, because $\sigma_n(x)$ has lifted to a single cycle. If $\sigma_{n+1}(x)$ is an inert cycle, and $|\sigma_n(x)| = p$, then $|\sigma_{n+1}(x)| = 2p$ and

$$\Phi^p_{n+1}(x) \equiv x + 2^n \pmod{2^{n+1}}. \tag{3.2}$$

By induction on n, the length of any cycle $|\sigma_n(x)|$ is a power of 2.

We call a cycle $\sigma_n(x)$ *stable* if $\sigma_m(x)$ is an inert cycle for all $m \geq n$. If $\sigma_n(x)$ is a stable cycle, then

$$|\sigma_m(x)| = 2^{m-n+1}\,|\sigma_{n-1}(x)|, \quad m \geq n.$$

For a stable cycle $\sigma_n(x)$, Lemma 3.1 guarantees that the map Φ restricted to

$$\{y \in \mathbf{Z}_2 : y \equiv x_i \pmod{2^n} \text{ for some } x_i \in \sigma_n(x)\}$$

has no periodic points.

Our main result concerning Φ is as follows.

THEOREM 3.1. *For the* $3x+1$ *conjugacy map* Φ*, suppose that* $|\sigma_n(x)| \geq 4$ *and that* $\sigma_n(x)$ *and* $\sigma_{n+1}(x)$ *are both inert cycles. Then* $\sigma_{n+2}(x)$ *is also an inert cycle. Consequently* $\sigma_n(x)$ *is a stable cycle.*

Theorem 3.1 follows from Corollary 5.1 at the end of Section 5.

The hypothesis $|\sigma_n(x)| \geq 4$ is necessary in Theorem 3.1. For example, $\sigma_5(3) = \{3\}$, so both $\sigma_6(3) = \{3, 35\}$ and $\sigma_7(3) = \{3, 99, 67, 35\}$ are inert, but $\sigma_8(3) = \{3, 227, 195, 163\}$ is split.

COROLLARY 3.1A. order$(\hat{\Phi}_n)$ = order$(\Phi_n) = 2^{n-4}$, *for* $n \geq 6$.

PROOF. $\sigma_6(5) = \{5, 17, 37, 49\}$ is stable. ∎

We next consider Table 2.2 in light of Theorem 3.1. Again let $X_{n,j}$ denote the set of cycles of $\hat{\Phi}_n$ of period 2^j. Call $X_{n,j}$ *stabilized* if it consists entirely of stable cycles.

COROLLARY 3.1B. *Assume that all* $X_{n,n-j}$ *are stabilized for* $0 \leq j \leq k-1$*, and that* $|X_{n,n-k}| = |X_{n+1,n+1-k}| = |X_{n+2,n+2-k}|$. *Then* $X_{m,m-k}$ *is stabilized for* $m \geq n$*, and* $|X_{m,m-k}| = |X_{n,n-k}|$.

This criterion gives the stabilized region indicated in Table 2.2. For $n = 20$ over 90% of all elements in $(\mathbf{Z}/2^n\mathbf{Z})^*$ are in stable cycles.

4. The $ax + b$ Conjugacy Map.

Consider now the $ax + b$ function

$$T_{a,b}(x) = \begin{cases} (ax+b)/2 & \text{if } x \equiv 1 \pmod 2 \\ x/2 & \text{if } x \equiv 0 \pmod 2, \end{cases} \tag{4.1}$$

where ab is odd. See [4], [5], [7], and [12] for various properties of $T_{a,b}$ under iteration on $\mathbf{Z}$.

The 2-adic shift map S is conjugate to the general $ax + b$ function $T_{a,b}$ by the $ax + b$ *conjugacy map* $\Phi_{a,b}\colon \mathbf{Z}_2 \to \mathbf{Z}_2$; *i.e.*, $\Phi_{a,b} \circ S \circ \Phi_{a,b}^{-1} = T_{a,b}$. If $x = \sum_l 2^{d_l}$, where $\{d_l\}$ is a finite or infinite sequence with $0 \leq d_1 < d_2 < \cdots$, then

$$\Phi_{a,b}(x) = -b \sum_l a^{-l} 2^{d_l}; \tag{4.2}$$

see [2]. Associated to $\Phi_{a,b}$ are the permutations $\Phi_{a,b,n}$ on $\mathbf{Z}/2^n\mathbf{Z}$ obtained by reducing $\Phi_{a,b}$ mod 2^n. The following result generalizes Theorem 3.1.

THEOREM 4.1. *For the $ax + b$ conjugacy map $\Phi_{a,b}$, suppose that a cycle $\sigma_n(x)$ of $\Phi_{a,b,n}$ has $|\sigma_n(x)| \geq 4$.*

(i) If $a \equiv 1 \pmod 4$, and $\sigma_n(x)$ is an inert cycle, then $\sigma_{n+1}(x)$ is an inert cycle.

(ii) If $a \equiv 3 \pmod 4$, and $\sigma_n(x)$ and $\sigma_{n+1}(x)$ are both inert cycles, then $\sigma_{n+2}(x)$ is an inert cycle.

This theorem follows from Corollary 5.1 in Section 5. The proof actually shows that in case (i) the weaker hypothesis $|\sigma_n(x)| \geq 2$ suffices, when $b \equiv 3 \pmod 4$.

There are examples of $ax + b$ conjugacy maps $\Phi_{a,b}$ for which all cycles eventually become stable. Such $\Phi_{a,b}$ then have no odd periodic points. Using Theorem 4.1 we easily check that the $25x - 3$ conjugacy map when taken mod 32 has an odd part consisting of two stable cycles of period 8.

5. **The Highest Order Bit.** Throughout this section, $\Phi = \Phi_{a,b}$ is a general $ax + b$ conjugacy map, where a and b are odd. We analyze the high bit of the iterates of Φ mod 2^{n+2}. All earlier results follow from Theorem 5.1 below.

For $x \in \mathbf{Z}_2$, expand x as

$$x = \sum_{k=0}^{\infty} \mathrm{bit}_k(x) 2^k, \tag{5.1}$$

where $\mathrm{bit}_k(x)$ is either 0 or 1. Define the bit sums

$$\mathrm{pop}_k(x) := \sum_{j=0}^{k} \mathrm{bit}_j(x). \tag{5.2}$$

The $ax + b$ conjugacy map is then given by

$$\Phi_{a,b}(x) = \sum_{k=0}^{\infty} \frac{-b}{a^{\mathrm{pop}_k(x)}} \mathrm{bit}_k(x) 2^k, \tag{5.3}$$

by (4.2).

LEMMA 5.1. *If $y, z \in \mathbf{Z}_2$ with $z \equiv y \pmod{2^n}$, then*

$$\Phi(z) - \Phi(y) - (z - y) \equiv 2^{n+1}\Big(\frac{ab+1}{2} + \frac{b(a-1)}{2}\mathrm{pop}_{n-1}(y)\Big) \cdot \big(\mathrm{bit}_n(y) + \mathrm{bit}_n(z)\big) \pmod{2^{n+2}}. \tag{5.4}$$

PROOF. Expand $\Phi(z) - \Phi(y) \pmod{2^{n+2}}$ using (5.3). We have $\mathrm{bit}_k(z) = \mathrm{bit}_k(y)$ and $\mathrm{pop}_k(z) = \mathrm{pop}_k(y)$ for $0 \leq k \leq n-1$, so the first n terms in $\Phi(z) - \Phi(y)$ cancel. Thus

$$\Phi(z) - \Phi(y) \equiv 2^n\Big(\Big(\frac{-b}{a^{\mathrm{pop}_n(z)}}\Big)\mathrm{bit}_n(z) - \Big(\frac{-b}{a^{\mathrm{pop}_n(y)}}\Big)\mathrm{bit}_n(y)\Big) + 2^{n+1}\Big(\Big(\frac{-b}{a^{\mathrm{pop}_{n+1}(z)}}\Big)\mathrm{bit}_{n+1}(z) - \Big(\frac{-b}{a^{\mathrm{pop}_{n+1}(y)}}\Big)\mathrm{bit}_{n+1}(y)\Big).$$

Substitute $a^{-1} \equiv a \pmod 4$ in the coefficient of 2^n, and $b \equiv a^{-1} \equiv 1 \pmod 2$ in the coefficient of 2^{n+1}:

$$\begin{aligned}\Phi(z) - \Phi(y) \equiv 2^n\big(ba^{\mathrm{pop}_n(y)}\,\mathrm{bit}_n(y) - ba^{\mathrm{pop}_n(z)}\,\mathrm{bit}_n(z)\big)\\ + 2^{n+1}\big(\mathrm{bit}_{n+1}(z) - \mathrm{bit}_{n+1}(y)\big) \pmod{2^{n+2}}.\end{aligned} \tag{5.5}$$

On the other hand

$$z - y \equiv 2^n\big(\mathrm{bit}_n(z) - \mathrm{bit}_n(y)\big) + 2^{n+1}\big(\mathrm{bit}_{n+1}(z) - \mathrm{bit}_{n+1}(y)\big) \pmod{2^{n+2}}. \tag{5.6}$$

Subtract (5.6) from (5.5):

$$\Phi(z) - \Phi(y) - (z-y) \equiv 2^n\Big((ba^{\mathrm{pop}_n(y)} + 1)\,\mathrm{bit}_n(y) - (ba^{\mathrm{pop}_n(z)} + 1)\,\mathrm{bit}_n(z)\Big) \pmod{2^{n+2}}.$$

Substitute $a^k \equiv 1 + (a-1)k \pmod 4$, $\mathrm{pop}_k(x)\,\mathrm{bit}_k(x) = \big(1 + \mathrm{pop}_{k-1}(x)\big)\,\mathrm{bit}_k(x)$, and then $\mathrm{pop}_{n-1}(z) = \mathrm{pop}_{n-1}(y)$:

$$\begin{aligned}
&\Phi(z) - \Phi(y) - (z-y)\\
&\quad\equiv 2^n\bigg(\Big(b\big(1 + (a-1)\,\mathrm{pop}_n(y)\big) + 1\Big)\,\mathrm{bit}_n(y)\\
&\qquad - \Big(b\big(1 + (a-1)\,\mathrm{pop}_n(z)\big) + 1\Big)\,\mathrm{bit}_n(z)\bigg)\\
&\quad\equiv 2^n\Big(\big(ab + 1 + b(a-1)\,\mathrm{pop}_{n-1}(y)\big)\,\mathrm{bit}_n(y)\\
&\qquad - \big(ab + 1 + b(a-1)\,\mathrm{pop}_{n-1}(z)\big)\,\mathrm{bit}_n(z)\Big)\\
&\quad\equiv 2^n\big(ab + 1 + b(a-1)\,\mathrm{pop}_{n-1}(y)\big)\big(\mathrm{bit}_n(y) - \mathrm{bit}_n(z)\big)\\
&\quad\equiv 2^{n+1}\Big(\frac{ab+1}{2} + \frac{b(a-1)}{2}\,\mathrm{pop}_{n-1}(y)\Big)\big(\mathrm{bit}_n(y) - \mathrm{bit}_n(z)\big) \pmod{2^{n+2}}.
\end{aligned}$$

This is equivalent to (5.4). ∎

Now fix $x \in \mathbf{Z}_2$, and fix $n \geq 0$. Set $|\sigma_n(x)| = 2^j$ and assume from now on that

$$\sigma_{n+1}(x) \text{ is inert,} \tag{5.7}$$

so that $|\sigma_{n+1}(x)| = 2^{j+1}$. We wish to determine whether or not $\sigma_{n+2}(x)$ is inert. According to (3.2) this occurs if and only if

$$\Phi^{2^{j+1}}(x) \equiv x + 2^{n+1} \pmod{2^{n+2}}. \tag{5.8}$$

We now introduce the quantities

$$e_k[i] := \mathrm{bit}_k\big(\Phi^i(x)\big).$$

In terms of the $e_k[i]$, we have

$$\sigma_{n+2}(x) \text{ is inert} \iff e_{n+1}[0] \neq e_{n+1}[2^{j+1}], \tag{5.9}$$

by (5.8). We proceed to evaluate $e_{n+1}[2^{j+1}] - e_{n+1}[0] \bmod 2$. The main theorems of this paper are deduced from the following formula.

THEOREM 5.1. *If* $|\sigma_n(x)| = 2^j$ *and* $\sigma_{n+1}(x)$ *is an inert cycle, then*

$$e_{n+1}[2^{j+1}] - e_{n+1}[0] \equiv 1 + \frac{ab+1}{2}2^j + \frac{b(a-1)}{2}N \pmod 2, \tag{5.10}$$

where

$$N = \sum_{i=0}^{2^j-1} \mathrm{pop}_{n-1}\big(\Phi^i(x)\big). \tag{5.11}$$

PROOF. First we define $X_i = \big(\Phi^{i+1+2^j}(x) - \Phi^{i+1}(x)\big) - \big(\Phi^{i+2^j}(x) - \Phi^i(x)\big)$. Since $\sigma_{n+1}(x)$ is an inert cycle, $\Phi^{i+2^j}(x) \equiv \Phi^i(x) + 2^n \pmod{2^{n+1}}$, so, by Lemma 5.1,

$$X_i \equiv 2^{n+1}\Big(\frac{ab+1}{2} + \frac{b(a-1)}{2}\mathrm{pop}_{n-1}\big(\Phi^i(x)\big)\Big) \pmod{2^{n+2}}.$$

Adding up the X_i gives

$$\sum_{i=0}^{2^j-1} X_i \equiv 2^{n+1}\Big(\frac{ab+1}{2}2^j + \frac{b(a-1)}{2}N\Big) \pmod{2^{n+2}}. \tag{5.12}$$

Next define $Y_i = 2^n\big((e_n[i+1+2^j] - e_n[i+1]) - (e_n[i+2^j] - e_n[i])\big)$. The sum of the Y_i telescopes:

$$\sum_{i=0}^{2^j-1} Y_i = 2^n(e_n[2^{j+1}] - e_n[2^j] - e_n[2^j] + e_n[0]).$$

Since $\sigma_{n+1}(x)$ is an inert cycle, $e_n[0] = e_n[2^{j+1}] \neq e_n[2^j]$, so

$$\sum_{i=0}^{2^j-1} Y_i = 2^n(2e_n[0] - 2e_n[2^j]) \equiv 2^{n+1} \pmod{2^{n+2}}. \tag{5.13}$$

On the other hand,

$$\begin{aligned} X_i - Y_i &\equiv 2^{n+1}(e_{n+1}[i+1+2^j] - e_{n+1}[i+1] - e_{n+1}[i+2^j] + e_{n+1}[i]) \\ &\equiv 2^{n+1}(e_{n+1}[i+1+2^j] + e_{n+1}[i+1] - e_{n+1}[i+2^j] - e_{n+1}[i]). \end{aligned}$$

In this form the sum of $X_i - Y_i$ also telescopes:

$$\sum_{i=0}^{2^j-1}(X_i - Y_i) \equiv 2^{n+1}(e_{n+1}[2^{j+1}] - e_{n+1}[0]) \pmod{2^{n+2}}.$$

Comparing this sum with (5.12) and (5.13), we get

$$2^{n+1}(e_{n+1}[2^{j+1}] - e_{n+1}[0]) \equiv 2^{n+1}\Big(\frac{ab+1}{2}2^j + \frac{b(a-1)}{2}N\Big) - 2^{n+1} \pmod{2^{n+2}},$$

which implies (5.10). ∎

COROLLARY 5.1. *(i) If* $a \equiv 1 \pmod 4$, *then*

$$e_{n+1}[2^{j+1}] - e_{n+1}[0] \equiv \begin{cases} 1 \pmod 2 \text{ if } b \equiv 3 \pmod 4 \text{ or } j \geq 1 \\ 0 \pmod 2 \text{ otherwise.} \end{cases}$$

(ii) If $a \equiv 3 \pmod 4$, *and* $\sigma_n(x)$ *is inert, then*

$$e_{n+1}[2^{j+1}] - e_{n+1}[0] \equiv \begin{cases} 1 \pmod 2 \text{ if } j \geq 2, \\ 0 \pmod 2 \text{ if } j = 1. \end{cases}$$

Note that (i) proves Theorem 4.1(i), and (ii) proves Theorem 4.1(ii), using (5.9). Theorem 3.1 then follows as a special case of Theorem 4.1(ii).

PROOF. (i) Here $a \equiv 1 \pmod 4$, so the term involving N in (5.10) drops out.
(ii) Here $a \equiv 3 \pmod 4$, and $j \geq 1$, so (5.10) simplifies to

$$e_{n+1}[2^{j+1}] - e_{n+1}[0] \equiv 1 + N \pmod 2.$$

The inertness of $\sigma_n(x)$ gives

$$\mathrm{bit}_{n-1}\big(\Phi^{i+2^{j-1}}(x)\big) = 1 - \mathrm{bit}_{n-1}\big(\Phi^{i}(x)\big),$$

so

$$\mathrm{pop}_{n-1}\big(\Phi^{i+2^{j-1}}(x)\big) + \mathrm{pop}_{n-1}\big(\Phi^{i}(x)\big) \equiv 1 \pmod 2.$$

Thus

$$N = \sum_{i=0}^{2^{j-1}-1} \Big(\mathrm{pop}_{n-1}\big(\Phi^{i+2^{j-1}}(x)\big) + \mathrm{pop}_{n-1}\big(\Phi^{i}(x)\big)\Big) \equiv \sum_{i=0}^{2^{j-1}-1} 1 = 2^{j-1} \pmod 2.$$

Now (ii) follows. ∎

6. **Cycle Structure of $\hat{\Phi}_n$: Short Cycles.** We consider the behavior of "short" cycles of the $3x+1$ conjugacy map; *i.e.*, the behavior of $|X_{n,j}|$ as $n \longrightarrow \infty$ for fixed j. We describe a heuristic model which relates the asymptotics of $|X_{n,j}|$ to the number of global odd periodic points of Φ.

We first note that the odd periodic points $\mathrm{Per}^*(\Phi)$ of Φ determine the entire set $\mathrm{Per}(\Phi)$ of periodic points of Φ. The relation

$$\Phi(2x) = 2\Phi(x) \tag{6.1}$$

implies that x has period 2^j if and only if $2x$ has period 2^j. Thus

$$\mathrm{Per}(\Phi) = \{2^k x : k \geq 0 \text{ and } x \in \mathrm{Per}^*(\Phi)\}. \tag{6.2}$$

Let F_j be the number of orbits of Φ containing an odd periodic point of minimal period 2^j. The $3x+1$ Conjugacy Finiteness Conjecture of Section 2 asserts that all F_j are finite.

We obtain a simple heuristic model for the 1-cycles $X_{n,1}$ of $\hat{\Phi}_n$ by classifying them into two types: those arising by reduction mod 2^n from an odd fixed point of Φ, and all the rest. Call these "immortal" and "mortal" 1-cycles, respectively. Our heuristic model is to assume that each "mortal" 1-cycle has equal probability of splitting or remaining inert, independently of all other 1-cycles. When a "mortal" 1-cycle splits, both its progeny in $X_{n+1,1}$ are "mortal." An "immortal" 1-cycle in $X_{n,1}$ always splits, and gives rise to two 1-cycles in $X_{n+1,1}$, at least one of which is "immortal." We also assume that only F_0 "immortal" 1-cycles appear in total, *i.e.*, for all large enough n each "immortal" 1-cycle splits into one "immortal" 1-cycle and one "mortal" 1-cycle.

This model is a branching process model with two types of individuals. The expected number of individuals $Z_{n,1}$ at step n is

$$E[Z_{n,1}] = F_0 n + c_0, \tag{6.3}$$

where c_0 is a constant depending on the levels of the initial occurrences of the F_0 "immortal" 1-cycles. The empirical data in Tables 6.3 and 6.4 seem consistent with this model, with $F_0 = 2$. We know that $F_0 \geq 2$ in any case. The two "immortal" 1-cycles that we know of both appear at $n = 1$, so that if $F_0 = 2$, then $c_0 = 0$ in (6.3).

To obtain a heuristic model for $|X_{n,j}|$ when $j \geq 1$, we use a refined classification of cycles of $\hat{\Phi}_n$. A *step* consists of passing from $\hat{\Phi}_{n-1}$ to $\hat{\Phi}_n$. For $0 \leq d \leq j \leq n$ let $X_{n,j,d}$ denote the set of cycles of $\hat{\Phi}_n$ of size 2^j which have remained inert for exactly d steps. Let $Y_{n,j,d}$ denote the subset of $X_{n,j,d}$ that consists of cycles that split in going to $\hat{\Phi}_{n+1}$. Then we have

$$|X_{n+1,j,0}| = 2\sum_{d=0}^{n} |Y_{n,j,d}|$$

and

$$|X_{n+1,j+1,d+1}| = |X_{n,j,d}| - |Y_{n,j,d}|.$$

We know the following facts about these quantities:

(1) If a cycle of length at least 8 has been inert for $d \geq 2$ steps, it remains inert. Thus $|Y_{n,j,d}| = 0$ if $j \geq 3$ and $d \geq 2$.

(2) Any cycle of length 4 which has been inert for $d = 2$ steps must split; *i.e.*, $|X_{n,2,2}| = |Y_{n,2,2}|$.

(3) Any odd periodic point x of Φ of period 2^j gives rise to a cycle of period 2^j of $\hat{\Phi}_n$ for all sufficiently large n. This cycle always splits. Such cycles are in both $X_{n,j,0}$ and $Y_{n,j,0}$.

The quantity we are interested in is

$$|X_{n,j}| = \sum_{d=0}^{n} |X_{n,j,d}|.$$

The facts above imply that $|X_{n,j}|$ is entirely determined by knowledge of $|X_{m,j,0}|$, $|Y_{m,j,0}|$, and $|Y_{m,j,1}|$, for all $m \leq n$.

Our heuristic model is then to suppose the following:

https://doi.org/10.4153/CJM-1996-060-x Published online by Cambridge University Press

(1) Each cycle in $X_{n,j,1}$ has (independently) probability $1/2$ of falling in $Y_{n,j,1}$.
(2) Each "mortal" cycle in $X_{n,j,0}$ has (independently) probability $1/2$ of falling in $Y_{n,j,0}$, and if so its two progeny in $X_{n+1,j,0}$ are "mortal."
(3) Each "immortal" cycle in $X_{n,j,0}$ lies in $Y_{n,j,0}$, and one of its progeny in $X_{n+1,j,0}$ is "immortal" and the other is "mortal," with finitely many exceptions.

This is a multi-type branching process model. If $Z_{n,j}$ denotes the total number of individuals in such a process, then one may calculate that, for large n,

$$E[Z_{n,1}] = \frac{1}{4}F_0 n^2 + \left(F_1 + \frac{1}{4}F_0\right)n - F_1 + \frac{1}{2}F_0 + c_1, \tag{6.4}$$

in which c_1 is a constant depending on the initial occurrence of "immortal" cycles. (We assume that $c_0 = 0$.) For $j \geq 2$, where stable cycles may occur, the formula for $E[Z_{n,j}]$ becomes quite complicated.

It might be interesting to further compare predictions of this model for $j \geq 1$ with actual data for Φ. We know of one odd periodic cycle of Φ of length 2, namely $\{1, -1/3\}$; *i.e.*, $\Phi(1) = -1/3$ and $\Phi(-1/3) = 1$. Thus $F_1 \geq 1$.

7. Appendix A. Solenoidal Maps.

Call a map $F: \mathbf{Z}_2 \longrightarrow \mathbf{Z}_2$ *solenoidal* if, for all n,

$$x \equiv y \pmod{2^n} \Longrightarrow F(x) \equiv F(y) \pmod{2^n}. \tag{A.1}$$

An equivalent condition in terms of the 2-adic metric $|\cdot|_2$ is that F is *nonexpanding*; *i.e.*,

$$|F(x) - F(y)|_2 \leq |x - y|_2, \quad \text{all } x, y \in \mathbf{Z}_2. \tag{A.2}$$

If F_1 and F_2 are solenoidal maps, then so is $F_1 \circ F_2$.

Call a family of functions $F_n: \mathbf{Z}/2^n\mathbf{Z} \longrightarrow \mathbf{Z}/2^n\mathbf{Z}$ *compatible* if F_n agrees with F_{n-1} under projection $\pi_n: \mathbf{Z}/2^n\mathbf{Z} \longrightarrow \mathbf{Z}/2^{n-1}\mathbf{Z}$; *i.e.*, if $\pi_n \circ F_n = F_{n-1} \circ \pi_n$. A compatible family $\{F_n\}$ has an *inverse limit* $F: \mathbf{Z}_2 \longrightarrow \mathbf{Z}_2$ defined by

$$F(x) \equiv F_n(x) \pmod{2^n}, \quad \text{for all } n. \tag{A.3}$$

The term "solenoidal" is justified by the following lemma.

LEMMA A.1. *F is solenoidal if and only if F is the inverse limit of a compatible family $\{F_n\}$.*

PROOF. If F is solenoidal, then F mod 2^n induces a function $F_n: \mathbf{Z}/2^n\mathbf{Z} \longrightarrow \mathbf{Z}/2^n\mathbf{Z}$, for each n; and $\{F_n\}$ is a compatible family. The reverse implication follows from (A.3). ∎

LEMMA A.2. *Let U be the inverse limit of a compatible family $\{U_n\}$. Then the following are equivalent.*
(i) U is a bijection.
(ii) For each n, U_n is a permutation.
(iii) For each n, if $U(x) \equiv U(y) \pmod{2^n}$ then $x \equiv y \pmod{2^n}$.

PROOF. (i) $\Rightarrow$ (ii). U is surjective, so U_n is surjective.

https://doi.org/10.4153/CJM-1996-060-x Published online by Cambridge University Press

(ii) $\Rightarrow$ (i). Write $V_n = U_n^{-1}$. Then $\{V_n\}$ is a compatible family. Let V be its inverse limit. By construction $U \circ V$ is the inverse limit of identity functions, so $U \circ V$ is the identity. Similarly $V \circ U$ is the identity. Hence U is a bijection.

(ii) $\Rightarrow$ (iii). If $U(x) \equiv U(y) \pmod{2^n}$ then $U_n(x \bmod 2^n) = U_n(y \bmod 2^n)$ so $x \bmod 2^n = y \bmod 2^n$.

(iii) $\Rightarrow$ (ii). Suppose that $U_n(a) = U_n(b)$. Select x and y in $\mathbf{Z}_2$ such that $a = x \bmod 2^n$, $b = y \bmod 2^n$. Then $U_n(x \bmod 2^n) = U_n(y \bmod 2^n)$, so $U(x) \equiv U(y) \pmod{2^n}$, so $x \equiv y \pmod{2^n}$, so $a = b$. ∎

COROLLARY A.3. *The following are equivalent.*

(i) U is a solenoidal bijection.

(ii) U is a solenoidal homeomorphism.

(iii) U is a 2-adic isometry.

U is a *2-adic isometry* if $|U(x) - U(y)|_2 = |x - y|_2$.

PROOF. (i) $\Rightarrow$ (iii). U is solenoidal so $|U(x) - U(y)|_2 \leq |x-y|_2$. On the other hand, by Lemma A.1, U is an inverse limit; and U is a bijection, so $|U(x) - U(y)|_2 \geq |x-y|_2$ by Lemma A.2 (i $\Rightarrow$ iii).

(iii) $\Rightarrow$ (ii). Since $|U(x) - U(y)|_2 \leq |x-y|_2$, U is solenoidal. By Lemma A.1, U is an inverse limit; by Lemma A.2 (iii $\Rightarrow$ i), U is a bijection. Since $|U(x) - U(y)|_2 \geq |x-y|_2$, U^{-1} is solenoidal. Finally, solenoidal implies continuous.

(ii) $\Rightarrow$ (i). Immediate. ∎

8. **Appendix B. Functions Solenoidally Conjugate to the Shift.** For any two solenoidal bijections V_0, V_1 define $U_{V_0,V_1}\colon \mathbf{Z}_2 \longrightarrow \mathbf{Z}_2$ by

$$U(x) = \begin{cases} V_0(x/2) & \text{if } x \equiv 0 \pmod 2, \\ V_1\big((x-1)/2\big) & \text{if } x \equiv 1 \pmod 2. \end{cases}$$

For example, take $V_0(x) = x$ and $V_1(x) = ax+(a+b)/2$; then U_{V_0,V_1} is the $ax+b$ function.

In this appendix we show that a map is solenoidally conjugate to the 2-adic shift map S—*i.e.*, conjugate to S by a solenoidal bijection—if and only if it is of the form U_{V_0,V_1}.

LEMMA B.1. *Let V be a solenoidal bijection. If $z \equiv w \pmod{2^{m-1}}$ then $V(z) \equiv V(w) + z - w \pmod{2^m}$.*

PROOF. If $z \equiv w \pmod{2^m}$ then $V(z) \equiv V(w) \pmod{2^m}$.

If $z \equiv w + 2^{m-1} \pmod{2^m}$ then still $V(z) \equiv V(w) \pmod{2^{m-1}}$. By Corollary A.3, V is an isometry, so if $V(z) \equiv V(w) \pmod{2^m}$ then $z \equiv w \pmod{2^m}$, contradiction. Thus $V(z) \equiv V(w) + 2^{m-1} \pmod{2^m}$. ∎

LEMMA B.2. *Set $U = U_{V_0,V_1}$. Fix $m \geq 1$. If $y \equiv x + 2^m e \pmod{2^{m+1}}$ then $U(y) \equiv U(x) + 2^{m-1}e \pmod{2^m}$.*

PROOF. Put $b = x \bmod 2$; then $U(x) = V_b\big(S(x)\big)$. Also $U(y) = V_b\big(S(y)\big)$, since $y \equiv x \pmod 2$. We have $S(y) \equiv S(x) + 2^{m-1}e \pmod{2^m}$; by Lemma B.1, $V_b\big(S(y)\big) \equiv V_b\big(S(x)\big) + 2^{m-1}e \pmod{2^m}$. ∎

LEMMA B.3. *Set* $U = U_{V_0,V_1}$. *Fix* $m \geq j \geq 1$. *If* $y \equiv x + 2^m e \pmod{2^{m+1}}$ *then* $U^j(y) \equiv U^j(x) + 2^{m-j}e \pmod{2^{m-j+1}}$.

PROOF. Lemma B.2 and induction on j. ∎

LEMMA B.4. *Set* $U = U_{V_0,V_1}$. *Fix* $m \geq 1$. *If* $y \equiv x + 2^m e \pmod{2^{m+1}}$ *then* $U^m(y) \equiv U^m(x) + e \pmod 2$.

PROOF. Lemma B.3 with $j = m$. ∎

LEMMA B.5. *Set* $U = U_{V_0,V_1}$. *Fix* $b_0, b_1, b_2, \ldots \in \{0, 1\}$. *Define* $x_0 = 0$ *and* $x_{m+1} = x_m + 2^m\big(b_m - U^m(x_m)\big)$. *Then* $y \equiv x_m \pmod{2^m}$ *if and only if* $U^i(y) \equiv b_i \pmod 2$ *for* $0 \leq i < m$.

PROOF. We induct on m. For $m = 0$ there is nothing to prove.

Say $y \equiv x_{m+1} \pmod{2^{m+1}}$. Then $y \equiv x_m + 2^m\big(b_m - U^m(x_m)\big) \pmod{2^{m+1}}$; by Lemma B.4, $U^m(y) \equiv U^m(x_m) + b_m - U^m(x_m) = b_m \pmod 2$. Also $y \equiv x_m \pmod{2^m}$, so by the inductive hypothesis $U^i(y) \equiv b_i \pmod 2$ for $0 \leq i < m$.

Conversely, say $U^i(y) \equiv b_i \pmod 2$ for $0 \leq i \leq m$. By the inductive hypothesis $y \equiv x_m \pmod{2^m}$. Write $y = x_m + 2^m e$. Then $b_m \equiv U^m(y) \equiv U^m(x_m) + e \pmod 2$ by Lemma B.4. Thus $y \equiv x_m + 2^m\big(b_m - U^m(x_m)\big) = x_{m+1} \pmod{2^{m+1}}$. ∎

THEOREM B.1. *Set* $U = U_{V_0,V_1}$. *Define* $Q(x) = \sum_{m=0}^{\infty}\big(U^m(x) \bmod 2\big)2^m$. *Then* Q *is a solenoidal bijection, and* $U = Q^{-1} \circ S \circ Q$.

Thus any map of the form U_{V_0,V_1} is solenoidally conjugate to S. (See Theorem B.2 below for the converse.) Q^{-1} generalizes the $ax + b$ conjugacy map.

PROOF. Injective: Say $Q(y) = Q(x)$. Define $b_m = U^m(x) \bmod 2$; then $U^m(y) \equiv U^m(x) \equiv b_m \pmod 2$. Next define $x_0 = 0$ and $x_{m+1} = x_m + 2^m\big(b_m - U^m(x_m)\big)$. By Lemma B.5, $y \equiv x_m \pmod{2^m}$ and $x \equiv x_m \pmod{2^m}$. Thus $y \equiv x \pmod{2^m}$ for every m; *i.e.*, $y = x$.

Solenoidal: Say $y \equiv x \pmod{2^n}$. Define $b_m = U^m(x) \bmod 2$, $x_0 = 0$, and $x_{m+1} = x_m + 2^m\big(b_m - U^m(x_m)\big)$. Then $x \equiv x_n \pmod{2^n}$ by Lemma B.5, so $y \equiv x_n \pmod{2^n}$; by Lemma B.5 again, $U^m(y) \equiv b_m \pmod 2$ for $0 \leq m < n$. Thus $Q(y) \equiv Q(x) \pmod{2^n}$.

Surjective: Given $b = \sum_{i=0}^{\infty} b_i 2^i$ with $b_i \in \{0, 1\}$, define $x_0 = 0$ and $x_{m+1} = x_m + 2^m\big(b_m - U^m(x_m)\big)$. Since $x_{m+1} \equiv x_m \pmod{2^m}$ the sequence $x_1, x_2, \ldots$ converges to a 2-adic limit y, with $y \equiv x_m \pmod{2^m}$. By Lemma B.5, $U^m(y) \equiv b_m \pmod 2$ for all m. Thus $Q(y) = b$.

Finally, it is immediate from the definition of Q that $Q \circ U = S \circ Q$. ∎

THEOREM B.2. *Let* Q *be a solenoidal bijection. Define* $U = Q^{-1} \circ S \circ Q$. *Then* $U = U_{V_0,V_1}$ *for some solenoidal bijections* V_0, V_1.

PROOF. If $Q(0)$ is even then $Q^{-1}(x) \equiv x \pmod 2$ for all x; so write

$$Q^{-1}(x) = \begin{cases} 2W_0(x/2) & \text{if } x \equiv 0 \pmod 2, \\ 1 + 2W_1\big((x-1)/2\big) & \text{if } x \equiv 1 \pmod 2. \end{cases}$$

https://doi.org/10.4153/CJM-1996-060-x Published online by Cambridge University Press

Then W_0, W_1 are solenoidal bijections, and $U = U_{V_0,V_1}$ where $V_i = Q \circ W_i$.

Similarly, if $Q(0)$ is odd then $Q^{-1}(x) \equiv -1 - x \pmod 2$ for all x; so write

$$Q^{-1}(x) = \begin{cases} 1 + 2W_0(x/2) & \text{if } x \equiv 0 \pmod 2, \\ 2W_1\big((x-1)/2\big) & \text{if } x \equiv 1 \pmod 2. \end{cases}$$

Again W_0, W_1 are solenoidal bijections, and $U = U_{V_0,V_1}$ where $V_i = Q \circ W_i$. ■

References

1. E. Akin, *Why is the* 3x + 1 *problem so hard?* Math. Magazine, to appear.
2. D. J. Bernstein, *A non-iterative* 2*-adic statement of the* 3x+1 *conjecture*, Proc. Amer. Math. Soc. **121**(1994), 405–408.
3. M. Boyle, J. Franks and B. Kitchens, *Automorphisms of one-sided subshifts of finite type*, Ergod. Th. Dyn. Sys. **10**(1990), 421–449.
4. R. E. Crandall, *On the '*3x + 1*' problem*, Math. Comp. **32**(1978), 1281–1292.
5. Z. Franco and C. Pomerance, *On a conjecture of Crandall concerning the* QX + 1 *problem*, Math. Comp. **49**(1995), to appear.
6. G. Hedlund, *Endomorphisms and automorphisms of the shift dynamical system*, Math. Systems Theory **3**(1969), 320–375.
7. E. Heppner, *Eine Bemerkung zum Hasse-Syracuse Algorithmus*, Arch. Math. **31**(1978), 317–320.
8. J. C. Lagarias, *The* 3x + 1 *problem and its generalizations*, Amer. Math. Monthly **92**(1985), 3–23.
9. ———, *The set of rational cycles for the* 3x + 1 *problem*, Acta Arithmetica **56**(1990), 33–53.
10. H. Müller, *Das '*3n + 1*' Problem*, Mitteilungen der Math. Ges. Hamburg **12**(1991), 231–251.
11. ———, *Über eine Klasse* 2*-adischer Funktionen im Zussamenhang mit dem "*3x+1*"-Problem*, Abh. Math. Sem. Univ. Hamburg **64**(1994), 293–302.
12. R. P. Steiner, *On the "*QX + 1 *problem," Q odd, I, II*, Fibonacci Quart. **19**(1981), 285–288, 293–296.

Department of Mathematics
University of California
Berkeley, CA
USA 94720

current address:
Department of Mathematics,
Statistics, and Computer Science
The University of Illinois at Chicago
Chicago, IL
USA 60607–7045
email: djb@math.uic.edu

AT&T Bell Laboratories
Murray Hill, NJ
USA 07974
email: jcl@research.att.com