The set of rational cycles for the $3x+1$ problem

by

JEFFREY C. LAGARIA (Murray Hill, N.J.)

1. Introduction. The notorious $3x+1$ problem concerns the behavior under iteration of the $3x+1$ function

$$T(n) = \begin{cases} (3n+1)/2, & n \equiv 1 \pmod{2}, \\ n/2, & n \equiv 0 \pmod{2}. \end{cases} \quad (1.1)$$

The $3x+1$ Conjecture is the claim that, starting from any positive integer $n$ the iterates $(n, T(n), T^2(n), \ldots)$ eventually reach the value 1, and subsequently run through the cycle $\{1, 2\}$ of period 2. The $3x+1$ Conjecture is often attributed to L. Collatz who studied similar iteration problems (but not necessarily this one); it was certainly made by B. Thwaites [14]. The $3x+1$ Conjecture remains unproved; it has however been verified for all $n \leq 10^{12}$. The Finite Cycles Conjecture asserts that the function $T$ has only finitely many cycles on $\mathbb{Z}$; it too remains unproved. The $3x+1$ Conjecture would be disproved by exhibiting a cycle on the positive integers other than $\{1, 2\}$. It is known that $T$ has no cycles in $\mathbb{Z}$ of length $< 250,000$, except those beginning with $1, 0, -1, -5$ and $-7$ (see [6], [7]). These results together with much of the previous work on the $3x+1$ problem are surveyed in [10].

This paper studies properties of rational cycles of the $3x+1$ problem, which are cycles of the function $T$ considered on the domain $\mathbb{Q}[2]$ of all rational numbers having an odd denominator. The $3x+1$ function $T$ is well defined on $\mathbb{Q}(2)$ and, more generally, is well defined on the set of 2-adic integers $\mathbb{Z}_2$, into which $\mathbb{Q}(2)$ is canonically embedded (see [10]). Unlike the set of integer cycles of $T$ which is presumed to be finite, the set $\mathfrak{S}$ of all elements of $\mathbb{Q}(2)$ in cycles of $T$ is large and well-behaved. Cycles of period $n$ can be indexed by the $n$ residue classes (mod 2) of their iterates. In Section 2 we show that every possible such sequence (mod 2) gives rise to an element in a unique rational cycle and conversely. Theorem 2.1 shows that for each $v = (v_0, \ldots, v_n) \in \mathcal{B}[2]$, there is a unique $x(v) \in \mathcal{Q}(2)$ with the property that $x(v)$ is

(1) The ring $\mathbb{Q}(2)$ is the (local) ring of fractions of $\mathbb{Z}$ at the prime ideal $(2)$, so would be denoted $\mathbb{Z}_{(2)}$ in the notation of [2], p. 38. To avoid confusion with the 2-adic integers $\mathbb{Z}_2$ we adopt the notation $\mathbb{Q}(2)$.
in a rational cycle of $T$ of period $n$ with $T_0(x(v)) = v_i \pmod{2}$ for $1 \leq i \leq n$, and in fact

$$x(v) = \sum_{j=0}^{n-1} \frac{v_j 2j^{v_j+1 + \ldots + v_{n-1}}}{2^n - 3^{v_0 + \ldots + v_{n-1}}}. \tag{1.2}$$

Such rationals are exactly those of the form

$$\sum_{j=0}^{k} \frac{3^{2^j} 0}{2^n - 3^{v_0 + \ldots + v_{n-1}}}. \tag{1.3}$$

with $n > a(0) > a(1) > \ldots > a(k) \geq 0$. Theorem 2.1 is essentially due to Böhm and Sontacchi [4] (who however only study integer cycles), and is also proved in Gurwood [8]. (See Seifert [12] for a related result.)

The set $\mathcal{C}$ has another interpretation, in terms of the set of all elements in integer cycles of the ensemble of $3x + k$ functions

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

with $k \geq 1$ and $k \equiv \pm 1 \pmod{6}$. Each rational cycle of $T$ is associated to an integer cycle of a unique such $T_k$ by clearing denominators; all the rationals in a given rational cycle of $T$ have this denominator $k$ when written in lowest terms. An integer cycle of $T_k$ obtained in this way has all integers relatively prime to $k$; a cycle with this property is called a primitive cycle of $T_k$. Conversely, each primitive cycle of $T_k$ arises from a rational cycle of $T$, so that the elements of $\mathcal{C}$ are in one-to-one correspondence with the set of elements of $\mathcal{C}$ in all primitive cycles of the set of $3x + k$ functions $T_k$ as $k$ varies over all positive integers with $k \equiv 1 \pmod{6}$.

The main results of this paper concern how the elements of $\mathcal{C}$ are distributed among the various $k$. The complexity of this problem arises from the fact that the representation (1.2) for an element in a cycle of period $n$ may not be in lowest terms, and large cancellations of common factors between the numerator and denominator of fractions (1.3) sometimes occur. Let $C_{\text{prim}}(k)$ count the number of primitive cycles of $T_k$ and let $C_{\text{prim}}(k, y)$ count the number of such primitive cycles of period at most $y$. In Section 3 we give heuristic arguments for the two conjectures that for all $k \equiv \pm 1 \pmod{6}$ one has:

1. $C_{\text{prim}}(k) > 1$.
2. $C_{\text{prim}}(k)$ is finite.

These conjectures both seem difficult. We study the more tractable function $C_{\text{prim}}(k, y)$. We show that $C_{\text{prim}}(k, \frac{k}{2} k^{1/2}) = 0$ for infinitely many $k$ (Theorem 3.1). This implies that if $C_{\text{prim}}(k) > 1$ for such $k$ then huge cancellations between numerator and denominator in (1.2) must occur for the numbers in the associated rational cycle of $T$ (see Theorem 3.2). We show that there is a constant $c_0$ such that for any $\epsilon > 0$ one has

$$C_{\text{prim}}(k, (1+\epsilon) \log k) \geq k^{1-c_0 \log \log k}, \tag{1.4}$$

for infinitely many $k$ (Theorem 3.3). We also show that any positive $n_0$ that occurs in a primitive cycle for one $T_k$ with $k > 0$ also occurs in a primitive cycle for infinitely many $T_k$ (Theorem 3.4). This holds for $n_0 = 1$ and 5 and is conjectured to hold for all positive $n_0 \equiv \pm 1 \pmod{6}$. Then we show that each negative $n_0$ is in a primitive cycle only for finitely many $T_k$ with $k > 0$ (Theorem 3.5).

Section 4 studies certain average values for the number of primitive cycles. We consider the sums

$$\Phi(x, y) = \sum_{k \equiv \pm 1 \pmod{6}} C_{\text{prim}}(k, y),$$

with $y = \beta \log x$ for a fixed $\beta > 0$. To estimate these sums we study the divisibility properties (mod $M$) of the 2$^n$ numerators of the rationals (1.2) associated to all $v \in \{0, 1\}^n$, i.e. of the set

$$\Sigma_n = \{ \sum_{j=0}^{n-1} v_j 2^j v_{j+1} + \ldots + v_{n-1} : v \in \{0, 1\}^n \}.$$

Let $F(n, M)$ denote the maximum number of elements of $\Sigma_n$ in any residue class (mod $M$). We prove that

$$F(n, M) < \begin{cases} (n+1) & M > 3^n, \\ 2n 2^n/M & 1 \leq M \leq 3^n, \end{cases}$$

where $\varphi = (\log 3)^{-1} = 0.63093$ (Theorem 4.1). We also prove a stronger estimate valid for $M = 2^m$ with $a \leq a_0 = 0.04766$:

$$F(n, M) \leq 2n 2^n \varphi$$

(Theorem 4.2). This is quite close to the expected value $2^n M / \varphi$ which would occur if the elements of $\Sigma_n$ were uniformly distributed in all residue classes (mod $M$). Using these bounds we show that, for any fixed $\beta \geq 1$,

$$\Phi(x, \beta \log x) \leq 4(\beta \log x)^{\varphi} x^{(\beta^2 - 1)/2} e^{\log \log x},$$

where

$$f(\beta) = \begin{cases} 1 & 1 \leq \beta \leq \beta_x, \\ (1 - \varphi) \beta + \varphi & \beta > \beta_x. \end{cases}$$

and $c_0$ is an absolute constant (Theorem 4.3). The same proof shows that

$$C_{\text{prim}}(k, \beta \log k) \leq 4(\beta \log k)^{\varphi} k^\beta.$$

For $\beta \leq \beta_x$ this upper bound is quite close to the lower bound (1.4) attained for infinitely many $k$, e.g. $C_{\text{prim}}(k, 1.01 \log k) < 5k(\log k)^3$. Finally, we conjecture
that there is a constant \( c \) such that for all \( n \) one has
\[
F(n, M) \leq \begin{cases} 
\lceil n^c \rceil, & M \geq 2^n, \\
\frac{n^c 2^{M}}{M}, & 1 \leq M \leq 2^n.
\end{cases}
\]

It seems likely that further progress can be made on this conjecture.

I am indebted to Ralph Tamlyn for the computation of Table 3.1.

2. Rational 3x+1 cycles. The 3x+1 function \( T \) defined by (1.1) makes sense on the ring \( \mathbb{Q}(2) \) of all rationals \( p/q \) such that \( q \) is odd, where one considers such rationals even or odd, according to the parity of their numerator \( p \). Associate to any such rational \( x \) its parity sequence \( b(x) = (b_0(x), b_1(x), \ldots, b_j(x), \ldots) \) where
\[
b_j(x) \equiv T^j(x) \pmod{2},
\]
and each \( b_j(x) = 0 \) or 1. Call \( b_j(x) \) the \( n \)-th bit in the parity sequence of \( x \).

The following result shows that every periodic parity sequence corresponds to a unique \( x \in \mathbb{Q}(2) \) in some rational cycle and vice versa; the proof follows that of Böhm and Sontacchi [4], Thm. 5.

**Theorem 2.1.** Given any 0-1 vector \( v = (v_0, v_1, \ldots, v_{n-1}) \) there is a unique \( x \) in \( \mathbb{Q}(2) \) which is periodic of period \( n \) under iteration by the 3x+1 function \( T \) and whose parity sequence starts with \( v \). It is given by
\[
x = x(v) = (2^n - 3^{v_0 + \cdots + v_{n-1}}) \sum_{j=0}^{n-1} v_j 3^{v_j + \cdots + v_{n-1}} 2^j.
\]

**Proof.** Let \( U_0(x) = x/2 \) and \( U_1(x) = (3x + 1)/2 \). A necessary condition for \( x \) to be periodic of period \( n \) with parity sequence starting with \( v \) is that
\[
x = U_{n-1} \left( U_{n-2} \left( \ldots U_0(x) \right) \right).
\]
Substituting the definition of the \( U_i(x) \) yields
\[
x = \frac{1}{2} \left( 3^{v_0 + \cdots + v_{n-1}} x + \sum_{j=0}^{n-1} v_j 2^{3^{v_j + \cdots + v_{n-1}} j} \right).
\]
The solution \( x(v) \) to this linear equation is (2.1), and \( x(v) \) clearly is in \( \mathbb{Q}(2) \). This shows that \( x(v) \) is unique if it exists.

The main assertion of the theorem is that the solution (2.1) actually is never extraneous, i.e., when the function \( T \) is applied to \( x(v) \) defined by (2.1) the parity sequence of \( x(v) \) starts out with \( v \). To see this, note that for \( y \in \mathbb{Q}(2) \) exactly one of \( U_0(y) \) and \( U_1(y) \) is in \( \mathbb{Q}(2) \); if \( y \) is even then \( U_0(y) \in \mathbb{Q}(2) \) and if \( y \) is odd then \( U_1(y) \in \mathbb{Q}(2) \). Also if a rational \( y \) \( \mathbb{Q}(2) \) then both \( U_0(y) \) \( \mathbb{Q}(2) \) and \( U_1(y) \) \( \mathbb{Q}(2) \). Consequently, given any \( y \) \( \mathbb{Q}(2) \) there is exactly one of the \( 2^n \) possible sequences \( w \) of 0-1 vectors with \( U_{n-1} \left( w_0 \right) \cdots w_{n-1} \right) \in \mathbb{Q}(2) \).

Now \( x(v) \in \mathbb{Q}(2) \) so \( T^{\alpha}(x(v)) \in \mathbb{Q}(2) \), while
\[
U_{n-1} \left( U_{n-2} \left( \ldots U_0(x(v)) \right) \right) \in \mathbb{Q}(2)
\]
by (2.2), hence
\[
T^{\alpha}(x(v)) = U_{n-1} \left( U_{n-2} \left( \ldots U_0(x(v)) \right) \right) = x(v)
\]
as required.

This result has two interesting corollaries.

**Corollary 2.1a.** For fixed \( k \), the integers given by
\[
\sum_{i=0}^{k} 2^{n_i} 3^i, \quad a_0 > a_1 > \ldots > a_k \geq 0,
\]
are all distinct.

**Proof.** Suppose not, and that \( \sum_{i=0}^{k} 2^{n_i} 3^i = \sum_{i=0}^{k} 2^{n_i} 3^i \). Take \( n = \max(a_0, b_0) + 1 \). Define the parity vectors \( v = (v_0, \ldots, v_{n-1}) \), \( w = (w_0, \ldots, w_{n-1}) \) with \( v_0 = 1 \) and all other \( v_j = 0 \) and all other \( w_j = 1 \). Then
\[
x(w) = (2^n - 3^k) \sum_{i=0}^{k} 2^{n_i} 3^i, \quad x(v) = (2^n - 3^k) \sum_{i=0}^{k} 2^{n_i} 3^i,
\]
hence \( x(v) = x(w) = x \), say. The parity sequences of \( x \) must start with both \( v \) and \( w \) by Theorem 2.1, so that \( v = w \), contradicting \( a_0, \ldots, a_k \neq (b_0, \ldots, b_k) \).

Corollary 2.1a has a simple direct proof due to Don Coppersmith. If \( B = \sum_{i=0}^{k} 2^{n_i} 3^i \) satisfies (2.3) for a fixed \( k \), then \( B \) is the highest power of 2 dividing \( B \). This determines \( a_k \), so one obtains
\[
B' = B - 2^{n_k} 3^k = \sum_{i=0}^{k-1} 2^{n_i} 3^i.
\]
Now \( a_{k-1} \) is determined similarly as the largest power of 2 dividing \( B' \), and proceeding recursively one can recover all of the \( a_i \), thus proving uniqueness of the representation (2.3).

The assertion of Corollary 2.1a is no longer true if one allows integers (2.3) with different \( k \), e.g.
\[
2^4 + 3 = 2^2 + 2 \cdot 3 + 3^3 = 19.
\]

A parity sequence is said to be aperiodic if it is not eventually periodic. A trajectory \( (x, T(x), \ldots, T^n(x), \ldots) \) for the 3x+1 function on \( \mathbb{Q}(2) \) is divergent if \( \lim_{m \to \infty} T^m(x) = \infty \). It is easily checked that any trajectory is either eventually periodic or divergent. Several authors have conjectured that no divergent trajectories exist (see [10]).
COROLLARY 2.1b. Any divergent trajectory must have an aperiodic parity sequence.

Proof. We use the fact proved in [10] that the mapping from \( Q [[2]] \) that sends \( x \) to its parity sequence \( b(x) \) is one-to-one. (This was proved more generally for all \( x \) in the 2-adic integers \( \mathbb{Z}_2 \).) Suppose the corollary were false, and that \( y \) gives a counterexample. By iterating \( y \) if necessary we may assume that it has a divergent trajectory with a purely periodic bit sequence. Suppose that this bit sequence has period \( v \). Then \( x(v) \) given by Theorem 2.1 has the same bit sequence, and \( x(v) \) has a purely periodic trajectory under \( T \) so \( x(v) \neq y \). This contradicts the map \( b(\cdot) \) being one-to-one. \( \square \)

It is an easy matter to count the number of cycles of a given length. Call a 0-1 vector \( v = (v_0, \ldots, v_{n-1}) \) reducible if \( v = w^j \) for some \( j \geq 2 \), where \( w^j \) denotes the concatenation of \( j \) copies of \( w \); otherwise call it irreducible. A vector \( v \) is irreducible if and only if its \( n \) cyclic permutations \( \sigma_k(v) = (v_k, v_{k+1}, \ldots, v_{n-1}, v_0, \ldots, v_{k-1}) \) are all distinct. An irreducible cycle of length \( n \) corresponds to a set of \( n \) cyclic permutations of an irreducible vector \( v \) of length \( n \). Let \( I(n) \) denote the number of irreducible cycles of length \( n \). Using the action of the group of cyclic permutations on the set \( \{0, 1\}^n \) one has

$$
\sum_{d|n} I(d) = 2^n.
$$

Möbius inversion gives

$$
I(n) = \frac{1}{n} \sum_{d|n} \mu(d) 2^{n/d},
$$

where \( \mu(d) \) is the Möbius function. From this formula one easily deduces that

$$
I(n) = \frac{1}{n} 2^n + O(2^{n/2}).
$$

Small values of \( I(n) \) are given in Table 2.1.

<table>
<thead>
<tr>
<th>( n )</th>
<th>( I(n) )</th>
<th>( n )</th>
<th>( I(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>11</td>
<td>186</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>12</td>
<td>335</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>13</td>
<td>630</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>14</td>
<td>1161</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>15</td>
<td>2182</td>
</tr>
<tr>
<td>6</td>
<td>9</td>
<td>16</td>
<td>4080</td>
</tr>
<tr>
<td>7</td>
<td>18</td>
<td>17</td>
<td>7710</td>
</tr>
<tr>
<td>8</td>
<td>30</td>
<td>18</td>
<td>14532</td>
</tr>
<tr>
<td>9</td>
<td>56</td>
<td>19</td>
<td>27594</td>
</tr>
<tr>
<td>10</td>
<td>99</td>
<td>20</td>
<td>52377</td>
</tr>
</tbody>
</table>

Table 2.2 gives the lexicographically largest member \( v \) of each irreducible cycle of length \( n \leq 6 \), and the corresponding values \( x(v) \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>( v )</th>
<th>( x(v) )</th>
<th>( x(v) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>11111</td>
<td>( \frac{1}{1} )</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>111100</td>
<td>( \frac{1}{4} )</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>1111000</td>
<td>( \frac{1}{1} )</td>
</tr>
<tr>
<td>3</td>
<td>110</td>
<td>1110000</td>
<td>( \frac{1}{4} )</td>
</tr>
<tr>
<td>100</td>
<td>( \frac{1}{6} )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1110</td>
<td>1000000</td>
<td>( \frac{1}{1} )</td>
</tr>
<tr>
<td>1100</td>
<td>( \frac{1}{6} )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td>( \frac{1}{6} )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10000</td>
<td>( \frac{1}{6} )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10100</td>
<td>( \frac{1}{6} )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10000</td>
<td>( \frac{1}{6} )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Since the 3x+1 function \( T \) does not change the denominator of any rational \( x \in Q [[2]] \) to which it is applied, it is clear that all rationals in a 3x+1 cycle of period \( n \) written in lowest terms have the same denominator, which we call the denominator \( \delta(v) \) of a cycle including \( x(v) \). Clearly

$$
\delta(v) = \frac{D(v)}{(N(v), D(v))},
$$

where

(2.7a)

$$
D(v) = 2^n - 3^{v_0} \cdots 3^{v_{n-1}},
$$

(2.7b)

$$
N(v) = \sum_{j=0}^{n-1} v_j 2^j 3^{v_{j+1}} \cdots 3^{v_{n-1}}
$$

are the denominator and numerator of the fraction (2.1) before it is reduced to lowest terms. Table 2.2 includes one example \( v = 110000 \) having \( D(v) \neq \delta(v) \), with \( D(v) = 55, \delta(v) = 11 \).

3. Primitive 3x+k cycles. The 3x+k function \( T_k \) is defined for \( k \equiv 1 \pmod{2} \) by

$$
T_k(n) = \begin{cases} 
(3n+k)/2, & \text{if } n \equiv 1 \pmod{2}, \\
(n/2), & \text{if } n \equiv 0 \pmod{2}.
\end{cases}
$$
A rational cycle for the $3x+1$ problem with denominator $k$ gives rise to an integral cycle for the $3x+k$ function obtained by clearing the denominator $k$. Since the denominator $D(v)$ of a rational cycle $x(v)$ of $T_k$ has $(D(v), 6) = 1$, we always have $k \equiv \pm 1 \pmod{6}$ in this correspondence. Conversely, all integral cycles of all $3x+k$ functions with $k \equiv \pm 1 \pmod{6}$ arise in this fashion from rational $3x+1$ cycles.

Note that $T_{-k}$ and $T_k$ are essentially the same function because $T_k(n) = T_{-k}(-n)$, so we suppose $k \geq 1$ in what follows.

The map $T_k$ sends $Z$ to $Z$; more generally define for $d|k$ the set $Z(d, k) = \{ n : (n, k) = d \}$ and observe that $T_k$ maps $Z(d, k)$ into $Z(d, k)$. The action of $T_k$ on $Z(d, k)$ is the same as the action of $T_{kd}$ on $Z(1, k/d)$ up to a multiplicative scale factor. For this reason we study the action of $T_k$ on the domain $Z(1, k)$, which we call the set of primitive integers (mod $k$). A cycle of $T_k$ on $Z(1, k)$ is called a primitive cycle (mod $k$). (Minimal invariant sets of residue classes (mod $N$) for a class of functions generalizing $T_k$ are studied by Matthews and Watts [11] and Buttsworth and Matthews [5].)

The discussion so far describes a bijection between the set $Z$ of elements of $Q(2)$ in some cycle of the $3x+1$ function $T_k$ and the set $Z$ of all members of primitive cycles of some $T_k$ with $k > 0$ and $k \equiv \pm 1 \pmod{6}$. In the remainder of this section we shall therefore suppose that $k > 0$ and $k \equiv \pm 1 \pmod{6}$.

3.1. Two conjectures about primitive cycles. Let $C_{prim}(k)$ count the number of primitive cycles of $T_k$, and set $C_{prim}(k, y)$ be the somewhat more tractable function that counts the number of primitive cycles of $T_k$ of period $\leq y$. One expects that the behavior of iterates of $T_k$ on $Z(1, k)$ will be qualitatively similar to that of the $3x+1$ function $T_1$ on $Z$. A heuristic argument similar to that in [10], Sec. 2.1, suggests that (averaged over a long series of iterates) $T_k(n)$ is about $\frac{4}{3}^{1/2} n$. One then expects that no trajectory can diverge to infinity, hence every trajectory becomes eventually periodic. This leads to the following conjecture.

PRIMITIVE CYCLES EXISTENCE CONJECTURE. For each $k \equiv \pm 1 \pmod{6}$ the $3x+k$ function $T_k$ has a primitive cycle, i.e. $C_{prim}(k) \geq 1$.

This conjecture seems difficult, if not intractable, for reasons indicated in Section 3.2.

How many primitive cycles are there for a fixed $k$? The following conjecture is an extension of one made for the $3x+1$ problem.

FINITE PRIMITIVE CYCLES CONJECTURE. For each $k \equiv \pm 1 \pmod{6}$, one has $C_{prim}(k) < \infty$.

Some evidence for this conjecture, in the case $k = 1$, is that $T_1$ has 5 small cycles and no other cycles of length $< 250,000$ (see [6], [7], [10]). A heuristic argument supporting this conjecture is described in Section 3.6. At present it also seems an intractably hard problem.

3.2. Existence of primitive cycles. To gain insight into the Primitive Cycles Existence Conjecture, we examine numerical evidence. Table 3.1 gives for $k \leq 150$ the smallest positive $n_0$ such that $n_0$ is in a primitive cycle of $T_k$, and gives the period length of that cycle. (This need not be the shortest primitive cycle of $T_k$.) Table 3.1 includes a number of examples of cycles of $T_k$ of minimal period approximately $k$, e.g. $k = 85, 107, 139$. The rational $x(v)$ given by (3.1) for such a cycle has a denominator $D(v) = 2^v - 3$ for some $v$ before being reduced to lowest terms, while in lowest terms the denominator $D(v) = k$. It is apparent that the unreduced denominator $D(v)$ must be of size at least the minimum of $[2^v - 3]$ for $0 \leq v \leq n$, and for $n = 85, 107, 139$ this is at least $\frac{1}{2} \cdot 2^n$. Consequently, there must be a cancellation of a huge common factor from the denominator $D(v)$ and numerator $N(v)$ of $x(v)$ in these examples.

<table>
<thead>
<tr>
<th>$k$</th>
<th>$n_0$</th>
<th>cycle length</th>
<th>$n_0$</th>
<th>cycle length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>77</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>3</td>
<td>79</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>4</td>
<td>83</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>6</td>
<td>85</td>
<td>7</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>4</td>
<td>89</td>
<td>17</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>7</td>
<td>91</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>5</td>
<td>11</td>
<td>95</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>5</td>
<td>5</td>
<td>97</td>
<td>18</td>
</tr>
<tr>
<td>25</td>
<td>7</td>
<td>16</td>
<td>101</td>
<td>7</td>
</tr>
<tr>
<td>29</td>
<td>1</td>
<td>5</td>
<td>103</td>
<td>5</td>
</tr>
<tr>
<td>31</td>
<td>3</td>
<td>23</td>
<td>107</td>
<td>106</td>
</tr>
<tr>
<td>33</td>
<td>1</td>
<td>3</td>
<td>109</td>
<td>19</td>
</tr>
<tr>
<td>37</td>
<td>19</td>
<td>6</td>
<td>113</td>
<td>29</td>
</tr>
<tr>
<td>41</td>
<td>1</td>
<td>20</td>
<td>115</td>
<td>13</td>
</tr>
<tr>
<td>43</td>
<td>1</td>
<td>11</td>
<td>119</td>
<td>1</td>
</tr>
<tr>
<td>47</td>
<td>5</td>
<td>18</td>
<td>121</td>
<td>5</td>
</tr>
<tr>
<td>49</td>
<td>25</td>
<td>38</td>
<td>125</td>
<td>1</td>
</tr>
<tr>
<td>53</td>
<td>103</td>
<td>29</td>
<td>127</td>
<td>1</td>
</tr>
<tr>
<td>55</td>
<td>1</td>
<td>12</td>
<td>131</td>
<td>13</td>
</tr>
<tr>
<td>59</td>
<td>1</td>
<td>28</td>
<td>133</td>
<td>11</td>
</tr>
<tr>
<td>61</td>
<td>1</td>
<td>6</td>
<td>137</td>
<td>14</td>
</tr>
<tr>
<td>65</td>
<td>19</td>
<td>24</td>
<td>139</td>
<td>11</td>
</tr>
<tr>
<td>67</td>
<td>17</td>
<td>30</td>
<td>143</td>
<td>7</td>
</tr>
<tr>
<td>71</td>
<td>29</td>
<td>10</td>
<td>145</td>
<td>1</td>
</tr>
<tr>
<td>73</td>
<td>19</td>
<td>60</td>
<td>149</td>
<td>19</td>
</tr>
</tbody>
</table>

We show below that in order for the Primitive Cycles Existence Conjecture to be true, the cancellation of huge common factors $(N(v), D(v))$ must occur for infinitely many $k$. It is this property that makes the Primitive Cycles Existence Conjecture appear difficult.
We first show there exist infinitely many \( k \) for which \( T_k \) has no short primitive cycle.

**Theorem 3.1.** There exist infinitely many \( k \equiv \pm 1 \pmod{6} \) such that \( T_k \) has no primitive cycle of period \( \leq \frac{3}{2}k^{1/3} \), i.e. \( C_{\text{prim}}(k, \frac{3}{2}k^{1/3}) = 0 \).

**Proof.** If \( v \) is a primitive cycle of period \( n \) of \( T_k \) then the rational number \( x(v) \) expressed in lowest terms has denominator \( k \). Hence \( k \) divides \( D(v) = 2^n - 3 \) where \( 1 \leq l \leq n \). Consider

\[
S(t) = \prod_{n=1}^{t} \sum_{i=1}^{n} |2^n - 3|.
\]

It is easy to see that \( S(t) \leq 3^{\Theta(2^{1/2} + 1)^{t/3}} \). Now if all \( T_k \) for \( k_0 \leq k \leq k \) have a primitive cycle of length \( \leq t \) then the least common multiple \( [k_0, k] \) of \( k_0 \) through \( k \) must divide \( S(t) \). It is well known (and equivalent to the prime number theorem) that

\[
\log [1, k] = k + o(k),
\]

as \( k \to \infty \) ([9], Theorem 43). Also \( [k_0, k] \geq [1, k][1, k_0] \), for any \( k_0 \). On choosing \( t = \frac{3}{2}k^{1/3} \) one has, using the upper bound for \( S(t) \), that for sufficiently large \( k_0 \),

\[
\log [k_0, k] > 0.99(k - k_0) \geq \log S(\frac{3}{2}k^{1/3})
\]

for \( k \geq 5k_0 \). This contradicts \( [k_0, k] S(\frac{3}{2}k^{1/3}) \), and thus proves that there is at least one such \( k \) in the interval \( [k_0, 5k_0] \) having no primitive cycle of length \( \leq \frac{3}{2}k^{1/3} \).

One can improve the constant \( \frac{3}{2} \) in Theorem 3.1 slightly with a more careful argument.

Now we can show that huge cancellations must sometimes occur, if the Primitive Cycles Existence Conjecture is true.

**Theorem 3.2.** There exist infinitely many \( k \equiv \pm 1 \pmod{6} \) such that either \( T_k \) has no primitive cycle or else every primitive cycle \( v \) of \( T_k \) has

\[
k = \frac{D(v)}{N(v), D(v)} \leq (\log D(v))^2.
\]

**Proof.** We first show \( D(v) \) is large for all \( v \). A result of A. Baker and N.I. Fel'dman ([3], Theorem 3.1) on linear forms in logarithms of algebraic numbers implies that there exists an effectively computable constant \( c_5 > 0 \) such that for all \( n \geq 2 \)

\[
|n \log 2 - \log 3| \geq n^{-c_5}.
\]

From this it is easily shown that there exists an effectively computable constant \( c_6 \) such that for \( n \geq 2 \) one has

\[
|2^n - 3| \geq \frac{1}{2} n^{-c_6} 2^n.
\]

Now take a \( T_k \) having no primitive cycle of period \( \leq \frac{3}{2}k^{1/3} \), which exists by Theorem 3.1. Let \( v \) be a primitive cycle of \( T_k \), necessarily of period \( n > \frac{3}{2}k^{1/3} \). Now

\[
\log_2 D(v) = \log_2 |2^n - 3| \geq n - c_1 \log_2 n - 1
\]

\[
\geq \frac{3}{2} k^{1/3} - O(\log k) \geq k^{1/3},
\]

for all \( k \geq k_2 \) for some constant \( c_2 \).

**3.3. Large values for \( C_{\text{prim}}(k) \).** We show that \( C_{\text{prim}}(k) \) takes occasional large values.

**Theorem 3.3.** There is a positive constant \( c_0 \) such that for any fixed \( \epsilon > 0 \) one has

\[
C_{\text{prim}}(k, (1 + \epsilon) \log k) \geq k^{1 - c_0 \log \log k}
\]

for infinitely many \( k \).

**Proof.** Consider the set \( S_n \) of 0-1 vectors \( v \) of length \( 2n \) containing exactly \( n \) ones. There are at least \( n^{n - (2n)} \) distinct primitive cycles associated to such \( v \) (with period dividing \( n \)), and each such cycle has a denominator \( \delta(v) | B_n = 2^n - 3 \). Now \( B_n \) has \( d(B_n) \) divisors \( k \), and at least one of them has many primitive cycles. There exists a constant \( c_0 \) such that \( d(B_n) \leq B_n^{c_0 \log \log B_n} \) for all \( B_n > 1 \) ([9], Theorem 317). Now let \( C_{\text{prim}}^+(k, n) \) count the number of primitive cycles of \( T_k \) with period dividing \( n \). Clearly \( C_{\text{prim}}(k, n) \geq C_{\text{prim}}^+(k, n) \). The argument just given shows that there is some \( k, B_n \) such that

\[
C_{\text{prim}}^+(k, 2n) \geq \frac{1}{n!} \left( \frac{2^n}{n} \right) d(B_n)^{-1} \geq 2^{2n - c_0 \log \log n}.
\]

Let \( k_n \) denote the smallest \( k \) such that (3.5) holds. We claim that, for any fixed \( \epsilon > 0 \), \( k_n \geq 2^{n - \epsilon} \) for all \( n \geq n_0(\epsilon) \). Assuming that this claim is proved, the bound (3.4) holds with \( 1 + \epsilon = (1 - \epsilon)^{-1} \) for all \( k_n \) with \( n \geq n_0(\epsilon) \) since \( 2n < (1 + \epsilon) \log n_0 \). Also since \( 2^n \geq k_n \geq 2^{1 - \epsilon} \) there are infinitely many different \( k_n \), for which (3.4) holds.

It remains to prove the claim. To do this, we use an estimate to be proved later (Theorem 4.1), which shows that the number of \( v \in \{0, 1\} \) with \( M|N(v) \) is at most \( n^{2^n} 2^M | M^* \), where \( \varphi = \log_2 3^{-1} \). Now suppose \( K \leq 2^{n - \epsilon} \), so that for any \( B = 2^{n - \epsilon} - 3 \) with \( K \) one has \( M = K/|N(v)| = n \geq 2^{2n} \) using (3.3). Consequently, the number of \( v \in \{0, 1\} \) having \( M|N(v) \) is at most \( 2n^{2^n} 2^{(1 - \epsilon) n} \). Now there are \( n+1 \) choices of \( k \), hence at most \( n+1 \) choices of \( M \), so that

\[
C_{\text{prim}}^+(K, 2n) \leq 2^{n^2 + c_1 2^{(1 - \epsilon) n}}.
\]

This contradicts (3.5) for all large enough \( n \), so \( k_n \neq K \) and thus \( k_n > 2^{n - \epsilon} \), proving the claim.
3.4. Primitive cycles containing a fixed integer. For fixed \( k \equiv \pm 1 \pmod{6} \) we may index primitive cycles by their smallest member \( n_0 \). This will always be an integer \( n_0 \equiv 1 \pmod{6} \). For how many \( k \) is \( n_0 \), a member of some primitive cycle? The simplest case is \( n_0 = 1 \). Table 3.1 suggests the possibility that 1 is in a cycle for a positive proportion of all \( T_k \) with \( k \geq 1 \). This seems hard to prove. However, it is easy to show that 1 is in a cycle for infinitely many \( k \). The vector \( v = 10^m \) has \( x(v) = 1/(2^n - 3) \), hence \( T_k \) for \( k = 2^n - 3 \) has a primitive cycle containing 1. More generally we have the following result.

**Theorem 3.4.** If a positive \( n_0 \) is in a primitive cycle for some \( T_k \) with \( k > 0 \), then it is in a primitive cycle for infinitely many \( T_k \) with \( k > 0 \). If in addition \( n_0 \equiv 1 \pmod{6} \) then it is the smallest element in such a primitive cycle for infinitely many \( k \).

**Proof.** By hypothesis there is a 0-1 vector \( v = (v_0, \ldots, v_{n-1}) \) such that

\[
x(v) = \frac{N(v)}{D(v)} = \frac{n_0}{k}
\]

with \( n_0, k = 1 \) and \( x(v) > 0 \). If \( l = v_0 + \cdots + v_{n-1}, \) then \( D(v) = 2^n - 3 > 0 \).

The vectors \( w_0 = 00^m \) have \( N(w_0) = N(v), D(w_0) > 0 \) and

\[
x(w_0) = \frac{N(w_0)}{D(w_0)} = \frac{N(v)}{2^n - 3}.
\]

The rational (3.7) reduces in lowest terms to a rational with numerator \( n_0 \) whenever

\[G_m = (N(w_0), D(w_0)) = (N(v), 2^{n+m} - 3)\]

has \( G_m = G_0 \), in which case \( x(w_0) = \frac{n_0}{k_m} \) with \( k_m = (2^n - 3)/G_0 \) and \( n_0, k_m = 1 \). The function \( G_m \) is periodic with period \( p = \text{ord}_{n_0}(2) \), i.e., the smallest positive \( p \geq 2 \) with \( 2^n \equiv 1 \pmod{N(v)} \). In particular \( G_m = G_0 \) whenever \( m = 0 \pmod{p} \). This shows that infinitely many \( k \) exist with \( n_0 \) in a primitive cycle of \( T_{n_0} \). Finally, we show that if \( n_0 \equiv 1 \pmod{6} \) then \( n_0 \) is the smallest element in the corresponding cycle of \( T_{n_0} \) for all sufficiently large \( m = 0 \pmod{p} \). Since \( n_0 \) is odd, the first entry of \( v \) is 1, hence for \( m > 4n \),

\[T_{n_0}^{2m}(n_0) \geq \frac{2^{2m} - 2^n}{2^{2m} - 2^n} > 2^n n_0,
\]

since \( n_0 \leq N(v) < 3^n - 2^n \). Consequently

\[T_k^{2m}(n_0) > n_0, \quad 1 \leq j \leq n.
\]

Since the last \( m \) entries of \( w_0 = 00^m \) are zero,

\[T_k^{n+1}(n_0) > T_k^n (n_0) = n_0, \quad n + 1 \leq j < n + m.
\]

Thus \( n_0 \) is the smallest element in the cycle. □
find $n$ distinct $v$ with $\delta(v) = 1$, and using the heuristic hypothesis the probability of this is $(|\Sigma_n|/D_n)^n$. We divide the set of all pairs $(n, l)$ into two classes:

Case 1: $1 \leq l \leq \frac{3}{4}n$. In this case $D_{n,l} \geq 2^n - 3^n/26^n \geq 2^{n-1}$ while $$|\Sigma_{n,l}| \leq \binom{n}{\lfloor \frac{3}{4}n \rfloor} \leq \frac{1}{\sqrt{n}} 2^n.$$ Hence $$\left(\frac{|\Sigma_{n,l}|/D_{n,l}\right)^n \leq (0.99)^{-n^2}.$$ 

Case 2: $\frac{3}{4}n \leq l \leq n$. In this case $D_{n,l} \geq 2^n - 3^n/26^n$ by (3.3) while $$|\Sigma_{n,l}| \leq \binom{n}{\lfloor \frac{3}{4}n \rfloor} \leq (1.98)^n.$$ Hence $$\left(\frac{|\Sigma_{n,l}|/D_{n,l}\right)^n \leq (0.99)^{-n^2}.$$ 

Now, summing over all pairs $(n, l)$ we see that

$$\sum_{n=1}^{\infty} \sum_{l=1}^{n} \left(\frac{|\Sigma_{n,l}|/D_{n,l}\right)^n$$

converges extremely rapidly. It is this fact that suggests $C_{\text{prim}}(1) < \infty$. Similar heuristic arguments suggest that $C_{\text{prim}}(k) < \infty$ for all $k$. How convincing is this heuristic argument? In its precise details, not very. The heuristic hypothesis is certainly false because the denominators $\delta(v)$ of elements in a cycle are correlated. However, the extreme rapidity of convergence in (3.10) suggests that $C_{\text{prim}}(1) < \infty$ would follow from a much weaker heuristic hypothesis concerning the distribution of $\{N(v) : v \in \Sigma_n\}$ (mod $D_n$). The next section gives general results on the distribution of $\{N(v) : v \in \{0, 1\}^n\}$ (mod $M$) for arbitrary moduli $M$, which show that the distribution is nearly uniform for $M < 2^{0.047n}$, and cannot be too non-uniform for all $M$.

4. Upper bounds for the number of primitive $3x+k$ cycles. We obtain upper bounds for the sums

$$\Phi(x, y) = \sum_{k \leq x \leq y \pmod{6}} C_{\text{prim}}(k, y),$$

where $y = \beta \log x$ for some constant $\beta$.

The general approach to obtaining such upper bounds is to show that for most $v$ the quantity $(N(v), D(v))$ cannot be very large. To do this we study the distribution of $\Sigma_n = \{N(v) : v \in \{0, 1\}^n\}$ (mod $M$) for an arbitrary modulus $M$.

4.1. Distribution of numerators (mod $M$). We study the sets

$$\Sigma_{n,l} = \left\{ \sum_{j=0}^{n-1} v_j 2^{j} 3^{j+1} + \ldots + v_{l-1} : v \in \{0, 1\}^n, \sum_{j=0}^{n-1} v_j = l \right\}$$

and their union

$$\Sigma_n = \bigcup_{n=0}^{n} \Sigma_{n,l} = \left\{ \sum_{j=0}^{n-1} v_j 2^{j} 3^{j+1} + \ldots + v_{n-1} : v \in \{0, 1\}^n \right\}.$$ 

Let $F(n, M)$ count the maximum number of elements of $\Sigma_n$ that occur in any congruence class (mod $M$). Note that the elements in each $\Sigma_{n,l}$ are all distinct by Corollary 2.1a, but those in $\Sigma_n$ need not always be distinct, and in the definition of $F(n, M)$ they are to be counted with multiplicity.

How big ought $F(n, M)$ to be? If the elements of $\Sigma_n$ were uniformly distributed (mod $M$) then about $2^n/M$ elements of $\Sigma_n$ would fall in each residue class (mod $M$). We propose the following conjecture.

**EQUIDISTRIBUTION CONJECTURE.** There exists an absolute constant $c$ such that if $(M, 6) = 1$ then

$$(4.2a) \quad F(n, M) \leq \left\lfloor \frac{n^2}{M} \right\rfloor, \quad M > 2^n,$$

$$(4.2b) \quad F(n, M) \leq \left\lfloor \frac{n^2}{2^n M} \right\rfloor, \quad M \leq 2^n.$$ 

We will show the conjecture is true for “large” $M > 3^n$, which is rather trivial, and also for all “small” $M < 2^{0.047n}$ (Theorem 4.2 below).

We begin with an upper bound for $F(n, M)$ valid for all $M$.

**THEOREM 4.1.** Given $M$ with $(M, 3) = 1$. Define $\alpha$ by $M = 2^{\alpha n}$. Then

$$(4.3a) \quad F(n, M) \leq \left\lfloor \frac{n+1}{2^{\alpha n - \alpha n}} \right\rfloor, \quad \alpha > \log_2 3,$$

$$(4.3b) \quad F(n, M) \leq \left\lfloor \frac{\alpha}{2n 2^{(1-\alpha n)}} \right\rfloor, \quad 0 < \alpha \leq \log_2 3,$$

where $\varphi = (\log_2 3)^{-1} \approx 0.63093$.

**Proof.** We first consider the easy case where $\alpha > \log_2 3$, i.e. $M > 3^n$. The maximum element of $\Sigma_n$ is

$$\sum_{j=0}^{n-1} 2^i 3^{n-i} = 3^n - 2^n,$$

so any two elements of $\Sigma_n$ in a congruence class (mod $M$) necessarily are equal. Now for any $M \in [0, 3^n - 1]$ there can be at most one element of value $M$ in $\Sigma_n$ for $0 \leq M \leq n$ by Corollary 2.1a, hence the value $M$ is taken at most $n+1$ times.

Now consider the more interesting case $0 < \alpha \leq \log_2 3$. Given $v \in \{0, 1\}^n$ write $v = \overline{w} \overline{w}$ where $\overline{w}$ is of length $m$ and $\overline{w}$ is of length $n-m$. Set $\langle \overline{w}, \overline{w} \rangle = \sum_{i=1}^{m} w_i^2$ and let $|\overline{w}|$ denote the length $m$ of $\overline{w}$.
Then

\begin{align}
N(v) &= \left( \sum_{j=0}^{m-1} v_j 3^{3j+1+\ldots+v_{m-1}} \right) 3^{(m+1)} + \left( \sum_{j=0}^{n-m-1} v_j 2^{3j+1+\ldots+v_{n-m-1}} \right) 2^m \\
&= N(w) 3^{(m+1)} + N(\bar{w}) 2^m.
\end{align}

Consider the set of $2^m$ vectors $v \in \{0, 1\}^n$ having a fixed vector $\bar{w}$, and choose $m = \lfloor \varphi n \rfloor$. We claim that for any fixed residue class $r \pmod{M}$ at most $m$ choices of $w \in \Sigma_n$ will yield $v = w \bar{w}$ with $N(v) \equiv r \pmod{M}$. To prove the claim, we prove that there is at most one choice of $w$ for which $\langle w, w \bar{w} \rangle = l$ with $0 \leq l \leq m$ and $N(w \bar{w}) = r$. Suppose not. If there were two different choices $w^{(1)}$ and $w^{(2)}$, giving the residue class $r \pmod{M}$, then (4.5) would give

\[ 3^{(m+1)} (N(w^{(1)}) - N(w^{(2)})) \equiv 0 \pmod{M}. \]

Since $(M, 3) = 1$ this gives

\[ N(w^{(1)}) - N(w^{(2)}) \equiv 0 \pmod{M}. \]

However, the choice of $m = \lfloor \varphi n \rfloor$ guarantees that $0 \leq N(w^{(0)}) < 3^m \leq M$, so (4.6) forces $N(w^{(1)}) = N(w^{(2)})$. Now since $\langle w^{(1)}, w^{(1)} \rangle = \langle w^{(2)}, w^{(2)} \rangle = l$, by Corollary 2.1a one has $w^{(1)} = w^{(2)}$, a contradiction proving the claim. The claim shows that

\[ F(n, M) \leq m 2^{n^2 - m} \leq 2n 2^{11 - o(n)}. \]

We are able to give a much sharper estimate for $F(n, M)$ valid for "small" $M$.

**Theorem 4.2.** Let $M$ be given satisfying $(M, 6) = 1$. If $M = 2^m$, with

\[ \alpha \leq \alpha = \frac{1 - H(\varphi)}{2 - H(\varphi)} = 0.04766, \]

then

\[ F(n, M) \leq 2n^2 2^{11 - 2n}. \]

Here $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ and $\varphi = (\log_2 3)^{-1}$.\]

**Proof.** We start with the decomposition $v \in \{0, 1\}^n$ as $v = w \bar{w}$, where $\bar{w}$ is an arbitrarily placed "window" of $m$ bits, which gives

\[ N(v) = 3^{(m+1)} N(w) + 2^m 3^{(m+1)} N(\bar{w}) + 2^{m+1} 3^{(m+1)} N(\bar{w}). \]

We will choose $m = \lfloor \varphi n \rfloor$ as $M = 2^m > 2n^2$. Now we divide the vectors $w \in \{0, 1\}^n$ into two sets, the normal set are those with $N(\bar{w}) \leq M$ and the oversized set are those with $N(\bar{w}) > M$. We claim that for any residue class $r \pmod{M}$ and any fixed choice of vectors $w, \bar{w}$ there are at most $m$ vectors $\bar{w}$ in the normal set such that $v = w \bar{w}$. This claim is proved the same way as in Theorem 4.1. Hence for a fixed window location, say with $|w| = l$ and $0 \leq l \leq n - m$, at most $(n - m - 1) 2^{m - m} \text{ vectors } v = w \bar{w}$ with $\bar{w}$ normal have $N(v) \equiv r \pmod{M}$. Now we let the window location vary, by varying $l$, and conclude that at most $(n - m)(m) 2^{m - m} \text{ vectors } v$ occur such that

(i) $N(v) \equiv r \pmod{M}$,

(ii) $v$ contains some window vector $w$ of length $m$ that is normal.

It remains to count the number $E$ of exceptional vectors $v$ such that $N(v) \equiv r \pmod{M}$ and all window vectors $w$ inside $v$ are oversize. We bound these by the size $|\Omega|$ of the set $\Omega$ consisting of those vectors $v$ in $\{0, 1\}^n$ all of whose window vectors $w$ of length $m$ are oversize. Suppose $v \in \Omega$. Let $(\bar{w}_0, \ldots, \bar{w}_{n - m - 1})$ denote the $n - m$ possible window vectors of $v$ of length $m$. If $B(j) = v_{j+1} + \ldots + v_{n-1}$ then (4.8) gives

\[ N(v) \geq 2 \sum_{j=0}^{n-m-1} 3^{2n^2 + n} N(\bar{w}_j). \]

Now $v \in \Omega$ implies $N(\bar{w}_j) \geq M$ for all $j$. Summing (4.9) over $l$ yields

\[ (n - m) N(v) \geq \sum_{j=0}^{n-m-1} 2 \sum_{i=0}^{n-m} 3^{2n^2 + n} N(\bar{w}_j) \geq 2^{1+\alpha} \sum_{i=0}^{n-m} 3^{2n^2 + n} \]

\[ \geq 2n^2 \left( \sum_{j=0}^{n-m} 3^{2n^2 + n} \right). \]

Now $N(v) = \sum_{j=0}^{n-m} v_j 3^{2n^2 + n}$, so this inequality yields

\[ n \sum_{j=0}^{n-m} v_j 3^{2n^2 + n} \geq (2n^2 - (n^2 - n) \left( \sum_{j=0}^{n-m} v_j 3^{2n^2 + n} \right) = (n^2 - n)2^n. \]

In particular, there exists some $l$ with $0 \leq l \leq m$ and $2^{1+\alpha} \geq 2^n$. This shows that $B(l) = \varphi(n-l)$, which says that the vector $v \in \Omega$ has at least $\varphi(n-l)$ ones in its last $n-l$ positions, where $l \leq m \leq n$. This restriction on $v \in \Omega$ yields the bound

\[ |\Omega| \leq \sum_{l=0}^{n-m} 2 \left( \sum_{j=0}^{n-l} \binom{n}{j} \right). \]

To simplify this inequality, we use a bound ([11], Lemma 4.7.2) for the tail of the binomial distribution:

\[ \sum_{j=ak}^n \binom{n}{j} \leq 2^{H(\alpha k)}, \]

valid for $\alpha \geq \frac{1}{2}$, where $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ is the binary entropy function. This yields

\[ |\Omega| \leq \sum_{l=0}^{n-m} 2^{1+\alpha} \leq m 2^{m+1} 2^{H(\alpha(n-l))} \leq m 2^{m+1} 2^{H(\alpha(1-o(n)))}, \]

where $H(\varphi) = 0.949955.$
Thus for \((M, 6) = 1\) we obtain the bound

\[
F(n, M) \leq (n-m)(m)2^{n-m} + |O| \leq (n-1)4n^2 2^{1-\alpha}n + n2^{an+H(\alpha)(1-\alpha)n}.
\]

This yields

\[
F(n, M) \leq 4n^2 2^{1-\alpha}n,
\]

whenever \((1-\alpha)n \geq \alpha n + H(\alpha)(1-\alpha)n\), and this condition simplifies to

\[
\alpha \leq \alpha_c = \frac{1-H(\alpha)}{2-H(\alpha)} \approx 0.476598.
\]

The upper bounds for \(n^{-1} \log F(n, 2^n)\) obtained in Theorems 4.1 and 4.2 are graphed in Fig. 4.1 by the heavy line. The flat segment between \(x_c\) and 1 is proved by a modification of the proof of Theorem 4.2 that we omit: one chooses \(m = \lceil x_c n - 2 \log_2 n - 1 \rceil\) for \(x_c \leq x \leq (\log_2 3)x_c\). The dotted line in Fig. 4.1 indicates the upper bound for \(n^{-1} \log F(n, 2^n)\) asserted by the Equidistribution Conjecture.

![Fig. 4.1. Upper bounds for \(n^{-1} \log F(n, 2^n)\) (dotted line indicates Equidistribution Conjecture)](image)

It is a peculiar fact that the argument of Theorem 4.2 completely loses its strength at the critical value \(x_c\). To obtain improved bounds for \(\alpha > \alpha_c\) by this approach apparently requires improved bounds either for the number of elements in the exceptional set or for \(|O|\).

### 4.2. Upper bounds for \(\Phi(x, y)\) and \(C_{\text{prim}}(k, \beta \log k)\)

We study

\[
\Phi(x, y) = \sum_{k \leq x, k = 1 \pmod{y}} C_{\text{prim}}(k, y)
\]

for \(y = \beta \log x\) as \(x \to \infty\) with \(\beta\) held constant. The count of all primitive cycles of length \(\leq \beta \log x\) is the "trivial" upper bound for this sum:

\[
\Phi(x, \beta \log x) \leq \sum_{n=1}^{\lceil \beta \log x \rceil} I(n).
\]

and this yields

\[
\Phi(x, \beta \log x) \leq \sum_{n=1}^{\lceil \beta \log x \rceil} \frac{2^n}{\log_2 x} + O(\beta \log x),
\]

where \(H(\alpha) = 0.949955\). (To prove this, one excludes all \(v\) with \(D(v) = [2^a - 3^b] > 2^{\log_2 x}\), arguing as in [10], Theorem D.)

The results of the previous section enable one to show that for \(\beta > 1\) the "trivial" upper bound (4.13) can be improved.

**Theorem 4.3.** For \(\beta > 1\) one has

\[
\Phi(x, \beta \log x) \leq 4(\beta \log x)^6 x^{(1-\beta_\theta)} + c_\theta \log \log x,
\]

where

\[
f(\beta) = \begin{cases} 1 & \text{if } 1 \leq \beta \leq \beta_\theta = (1-\alpha) \approx 1.05005, \\ (1-\beta) + \frac{\beta}{\beta_\theta} & \text{if } \beta > \beta_\theta, \\ 0 & \text{if } \beta < 1,
\end{cases}
\]

with \(\beta_\theta = (\log_2 3)^{-1} \approx 0.63093\), and \(c_\theta\) is an absolute constant.

**Proof.** Let \(n = \log x\), and consider all 0-1 vectors \(v\) of length \(\lceil \beta n \rceil\). For simplicity in what follows we treat \(\beta n\) as an integer; the proof works with \(\lceil \beta n \rceil\) replacing \(\beta n\) throughout. How many of these \(v\) can produce an \(x(v)\) which in lowest terms has a denominator \(\delta(v) < x\)? To begin with, the unreduced denominator

\[
D(v) = 2^{\beta n} - 3\]

takes \(\beta n + 1\) possible values. For each one of these values it has at most \(2^{\beta n / \log \log x}\) possible divisors \(M\), for an absolute constant \(c_\theta\). Using (3.3) one has

\[
|D(v)| \geq (\beta n)^{-\gamma} 2^{\gamma n} \geq x^{(1-\beta_\theta)} (\beta \log x)^{\gamma},
\]

and this implies that in order to have \(|D(v)|/M| \leq x\) one must have

\[
M \leq (\beta \log x)^{-\gamma} x^{\gamma - 1} = (\beta n)^{\gamma - 1} 2^{\gamma n - 1}.
\]

Now for any fixed divisor \(M\) let \(F_0(n, M) = \# \{v \in \{0, 1\}^n : M|N(v)\}\). Since \(F_0(n, M) \leq F(n, M)\) Theorems 4.1 and 4.2 can be used to bound the number of such \(M\). They give

\[
F_0(\beta n, M) \leq 2\beta n 2^{\beta n}/M^* \quad \text{if } M \leq 3^{2n},
\]

\[
F_0(\beta n, M) \leq (\beta n)^{\gamma} 2^{\gamma n}/M \quad \text{if } M \leq 2^{\gamma n}.\]
Now (4.17) gives $M \geq 2^{2^{n+1}}$ with

$$a_0 = 1 - \frac{1}{\beta} \log \beta n.$$  

Hence the number $G(n, \beta n)$ of $\nu$ of length $\beta n$ yielding a cycle with $\delta(\nu) \leq 2^n$ is bounded by

$$G(n, \beta n) \leq \sum_{i=0}^{n} \sum_{M > 2^{2^{n+1}}} \mathcal{F}_i(\beta n, M)$$

$$\leq (\beta \log x + 1)x^{c_0/\log \log x}(2(\beta \log x)^d x^{f(\beta)})$$

where $f(\beta)$ is given by (4.16). Since the right side of (4.18) is a monotone increasing function of $\beta$, we have

$$\Phi(x, \beta \log x) \leq \sum_{j=1}^{bn} G(n, j) \leq \beta n G(n, \beta n) \leq 4(\beta \log x)^{b} x^{f(\beta) + c_0/\log \log x}.$$  

Remarks. (1) The proof gave away a few powers of logarithms more than necessary for $\beta > \beta_c$.

(2) It is known that for any $\epsilon > 0$ one has $d(B) \leq B^{1+\epsilon/\log \log B}$ for all sufficiently large $B > B_0(\epsilon)$. Hence any $c_0 > 1$ can be used in (4.15) provided that a suitable multiplicative constant is added.

(3) The Equidistribution Conjecture implies that

$$\Phi(x, \beta \log x) \leq C(\beta, \epsilon) x^{1+\epsilon}$$

holds for all $x$, where $C(\beta, \epsilon)$ is a constant depending on $\beta$ and $\epsilon$.

(4) A similar proof gives the upper bound

$$C_{\text{prim}}(k, \beta \log k) \leq \sum_{m=1}^{k \log \log k} \mathcal{F}_m \left( m, \frac{2^m - 3^m}{k} \right)$$

$$\leq 4(\beta \log k)^{\delta} k^{f(\beta)},$$

valid for $\beta > 1$, where $f(\beta)$ is given by (4.16). This upper bound is close to the occasional large values of $C_{\text{prim}}(k)$ given by Theorem 3.3, for $\beta < \beta_c$.

References


