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 $\Phi$ on the 2-adic integers $\mathbb{Z}_2$ conjugates $S$ to $T$, i.e., $\Phi \circ S \circ \Phi^{-1} = T$. The map $\Phi \mod 2^n$ induces a permutation $\Phi_n$ on $\mathbb{Z}/2^n\mathbb{Z}$. We study the cycle structure of $\Phi_n$. In particular we show that it has order $2^{n-4}$ for $n \geq 6$. We also count 1-cycles of $\Phi_n$ for $n$ up to 1000; the results suggest that $\Phi$ 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

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

(1.1)

on the integers $\mathbb{Z}$. 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 $\mathbb{Z}_2$ of 2-adic integers. It is a measure-preserving map on $\mathbb{Z}_2$ with respect to the 2-adic measure, and it is strongly mixing, so it is ergodic; see [8]. More is true. Let $S: \mathbb{Z}_2 \to \mathbb{Z}_2$ be the 2-adic shift map defined by

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

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 $\Phi: \mathbb{Z}_2 \to \mathbb{Z}_2$ with

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

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

The map $\Phi$ 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 $\mathbb{Z}/2\mathbb{Z}$, with nontrivial element $V(x) = -1 - x$. (See [6, Theorem 6.9] and the introduction to [3].) We obtain a unique function $\Phi$ by adding to (1.3) the side condition $\Phi(0) = 0$. We call $\Phi$ the 3x + 1 conjugacy map. This function has been constructed several times, apparently first in [8], where $\Phi^{-1}$ is denoted $\mathcal{Q}_\infty$, and also in [1], [2].
An important property of $\Phi$ is that it is solenoidal. Here we say that a function $f$ on $\mathbb{Z}_2$ is solenoidal if, for every $n$, it induces a function mod $2^n$, i.e.,

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

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

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

(1.4)

For completeness, we give a self-contained proof that $\Phi$ is unique. Let $\Phi$ and $\Phi'$ 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 $\Phi^{-1}$ ([8]). Let $T^m$ denote the $m$-th iterate of $T$. Then

$$\Phi^{-1}(x) = \sum_{i=0}^{\infty} (T^i(x) \mod 2)2^i.$$ 

(1.5)

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

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

$$x = \sum d_i 2^i,$$

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

$$\Phi(x) = -\sum d_i 3^{-i} 2^i.$$ 

(1.6)

This also implies (1.3) and (1.4), and shows that $\Phi$ is solenoidal.

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

**3x + 1 Conjecture.** $\mathbb{Z}^+ \subseteq \Phi(\frac{1}{2} \mathbb{Z}).$

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

**Periodicity Conjecture.** $\Phi(\mathbb{Q} \cap \mathbb{Z}_2) = \mathbb{Q} \cap \mathbb{Z}_2.$

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

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

(1.7)
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 \( \mathbb{Z} \). (This follows from [9, Corollary 2.1b].)

This paper studies the \( 3x + 1 \) conjugacy map \( \Phi \) for its own sake. The function \( \Phi \) is a solenoidal bijection; it induces permutations \( \Phi_n \) of \( \mathbb{Z}/2^n\mathbb{Z} \). Our object is to determine properties of the cycle structure of the permutations \( \Phi_n \). In effect, our results give information about the iterates \( \Phi^k \) of \( \Phi \). We prove in particular that \( \Phi_n \) 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 \( \Phi^k \) for any \( k \geq 2 \). We do note that the Periodicity Conjecture is equivalent, for any \( k \geq 1 \), to the assertion that \( \Phi^k(Q \cap \mathbb{Z}_2) = Q \cap \mathbb{Z}_2 \). Consequently information about \( \Phi^k \) 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 \( \Phi_n \) for \( n \leq 20 \). This table motivated our results. We also give data on 1-cycles of \( \Phi_n \) for \( n \leq 1000 \). We conjecture that \( \Phi \) has exactly two odd fixed points. In Section 3 we formulate results on the progressive stabilization of the “long” cycles of \( \Phi_n \). 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 \( x \pmod{2^{n+2}} \).

In Section 6 we reconsider “short” cycles of \( \Phi_n \), 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 \( \Phi_U \).

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, \( \Phi \) and \( \Phi^{-1} \) are nowhere differentiable on \( \mathbb{Z}_2 \); 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), \( \Phi_n \) takes odd numbers to odd numbers. Let \( \Phi_n : (\mathbb{Z}/2^n\mathbb{Z})^* \rightarrow (\mathbb{Z}/2^n\mathbb{Z})^* \) denote its restriction. The properties of \( \Phi_n \) are completely determined by \( \Phi_n \). Indeed, \( \Phi(2^i x) = 2^i \Phi(x) \) by (1.6), so the action of \( \Phi_{n-j} \) describes the action of \( \Phi_n \) on odd numbers times \( 2^j \).
Each \( \Phi_n \) consists of cycles of various lengths, all of which are powers of 2. (See Section 3 for a proof.) The exact form of \( \Phi_n \) for \( n \leq 6 \) appears in Table 2.1.

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

\[
(2.1) \quad \text{order}(\Phi_n) = 2^{n-4}, \quad n \geq 6.
\]

We also see a progressive stabilization of the number of “long” cycles in \( \Phi_n \). In Sections 3–5 we prove both these facts.

How does \( |X_{n,j}| \), the number of cycles of \( \Phi_n \) of size \( 2^j \), behave as \( n \to \infty \), 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

\[
(2.2) \quad |X_{n,0}| \sim F_0 n \quad \text{as} \; n \to \infty,
\]

where \( F_0 \) is the number of odd fixed points of \( \Phi \). Comparison with Table 2.4 suggests the following conjecture.

**Fixed Point Conjecture.** The \( 3x + 1 \) conjugacy map \( \Phi \) 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 \( \Phi \). 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.
Table 2.2. Number of cycles $|X_n|$ of $\Phi_n$ of order $2^j$, $0 \leq j \leq n$.

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

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

We have no idea whether the 3x + 1 conjugacy map $\Phi$ 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 $\Phi_n$: Inert Cycles and Stable Cycles. There is a simple relation between the cycles of $\Phi_n$ and those of $\Phi_{n+1}$: For $x \in \mathbb{Z}_2$, the cycle $\sigma_{n+1}(x)$ that $x$ belongs to in $\Phi_{n+1}$ has length $|\sigma_{n+1}(x)|$ either equal to or double the length of the cycle $\sigma_n(x)$ that $x$ belongs to in $\Phi_n$.

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

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

LEMMA 3.1. Let $f_{n+1}: \mathbb{Z}/m^{n+1} \mathbb{Z} \rightarrow \mathbb{Z}/m^{n+1} \mathbb{Z}$ 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 $1 \leq k \leq m$. 
THE 3x + 1 CONJUGACY MAP

Table 2.3. Number of 1-cycles in \( \Phi_{10j+}\).

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

We call a cycle \( \sigma_n(x) \) \textit{split} if \( |\sigma_{n+1}(x)| = 2^k |\sigma_n(x)| \) with \( k = 1 \) or 2.

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

Lemma 3.1 applies to \( \Phi_{n+1} \), because \( \Phi \) 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 \( \sigma_{n+1}(x) \) \textit{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 \( \sigma_{n+1}(x) \) \textit{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

\[
\Phi^p_{n+1}(x) \equiv x + 2^n \pmod{2^{n+1}}.
\]

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

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

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

Table 2.4. Number of 1-cycles in \( \Phi_{100j+10k} \).

\[
(k,j) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 \\
---|---|---|---|---|---|---|---|---|---|---
1  | 10 | 96 | 380 | 700 | 844 | 1278 | 1078 | 1330 | 1944 | 2030 \\
2  | 26 | 90 | 458 | 788 | 840 | 1176 | 1130 | 1142 | 2180 | 2162 \\
3  | 50 | 116 | 452 | 916 | 1134 | 1000 | 1212 | 1170 | 2194 | 2230 \\
4  | 92 | 156 | 544 | 780 | 942 | 914 | 1270 | 1240 | 2226 | 2128 \\
5  | 108 | 240 | 574 | 678 | 874 | 998 | 1462 | 1346 | 2130 | 2206 \\
6  | 100 | 278 | 588 | 908 | 910 | 1110 | 1476 | 1538 | 2294 | 2362 \\
7  | 132 | 282 | 628 | 818 | 866 | 1172 | 1360 | 1562 | 2204 | 2354 \\
8  | 144 | 320 | 634 | 784 | 932 | 1172 | 1358 | 1778 | 2184 | 2362 \\
9  | 98 | 378 | 784 | 870 | 1060 | 1072 | 1190 | 1974 | 2114 | 2242 \\
10 | 90  | 404 | 714 | 892 | 1150 | 1086 | 1208 | 1808 | 2056 | 2308 \\
\]
For a stable cycle $\sigma_n(x)$, Lemma 3.1 guarantees that the map $\Phi$ restricted to
\[
\{y \in \mathbb{Z}_2 : y \equiv x_i \pmod{2^n} \text{ for some } x_i \in \sigma_n(x)\}
\]
has no periodic points.

Our main result concerning $\Phi$ is as follows.

**Theorem 3.1.** For the $3x+1$ conjugacy map $\Phi$, 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.** $\text{order}(\Phi_n) = \text{order}(\Phi_n) = 2^{n-4}$, 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 $\Phi_n$ 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 $(\mathbb{Z}/2^n\mathbb{Z})^*$ are in stable cycles.

4. The $ax + b$ Conjugacy Map. Consider now the $ax + b$ function
\[
T_{a,b}(x) = \begin{cases} 
(ax + b)/2 & \text{if } x \equiv 1 \pmod{2} \\
 x/2 & \text{if } x \equiv 0 \pmod{2},
\end{cases}
\]
where $ab$ is odd. See [4], [5], [7], and [12] for various properties of $T_{a,b}$ under iteration on $\mathbb{Z}$.

The 2-adic shift map $S$ is conjugate to the general $ax + b$ function $T_{a,b}$ by the $ax + b$ conjugacy map $\Phi_{a,b} : \mathbb{Z}_2 \to \mathbb{Z}_2$; i.e., $\Phi_{a,b} \circ S \circ \Phi_{a,b}^{-1} = T_{a,b}$. If $x = \sum 2^d$, where $\{d_i\}$ is a finite or infinite sequence with $0 \leq d_1 < d_2 < \cdots$, then
\[
\Phi_{a,b}(x) = -b \sum_{i} a^{-d_i} 2^{d_i};
\]
see [2]. Associated to $\Phi_{a,b}$ are the permutations $\Phi_{a,b,n}$ on $\mathbb{Z}/2^n\mathbb{Z}$ 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 \( \Phi \mod 2^{n+2} \). All earlier results follow from Theorem 5.1 below.

For \( x \in \mathbb{Z}_2 \), expand \( x \) as

\[
x = \sum_{k=0}^{\infty} \text{bit}_k(x)2^k,
\]

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

\[
\text{pop}_k(x) := \sum_{j=0}^{k} \text{bit}(x).
\]

The \( ax + b \) conjugacy map is then given by

\[
\Phi_{a,b}(x) = \sum_{k=0}^{\infty} \frac{-b}{a^{\text{pop}_k(x)}} \text{bit}_k(x)2^k,
\]

by (4.2).

LEMMA 5.1. If \( y, z \in \mathbb{Z}_2 \) with \( z \equiv y \pmod{2^n} \), then

\[
\Phi(z) - \Phi(y) - (z - y) \equiv 2^{n+1} \left( \frac{ab + 1}{2} + \frac{b(a - 1)}{2} \text{pop}_{n-1}(y) \right) \cdot (\text{bit}_n(y) + \text{bit}_n(z)) \pmod{2^{n+2}}.
\]

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

\[
\Phi(z) - \Phi(y) \equiv 2^n \left( \left( \frac{-b}{a^{\text{pop}_n(x)}} \right) \text{bit}_n(z) - \left( \frac{-b}{a^{\text{pop}_n(y)}} \right) \text{bit}_n(y) \right) + 2^{n+1} \left( \left( \frac{-b}{a^{\text{pop}_{n+1}(x)}} \right) \text{bit}_{n+1}(z) - \left( \frac{-b}{a^{\text{pop}_{n+1}(y)}} \right) \text{bit}_{n+1}(y) \right).
\]
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 \( 2^{n+1} \):

\[
\Phi(z) - \Phi(y) \equiv 2^n \left( ba^{\text{pop}_n(y)} \text{bit}_n(y) - ba^{\text{pop}_n(z)} \text{bit}_n(z) \right) + 2^{n+1} \left( \text{bit}_{n+1}(z) - \text{bit}_{n+1}(y) \right) \pmod{2^{n+2}}.
\]

(5.5)

On the other hand

\[
z - y \equiv 2^n \left( \text{bit}_n(z) - \text{bit}_n(y) \right) + 2^{n+1} \left( \text{bit}_{n+1}(z) - \text{bit}_{n+1}(y) \right) \pmod{2^{n+2}}.
\]

(5.6)

Subtract (5.6) from (5.5):

\[
\Phi(z) - \Phi(y) - (z - y) \equiv 2^n \left( \left( ba^{\text{pop}_n(y)} + 1 \right) \text{bit}_n(y) - \left( ba^{\text{pop}_n(z)} + 1 \right) \text{bit}_n(z) \right) \pmod{2^{n+2}}.
\]

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

\[
\Phi(z) - \Phi(y) - (z - y) \equiv 2^n \left( \left( b \left( 1 + (a - 1) \text{pop}_n(y) \right) + 1 \right) \text{bit}_n(y) \right.
\]
\[
- \left( \left( b \left( 1 + (a - 1) \text{pop}_n(z) \right) + 1 \right) \text{bit}_n(z) \right)
\]
\[
\equiv 2^n \left( \left( ab + 1 + b(a - 1) \text{pop}_{n-1}(y) \right) \text{bit}_n(y) \right.
\]
\[
- \left( \left( ab + 1 + b(a - 1) \text{pop}_{n-1}(z) \right) \text{bit}_n(z) \right)
\]
\[
\equiv 2^n \left( ab + 1 + b(a - 1) \text{pop}_{n-1}(y) \right) \left( \text{bit}_n(y) - \text{bit}_n(z) \right)
\]
\[
\equiv 2^{n+1} \left( \frac{ab + 1}{2} + \frac{b(a - 1)}{2} \text{pop}_{n-1}(y) \right) \left( \text{bit}_n(y) - \text{bit}_n(z) \right) \pmod{2^{n+2}}.
\]

This is equivalent to (5.4). \( \blacksquare \)

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

\[
\sigma_{n+1}(x) \text{ is inert},
\]

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

\[
\Phi^{2^{n+1}}(x) \equiv x + 2^{n+1} \pmod{2^{n+2}}.
\]

(5.8)

We now introduce the quantities

\[
e_k[i] := \text{bit}_k \left( \Phi^i(x) \right).
\]

In terms of the \( e_k[i] \), we have

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

by (5.8). We proceed to evaluate \( e_{n+1}[2^{i+1}] - e_{n+1}[0] \pmod{2} \). The main theorems of this paper are deduced from the following formula.
THEOREM 5.1. If \( |\sigma_n(x)| = 2^l \) and \( \sigma_{n+1}(x) \) is an inert cycle, then

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

where

\[
(5.11) \quad N = \sum_{i=0}^{2^l-1} \text{pop}_{n-1}(\Phi'(x)).
\]

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

\[
X_i \equiv 2^{n+1} \left( \frac{ab + 1}{2} 2^l + \frac{b(a - 1)}{2} \text{pop}_{n-1}(\Phi'(x)) \right) \pmod{2^{n+2}}.
\]

Adding up the \( X_i \) gives

\[
(5.12) \quad \sum_{i=0}^{2^l-1} X_i \equiv 2^{n+1} \left( \frac{ab + 1}{2} 2^l + \frac{b(a - 1)}{2} N \right) \pmod{2^{n+2}}.
\]

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

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

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

\[
(5.14) \quad \sum_{i=0}^{2^l-1} Y_i = 2^n (2e_n[0] - 2e_n[2^l]) \equiv 2^{n+1} \pmod{2^{n+2}}.
\]

On the other hand,

\[
X_i - Y_i \equiv 2^{n+1} (e_{n+1}[i + 1 + 2^l] - e_{n+1}[i + 1] - e_{n+1}[i + 2^l]) \equiv 2^{n+1} (e_{n+1}[i + 1 + 2^l] + e_{n+1}[i + 1] - e_{n+1}[i + 2^l] - e_{n+1}[i]).
\]

In this form the sum of \( X_i - Y_i \) also telescopes:

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

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

\[
2^{n+1} (e_{n+1}[2^{i+1}] - e_{n+1}[0]) \equiv 2^{n+1} \left( \frac{ab + 1}{2} 2^l + \frac{b(a - 1)}{2} N \right) - 2^{n+1} \pmod{2^{n+2}},
\]

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
\[ \text{bit}_{n-1}(\Phi^{j+2^{j-1}}(x)) = 1 - \text{bit}_{n-1}(\Phi^i(x)), \]
so
\[ \text{pop}_{n-1}(\Phi^{j+2^{j-1}}(x)) + \text{pop}_{n-1}(\Phi^i(x)) \equiv 1 \pmod{2}. \]

Thus
\[ N = \sum_{i=0}^{2^{j-1}-1} \left( \text{pop}_{n-1}(\Phi^{i+2^{j-1}}(x)) + \text{pop}_{n-1}(\Phi^i(x)) \right) \equiv \sum_{i=0}^{2^{j-1}-1} 1 = 2^{j-1} \pmod{2}. \]

Now (ii) follows.

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

We first note that the odd periodic points $\text{Per}^*(\Phi)$ of $\Phi$ determine the entire set $\text{Per}(\Phi)$ of periodic points of $\Phi$. The relation
\[ (6.1) \quad \Phi(2x) = 2\Phi(x) \]
implies that $x$ has period $2^j$ if and only if $2x$ has period $2^j$. Thus
\[ (6.2) \quad \text{Per}(\Phi) = \{2^kx : k \geq 0 \text{ and } x \in \text{Per}^*(\Phi)\}. \]

Let $F_j$ be the number of orbits of $\Phi$ 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 $X_n$ of $\Phi_n$ by classifying them into two types: those arising by reduction mod $2^n$ from an odd fixed point of $\Phi$, 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 $X_{n+1}$ are “mortal.” An “immortal” 1-cycle in $X_n$ always splits, and gives rise to two 1-cycles in $X_{n+1}$, 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 $Z_n$ at step $n$ is

$$E[Z_n] = F_0 n + c_0,$$

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 $|X_n|$ when $y > 1$, we use a refined classification of cycles of $\Phi_n$. A step consists of passing from $\Phi_{n-1}$ to $\Phi_n$. For $0 \leq d \leq j \leq n$ let $X_{n,j,d}$ denote the set of cycles of $\Phi_n$ 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 $\Phi_{n+1}$. 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 $\Phi$ of period $2^j$ gives rise to a cycle of period $2^j$ of $\Phi_n$ 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:
(1) Each cycle in $X_{nj,1}$ has (independently) probability $1/2$ of falling in $Y_{nj,1}$.
(2) Each "mortal" cycle in $X_{nj,0}$ has (independently) probability $1/2$ of falling in $Y_{nj,0}$, and if so its two progeny in $X_{nj+1,0}$ are "mortal."
(3) Each "immortal" cycle in $X_{nj,0}$ lies in $W_{nj}^{1/0}$, and one of its progeny in $X_{nj+1,0}$ is "immortal" and the other is "mortal," with finitely many exceptions.

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

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

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 $E[Z_{nj}]$ becomes quite complicated.

It might be interesting to further compare predictions of this model for $j \geq 1$ with actual data for $\Phi$. We know of one odd periodic cycle of $\Phi$ 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 $F: Z_2 \to Z_2$ solenoidal if, for all $n$,

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

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

$$(A.2) \quad |F(x) - F(y)|_2 \leq |x - y|_2, \quad \text{all } x, y \in Z_2.$$ 

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

Call a family of functions $F_n: Z/2^n Z \to Z/2^n Z$ compatible if $F_n$ agrees with $F_{n-1}$ under projection $\pi_n: Z/2^n Z \to Z/2^{n-1} Z$; i.e., if $\pi_n \circ F_n = F_{n-1} \circ \pi_n$. A compatible family $\{F_n\}$ has an inverse limit $F: Z_2 \to Z_2$ defined by

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

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 $F \pmod{2^n}$ induces a function $F_n: Z/2^n Z \to Z/2^n Z$, 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) $\implies$ (ii). $U$ is surjective, so $U_n$ is surjective.
(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). Suppose that \(U_n(a) = U_n(b)\). Select \(x\) and \(y\) in \(\mathbb{Z}_2\) such that \(a = x + 2^m\), \(b = y + 2^m\). Then \(U_n(x + 2^m) = U_n(y + 2^m)\), so \(U(x) \equiv U(y) \pmod{2^m}\), 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 \(U_{V_0, V_1} : \mathbb{Z}_2 \to \mathbb{Z}_2\) by

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

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 \(z \equiv w + 2^m \pmod{2^m}\) then still \(V(z) \equiv V(w) \pmod{2^m}\). 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 \(V(z) \equiv V(w) + 2^m \pmod{2^m}\).

**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 \(b = x \pmod{2}\); then \(U(x) = V_b(S(x))\). Also \(U(y) = V_b(S(y))\), since \(y \equiv x \pmod{2}\). We have \(S(y) \equiv S(x) + 2^m e \pmod{2^m}\); by Lemma B.1, \(V_b(S(y)) \equiv V_b(S(x)) + 2^{m-1} e \pmod{2^m}\).
LEMMA B.3. Set $U = U_{\nu_0, \nu_1}$. Fix $m \geq j \geq 1$. If $y \equiv x + 2^m e \pmod{2^{m+1}}$ then $U^j(y) \equiv U^j(x) + 2^m e \pmod{2^{m-j+1}}$.

**Proof.** Lemma B.2 and induction on $j$. □

LEMMA B.4. Set $U = U_{\nu_0, \nu_1}$. 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 $U = U_{\nu_0, \nu_1}$. Fix $b_0, b_1, b_2, \ldots \in \{0, 1\}$. Define $x_0 = 0$ and $x_{m+1} = x_m + 2^m(b_m - U^m(x_m))$. Then $y \equiv x_m \pmod{2^m}$ if and only if $U^j(y) \equiv b_j \pmod{2}$ for $0 \leq j < m$.

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

Say $y \equiv x_{m+1} \pmod{2^{m+1}}$. Then $y \equiv x_m + 2^m(b_m - U^m(x_m)) \pmod{2^{m+1}}$; 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 $U^j(y) \equiv b_j \pmod{2}$ for $0 \leq j < m$.

Conversely, say $U^j(y) \equiv b_j \pmod{2}$ for $0 \leq j \leq m$. 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 $y \equiv x_m + 2^m(b_m - U^m(x_m)) = x_{m+1} \pmod{2^{m+1}}$. □

**Theorem B.1.** Set $U = U_{\nu_0, \nu_1}$. Define $Q(x) = \sum_{m=0}^{\infty}(U^m(x) \bmod 2) 2^m$. Then $Q$ is a solenoidal bijection, and $U = Q^{-1} \circ S \circ Q$.

Thus any map of the form $U_{\nu_0, \nu_1}$ 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 $x_{m+1} = x_m + 2^m(b_m - U^m(x_m))$. 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 $x_{m+1} = x_m + 2^m(b_m - U^m(x_m))$. 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 $x_{m+1} = x_m + 2^m(b_m - U^m(x_m))$. Since $x_{m+1} \equiv x_m \bmod{2^m}$ the sequence $x_1, x_2, \ldots$ converges to a $2$-adic limit $y$, with $y \equiv x_m \bmod{2^m}$. 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 $U = U_{\nu_0, \nu_1}$ for some solenoidal bijections $\nu_0, \nu_1$.

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

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

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

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

REFERENCES