CARRY PROPAGATION IN SIGNED DIGIT REPRESENTATIONS

CLEMENS HEUBERGER AND HELMUT PRODINGER

Abstract. Von Neumann's addition method adds two numbers given in q-ary representation by forming a number consisting of the added digits, reduced modulo q, and another number, representing the carries and repeating this until the string of carries consists only of zeros. The average number of iterations was studied by Knuth.

We extend these results by considering the (q, d) system, with base q and digits $d, d+1, \dots, d+q-1$, as well as the *symmetric signed digit expansions,* for even q, with digits $-q/2, \dots, q/2$, and a special rule to make representations of integers unique.

1. Introduction

Knuth [5] has analyzed Burks', Goldstine's, and von Neumann's addition algorithm [1, Section 5.6]: Assume that two integers are given in q-ary notation, say $(\dots x_2x_1x_0)_q$ and $(\dots y_2y_1y_0)_q$; then the integer $(\dots z_2z_1z_0)_q$ with $z_i = (x_i + y_i) \bmod q$ is formed, as well as $(\dots c_2c_1c_0)_q$ (the carries), where $c_{i+1} = [x_i + y_i \geq q]$.[1] The process is iterated by adding $(\dots z_2z_1z_0)_q$ and $(\dots c_2c_1c_0)_q$ until the string of carries contains only zeros.

Knuth studied the average number of iterations, assuming two random integers with n digits. The result is $\sim \log_q n$; a more precise version will appear later in this paper. It turns out that the longest subsequence of the form $\dots i(q-1)(q-1)\dots(q-1)j\dots$ with $i \neq q-1$ and $j \geq q$ in $\big(\dots(x_2+y_2)(x_1+y_1)(x_0+y_0)\big)_q$ is responsible for the number of iterations. While this instance is not hard to model directly, it is useful to imagine the situation by using an automaton,[2] see Figure 1.

The longest sequence of solid edges that is passed while scanning the input "word" $\dots(x_2+y_2)(x_1+y_1)(x_0+y_0)$ plus two is the number of iterations.

In this paper our aim is to extend Knuth's results to other positional number systems. We still use the basis $q \geq 2$, but a second (integer) parameter d with $-(q-1) \leq d \leq 0$ and the set of q digits $\{d, d+1, \dots, d+q-1\}$. If $d \neq 0$ and $d \neq -(q-1)$ then we have positive and negative digits and it is not hard to see that every integer can then be uniquely represented as $\sum a_k q^k$ with $a_k \in \{d, d+1, \dots, d+q-1\}$. The most popular such system is the balanced ternary with $q = 3$ and digits $\{\bar{1}, 0, 1\}$.[3] See [6,

---

This paper was written while the first author was a visitor at the John Knopfmacher Centre for Applicable Analysis and Number Theory, School of Mathematics, University of the Witwatersrand, Johannesburg. He thanks the centre for its hospitality.

[1]We use Iverson's notation: $[P] = 1$ if condition P is true, 0 otherwise, compare [3].

[2]In this paper, all automata read strings (representations of integers) from right to left, i. e. starting with the least significant digit.

[3]Often, we will write $\bar{1}$ instead of -1, etc.

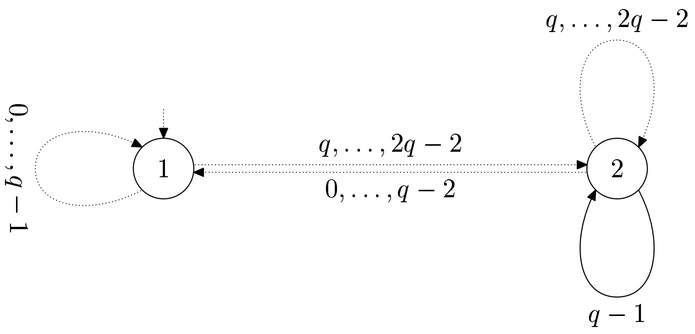


FIGURE 1. Automaton to find carry generating sequences in the q-ary number system.

Section 4.1] for more background on positional number systems. The addition of two integers given in this (q,d) system works as before, with carries if $x_i + y_i$ is outside the allowed range $d, d+1, \ldots, d+q-1$. Note carefully that carries might now be ± 1 and that the sequence of sums might be oscillating, being smaller or larger than the true value of the sum of the two integers (cf. Table 1). This is in sharp contrast to the traditional q-ary system, where the sums are monotonically increasing until the algorithm stops. Thus it is perhaps natural that the description of subsequences being responsible for the number of iterations is significantly more complicated; the corresponding automata are described in later sections. The asymptotic result $\sim \log_q n$ appears again, but the parameter d influences the next term in the asymptotic expansion.

$(12\bar{1}\bar{1}\bar{1}13)_{(5,-1)}$	$= (\ldots x_2x_1x_0)_{(5,-1)}$	$= 21108$
$(22\bar{1}0\bar{1}23)_{(5,-1)}$	$= (\ldots y_2y_1y_0)_{(5,-1)}$	$= 36863$
$(3\bar{1}3\bar{1}331)_{(5,-1)}$	$= (\ldots z_2z_1z_0)_{(5,-1)}$	$= 45591$
$(1\bar{1}0\bar{1}010)_{(5,-1)}$	$= (\ldots c_2c_1c_0)_{(5,-1)}$	$= 12380$
$(\bar{1}3333\bar{1}1)_{(5,-1)}$	$= (\ldots z_2z_1z_0)_{(5,-1)}$	$= -3929$
$(1\bar{1}0\bar{1}0100)_{(5,-1)}$	$= (\ldots c_2c_1c_0)_{(5,-1)}$	$= 61900$
$(13323\bar{1}\bar{1}1)_{(5,-1)}$	$= (\ldots z_2z_1z_0)_{(5,-1)}$	$= 135971$
$(\bar{1}0001000)_{(5,-1)}$	$= (\ldots c_2c_1c_0)_{(5,-1)}$	$= -78000$
$(0332\bar{1}\bar{1}\bar{1}1)_{(5,-1)}$	$= (\ldots z_2z_1z_0)_{(5,-1)}$	$= 57346$
$(00010000)_{(5,-1)}$	$= (\ldots c_2c_1c_0)_{(5,-1)}$	$= 625$
$(0333\bar{1}\bar{1}\bar{1}1)_{(5,-1)}$	$= (\ldots z_2z_1z_0)_{(5,-1)}$	$= 57971$
$(00000000)_{(5,-1)}$	$= (\ldots c_2c_1c_0)_{(5,-1)}$	$= 0$

TABLE 1. Example for carry propagation in the (q,d) system with $q = 5$ and $d = -1$.

If q is odd, then the system with a symmetric set of digits $\{-\frac{q-1}{2},\dots,\frac{q-1}{2}\}$ is of special interest, since it minimizes the value $\sum |a_k|$ (the sum of absolute digits), as was shown in [4]. For even q, no (q,d) system can have a symmetric set of digits, but as was also shown in [4], there is a certain symmetric system that again minimizes the sum of absolute digits: It uses digits $-\frac{q}{2},\dots,\frac{q}{2}$, whence it is redundant. However, there are rules describing when $q/2$ resp. when $-q/2$ must be used, making the system unique. If a number m shall be represented, and if $m \equiv \frac{q}{2} \mod q$, then $q/2$ is used iff $\{\frac{m}{q^2}\} < \frac{1}{2}$,[4] and the process is repeated after subtracting the digit and dividing by q. Equivalently, one can notice that left of digit $q/2$ only digits i with $0 \le i \le q/2-1$ are allowed, and left of digit $-q/2$ only digits i with $-q/2+1 \le i \le 0$ are allowed. We will use the name "symmetric signed digit expansion."

The adaption of von Neumann's algorithm to this situation works as follows: When adding two digits, the result is in the range $-q,\dots,q$, and numbers $q/2+1,\dots,q$ would result in $-q/2+1,\dots,0$ and a carry of 1, while numbers $-q,\dots,-q/2-1$ would result in $0,\dots,q/2-1$ and a carry of -1. The digits $\pm q/2$ require special care. If we have $q/2$, then the algorithm to produce the symmetric signed digit expansion would look at $\{m/q^2\}$, and if that would be $\ge 1/2$ would replace $q/2$ by $-q/2$, with a carry of 1. This decision can however be made solely by looking at the position to the left of $q/2$. If there is z, and $z \mod q \ge q/2$, then we replace $q/2$ by $-q/2$, with a carry of 1, otherwise not. The situation when we see $-q/2$ is completely symmetric. So we might say that a carry is triggered when admissibility is violated.

The analysis of this system is somehow more complicated than the (q,d) system. Although there are symmetries that make computations a bit simpler, the digits are no longer equally likely (in the (q,d) system each digit tends to occur with the same frequency $1/q$)! The balancing that has been achieved results in the fact that the digits $\pm q/2$ (together) occur only with frequency $1/(q+1)$, and the digit zero accordingly more often. The system $q=2$, which is the one that has been known before [4], see e. g. [7] and the references in [4], requires a special treatment. This is too technical to be described in the introduction.

We use the following methods to achieve our results: Appropriate automata are set up, and the longest run of solid edges is the parameter of interest. In order to model this we are interested in all runs through the automaton where the lengths of runs of solid edges are $\le k$. For that, we basically have to double the size of the underlying transition matrix. This leads to a generating function that can be achieved by heavy use of computer algebra. From that, an adaptation of Knuth's bootstrapping method allows to approximate the average value of the number of iterations of von Neumann's algorithm by a series involving exponential functions. The asymptotic study of such series is, however, well known (by Mellin transform techniques, see e. g. [2]), leading to the results.

[4] We use $\{x\}$ for the fractional part of x.

2. (q,d) Expansions

Let $q \geq 3$ and $-q+2 \leq d \leq -1$. It is well known that every integer x has a unique (q,d) expansion

$$x = \sum_{j \geq 0} x_j q^j, \qquad x_j \in \{d, \ldots, d+q-1\},$$

where $x_j \neq 0$ only holds for finitely many j.

For two integers x and y with (q,d) expansions[5] $\mathbf{x}$ and $\mathbf{y}$ we define $(\mathbf{z}, \mathbf{c}) := \operatorname{add}(\mathbf{x}, \mathbf{y})$ by

$$\begin{aligned} c_0 &:= 0, \\ c_{j+1} &:= \left\lfloor \frac{x_j + y_j - d}{q} \right\rfloor, && j \geq 0, && (1)\\ z_j &:= x_j + y_j - c_{j+1} q, && j \geq 0. && (2) \end{aligned}$$

It is easily seen that these definitions imply $c_j \in \{0, \pm 1\}$ and $d \leq z_j \leq d+q-1$ for $j \geq 0$. Furthermore, definition (2) yields

$$\sum_{j \geq 0} x_j q^j + \sum_{j \geq 0} y_j q^j = \sum_{j \geq 0} z_j q^j + \sum_{j \geq 0} c_j q^j. \tag{3}$$

It follows that $\mathbf{z}$ is the (q,d) expansion for $x+y$ if $\mathbf{c} = \mathbf{0}$.

If $\mathbf{c} \neq \mathbf{0}$, we may iterate the process: We set $\mathbf{z}^{(0)} := \mathbf{x}$, $\mathbf{c}^{(0)} := \mathbf{y}$, and

$$(\mathbf{z}^{(k+1)}, \mathbf{c}^{(k+1)}) := \operatorname{add}(\mathbf{z}^{(k)}, \mathbf{c}^{(k)}), \qquad k \geq 0. \tag{4}$$

We will prove in Lemma 2.2 that this process yields $\mathbf{c}^{(k)} = \mathbf{0}$ for some k, and therefore the (q,d) expansion of $x+y$ is given by $\mathbf{z}^{(k)}$. The first iteration where this happens will be denoted by

$$t(\mathbf{x}, \mathbf{y}) := \min\{k \geq 0 : \mathbf{c}^{(k)} = \mathbf{0}\}. \tag{5}$$

Our aims are to give a syntactical description of all (q,d) expansions $\mathbf{x}$ and $\mathbf{y}$ with $t(\mathbf{x}, \mathbf{y}) = k$ for a given k and to calculate the asymptotic behavior of the expected value t_n of $t(\mathbf{x}, \mathbf{y})$ where $\mathbf{x}$ and $\mathbf{y}$ range over all sequences of allowed digits of length n.

2.1. Syntactical Properties.

Throughout this section, we will assume that $\mathbf{x}$ and $\mathbf{y}$ are the (q,d) expansions of given integers x and y and that $(\mathbf{c}^{(k)})_{k \geq 0}$ and $(\mathbf{z}^{(k)})_{k \geq 0}$ are given by (4).

Lemma 2.1. *Let $j \geq 0$ and $k \geq 1$.*

1. *If $c_{j+1}^{(k+1)} \neq 0$, then $c_{j+1}^{(k+1)} = c_j^{(k)}$.*
2. *If $c_j^{(k)} = 0$, then $z_j^{(k+1)} = z_j^{(k)}$.*
3. *$c_j^{(j+k)} = 0$.*
4. *Let $c_j^{(k)} \neq 0$ and $l \geq 1$ minimal such that $c_j^{(k+l)} \neq 0$. Then $c_j^{(k+l)} = -c_j^{(k)}$.*

[5]We will denote infinite sequences $(x_j)_{j \geq 0}$ by boldface symbols. If the range is clear from the context, we will also use boldface symbols for finite sequences.

(5) *If* $c_{j+1}^{(k+1)} \neq c_j^{(k)}$, *then* $c_{j+1}^{(k+m)} = 0$ *for all* $m \geq 1$.

Proof. We will repeatedly use the fact that $d \leq x \leq d+q-1$ is equivalent to $|x-\mu| \leq (q-1)/2$ for $\mu = d + (q-1)/2$. Furthermore, for $m \geq 0$ and $\sigma \in \{\pm 1\}$, the equation $c_{j+1}^{(m+1)} = \sigma$ holds if and only if $\sigma(z_j^{(m)} + c_j^{(m)} - \mu) \geq (q+1)/2$.

(1) From $c_{j+1}^{(k+1)}(z_j^{(k)} + c_j^{(k)} - \mu) \geq (q+1)/2$ and $|z_j^{(k)} - \mu| \leq (q-1)/2$ we conclude $c_{j+1}^{(k+1)} c_j^{(k)} \geq 1$.
(2) This follows from part 1 and (2).
(3) Applying part 1 j times, we conclude that $c_j^{(j+k)}$ is zero or equal to $c_0^{(k)}$, which vanishes by definition.
(4) We use induction on j. For $j = 0$, there is nothing to show. Assume that $c_j^{(k)} = 1$. Then $z_{j-1}^{(k)} = z_{j-1}^{(k-1)} + c_{j-1}^{(k-1)} - q \leq q + 2d - 2 \leq q + d - 3$. By induction hypothesis, we have $|\sum_{m=0}^{l-1} c_{j-1}^{(k+m)}| \leq 1$, and therefore
$$z_{j-1}^{(k+l-1)} + c_{j-1}^{(k+l-1)} = z_{j-1}^{(k)} + \sum_{m=0}^{l-1} c_{j-1}^{(k+m)} - q \sum_{m=1}^{l-1} c_j^{(k+m)} \leq q + d - 2.$$
This implies that $c_j^{(k+l)} \neq 1$. The case $c_j^{(k)} = -1$ is analogous.
(5) By part 1, we have $c_{j+1}^{(k+1)} = 0$. If there is no $l \geq 1$ such that $c_j^{(k+l)} \neq 0$, we are done by part 1. Otherwise, we take $l \geq 1$ minimal with $c_j^{(k+l)} \neq 0$ and conclude from part 1 that $c_{j+1}^{(k+2)} = \cdots = c_{j+1}^{(k+l)} = 0$ and from part 4 that $c_j^{(k+l)} = -c_j^{(k)}$. The assumption $c_{j+1}^{(k+1)} = 0$, (2) and part 2 yield $z_j^{(k)} + c_j^{(k)} = z_j^{(k+1)} = \cdots = z_j^{(k+l)}$. This implies $d \leq z_j^{(k)} = z_j^{(k+l)} + c_j^{(k+l)} \leq d + q - 1$ and therefore we have $c_{j+1}^{(k+l+1)} = 0$. We iterate this procedure until we do not find any l with $c_j^{(k+l)} \neq 0$. By part 3 this will be the case after a finite number of steps.

□

Lemma 2.2. *Let* $J := \max\{j : x_j + y_j \neq 0\}$. *Then* $t(\mathbf{x}, \mathbf{y}) \leq J + 2$.

Proof. By Lemma 2.1, part 3, $c_j^{(J+2)} = 0$ for $0 \leq j \leq J+1$.

Next, we prove $c_{J+2}^{(k)} = 0$ by induction on k. $c_{J+2}^{(0)} = 0$ holds by definition. For $k \geq 0$, we have $z_{J+1}^{(k)} + c_{J+1}^{(k)} = z_{J+1}^{(0)} + \sum_{l=0}^{k} c_{J+1}^{(l)} - q \sum_{l=1}^{k} c_{J+2}^{(l)}$. By induction hypothesis and Lemma 2.1, part 4 we see that $|z_{J+1}^{(k)} + c_{J+1}^{(k)}| \leq 1$. This implies $c_{J+2}^{(k+1)} = 0$.

For $j > J+2$, the relation $c_j^{(J+2)} = 0$ follows from Lemma 2.1, part 1. □

Proposition 2.3. *Let* $k \geq 1$. *Then the following properties are equivalent:*

(1) $t(\mathbf{x}, \mathbf{y}) \geq k + 1$.

(2) *There is a* $j \geq 0$ *and a sequence* $(s_l)_{1 \leq l \leq k} \in \{\pm 1\}^k$ *such that*

$$s_1 \left(x_j + y_j - d - \frac{q-1}{2} \right) \geq \frac{q+1}{2}, \tag{6}$$

$$x_{j+l} + y_{j+l} = \begin{cases} d+q-1 & \text{if } s_l = 1 \quad \text{and } s_{l+1} = 1, \\ d-1 & \text{if } s_l = 1 \quad \text{and } s_{l+1} = -1, \\ d+q & \text{if } s_l = -1 \text{ and } s_{l+1} = 1, \\ d & \text{if } s_l = -1 \text{ and } s_{l+1} = -1, \end{cases} \qquad 1 \leq l \leq k-1. \tag{7}$$

(3) *There is a* $j \geq 0$ *such that the subsequence* $(x_{j+l} + y_{j+l})_{0 \leq l \leq k-1}$ *of length* k *is "accepted" (by considering* 1, 2, 3 *as final states; all edges not shown are leading to a "sink") by the finite automaton given in Figure 2.*

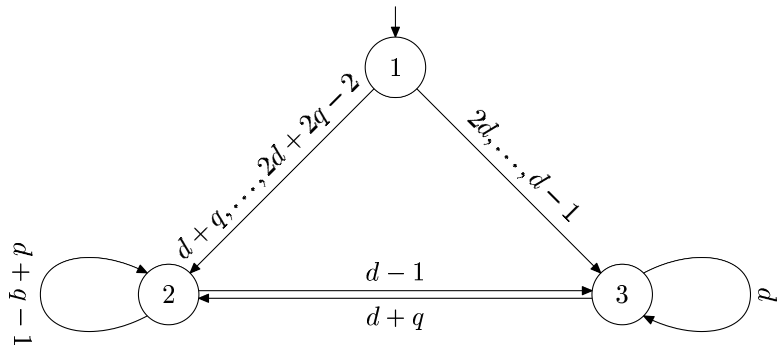


FIGURE 2. Automaton recognizing subsequences of length k which require $k+1$ carries in the (q,d) expansion.

Proof. We first prove that 1 implies 2. If $\mathbf{x}$, $\mathbf{y}$ induce $k+1$ carries, there is some integer j such that $c_{j+k}^{(k)} = \sigma$ for some $\sigma \in \{\pm 1\}$. Lemma 2.1, parts 3 and 1 imply that $j \geq 0$ and $c_{j+l}^{(l)} = \sigma$ for $1 \leq l \leq k$. Lemma 2.1, parts 5 and 1 yield $c_{j+l+1}^{(m+1)} = c_{j+l}^{(m)}$ for $1 \leq l \leq k-1$ and $1 \leq m \leq l$.

For $1 \leq l \leq k$ we define $m_l := \min\{m \geq 1 : c_{j+l}^{(m)} \neq 0\}$ and $s_l := c_{j+l}^{(m_l)}$. This implies $c_{j+l+1}^{(1)} = -s_l\,[s_{l+1} \neq s_l]$ for $1 \leq l \leq k-1$. We obtain

$$\begin{aligned} z_{j+l}^{(l)} &= z_{j+l}^{(0)} + c_{j+l}^{(0)} + \sum_{m=1}^{l-1} c_{j+l}^{(m)} - q \sum_{m=1}^{l-1} c_{j+l+1}^{(m+1)} - q c_{j+l+1}^{(1)} \\ &= x_{j+l} + y_{j+l} + \sigma(q-1)\,[s_l = -\sigma] + q s_l\,[s_{l+1} \neq s_l] \end{aligned} \tag{8}$$

for $1 \leq l \leq k-1$.

For $0 \leq l \leq k-1$, the equation $c_{j+l+1}^{(l+1)} = \sigma$ implies that $\sigma(z_{j+l}^{(l)} + c_{j+l}^{(l)} - \mu) \geq (q+1)/2$, where $\mu = d + (q-1)/2$ is defined as in the proof of Lemma 2.1. We note that $\sigma = s_1$ and set $l = 0$ to get (6). For $1 \leq l \leq k-1$ we have $c_{j+l}^{(l)} = \sigma$, and we conclude that $\sigma(z_{j+l}^{(l)} - \mu) \geq (q-1)/2$. Since $d \leq z_{j+l}^{(l)} \leq d+q-1$, equality must hold. Therefore, we get

$z_{j+l}^{(l)} = d + (1+\sigma)(q-1)/2$. Combining this with (8) and studying the various choices for s_l, s_{l+1}, and σ yields (7).

We will now prove the other direction. Inequality (6) implies $c_{j+1}^{(1)} = s_1$. From (7) we see that

$$c_{j+l+1}^{(1)} = s_{l+1} \left[s_l \neq s_{l+1} \right], \qquad z_{j+l}^{(1)} = \mu + s_l(q-1)/2 \tag{9}$$

for $1 \leq l \leq k-1$.

As previously, we define $m_l = \min\{m \geq 1 : c_{j+l}^{(m)} \neq 0\}$ for $1 \leq l \leq k$. We claim that

$$s_l = c_{j+l}^{(m_l)}, \qquad 1 \leq l \leq k, \tag{10}$$

$$c_{j+l}^{(m)} = c_{j+l+1}^{(m+1)}, \qquad 1 \leq m \leq l \leq k-1. \tag{11}$$

We prove the claim by induction on l. For $l = 1$, equation (10) has already been observed. Since $z_{j+1}^{(1)} + c_{j+1}^{(1)} = \mu + s_1(q+1)/2$, we have $c_{j+2}^{(2)} = s_1 = c_{j+1}^{(1)}$, which proves (11).

Assume now that $l \geq 2$ and prove first (10). By (9) the only interesting case is $s_l = s_{l-1}$, which implies $m_l \geq 2$. Using the induction hypothesis, we get $m_l = m_{l-1} + 1$ and (10) follows.

To prove (11), we proceed by induction on m. By Lemma 2.1, part 1 the only interesting case is $c_{j+l}^{(m)} \neq 0$. From (9), the induction hypothesis and Lemma 2.1, part 4, we get

$$\begin{aligned} z_{j+l}^{(m)} &= z_{j+l}^{(1)} + \sum_{t=1}^{m-1} c_{j+l}^{(t)} - q \sum_{t=1}^{m-1} c_{j+l+1}^{(t+1)} \\ &= \mu + s_l(q-1)/2 + (1-q)s_l \left[s_l = -c_{j+l}^{(m)} \right]. \end{aligned}$$

This yields $z_{j+l}^{(m)} + c_{j+l}^{(m)} = \mu + c_{j+l}^{(m)}(q+1)/2$, and therefore $c_{j+l+1}^{(m+1)} = c_{j+l}^{(m)}$, which completes the proof of the claim.

Applying (11) for $m = l$ and $1 \leq l \leq k-1$ yields $c_{j+k}^{(k)} = c_{j+k-1}^{(k-1)} = \cdots = c_{j+1}^{(1)} = s_1 \neq 0$, which proves that there are at least $k+1$ carries.

The equivalence of 2 and 3 is clear if we associate node 1 to $l = 0$, node 2 to $s_l = 1$ and node 3 to $s_l = -1$. □

We modify the automaton given in Figure 2 in such a way that it reads the sequence $(x_j + y_j)_{j \geq 0}$ in one run and decides whether $t(\mathbf{x}, \mathbf{y}) \leq k+1$ for a $k \geq 1$. To this aim, it has to decide whether all subsequences that are accepted by the old automaton have length $\leq k$. It is clear that maximal accepted subsequences (i. e. accepted subsequences which are not a prefix or a suffix of an accepted subsequence) do not overlap, but they may be adjacent.

If an accepted subsequence ends with some digit which is not contained in the drawing of the old automaton (i. e., a digit leading to the invisible sink), then we immediately have to restart with the same digit. As an example, consider the case that we read a digit $2d \neq d-1$ in node 2. We have to go immediately to node 3, counting this move as the first digit in the new run to accept the new subsequence. In order to facilitate counting, we do not count the first edge that is accepted by the old automaton, and add 1 afterwards.

We introduce all transitions which we do not count as "dotted edges:" These are the two old edges from node 1 to nodes 2 and 3, and all edges which are missing in the old automaton. The result is shown in Figure 3. Therefore, maximal subsequences of length l which are accepted by the old automaton correspond to $l-1$ consecutive solid edges when reading the whole word in the new automaton. Therefore, $t_n(\mathbf{x},\mathbf{y}) \le k+1$ if and only if the automaton does not traverse $k-1$ consecutive solid edges when reading $(x_j+y_j)_{j\ge 0}$. We summarize these results in the following theorem.

Theorem 2.4. (1) *$t(\mathbf{x},\mathbf{y})=0$ if and only if $\mathbf{y}=0$.*
(2) *$t(\mathbf{x},\mathbf{y}) \le 1$ if and only if $d \le x_j+y_j \le d+q-1$ for all $j \ge 0$.*
(3) *Let $k \ge 0$. Then $t(\mathbf{x},\mathbf{y}) \le k+2$ if and only if the automaton in Figure 3 does not traverse more than k consecutive solid edges when reading[6] the sequence $(x_j+y_j)_{j\ge 0}$.*

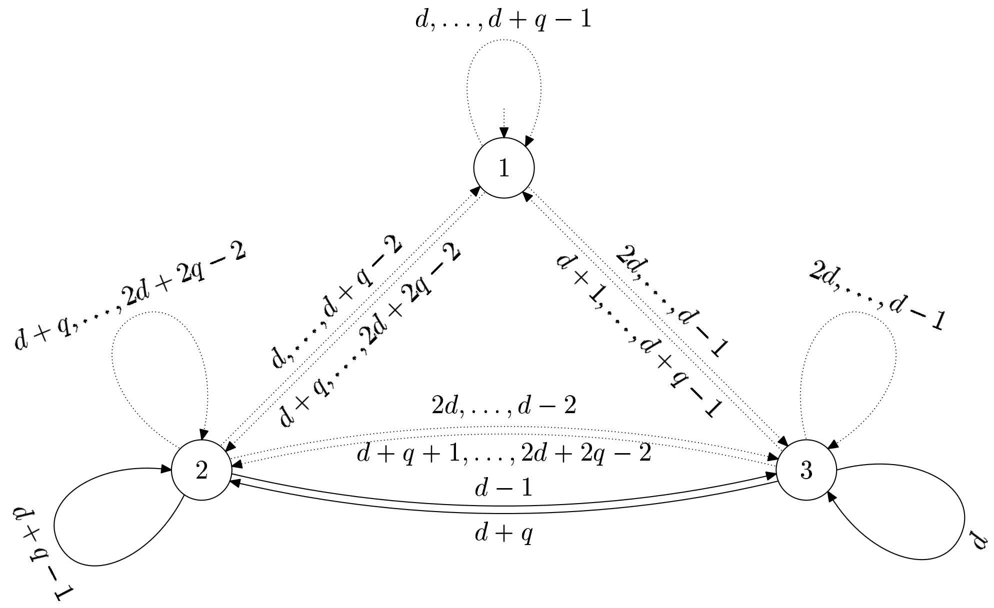


FIGURE 3. $t(\mathbf{x},\mathbf{y}) \le k+2$ if and only if at most k consecutive solid edges are traversed when processing $\mathbf{x}+\mathbf{y}$.

2.2. **Generating Functions.** We are interested in the expected value t_n of $t(\mathbf{X},\mathbf{Y})$, where $\mathbf{X}=(X_j)_{0\le j\le n-1}$ and $\mathbf{Y}=(Y_j)_{0\le j\le n-1}$ are (independent) random sequences $\in \{d,\dots,d+q-1\}^n$. The equidistribution measure $\mathbb{P}_n$ on $\{d,\dots,d+q-1\}^n$ is simply the product of the equidistribution measure $\mathbb{P}_1$ on $\{d,\dots,d+q-1\}$. The aim of this section is to calculate a probability generating function $G^{\le k}(z)=\sum_{n\ge 0} p_{nk} z^n$, where $p_{nk} := \mathbb{P}_n(t(\mathbf{X},\mathbf{Y}) \le k+2)$ for $k \ge 0$.

[6]Strictly speaking, the automaton reads the sequence $(x_j+y_j)_{0\le j\le J}$ for some J such that $x_j+y_j=0$ for $j>J$.

Since the automaton in Figure 3 reads $(X_j+Y_j)_{0\le j\le n-1}$, we have to calculate $w(i) := \mathbb{P}_1(X_j+Y_j=i)$. An elementary computation leads to the following weights of digits:

$$w(i)=\begin{cases}\frac{i+1-2d}{q^2} & \text{if } 0\le i-2d\le q-1,\\ \frac{2q-1-i+2d}{q^2} & \text{if } q-1<i-2d\le 2q-2,\\ 0 & \text{otherwise.}\end{cases}$$

We must compute (probability) generating functions of the type $F_{ij}(z)$, where the coefficient of z^n is the probability to reach state j when starting in state i, assuming a random word of length n.

Using the weights $w(i)$ accordingly for the edges in the automaton in Figure 3 and the variable z to label letters (digits) we can write the transition matrix T as $T=B+R$ with

$$B := \frac{z}{q^2}\begin{pmatrix} \frac{q^2}{2}+\frac{q}{2}-dq-d^2+d & \frac{q^2}{2}-\frac{q}{2}+dq+\frac{d^2}{2}-\frac{d}{2} & \frac{d^2}{2}-\frac{d}{2}\\ \frac{q^2}{2}-\frac{q}{2}-dq-d^2 & \frac{q^2}{2}-\frac{q}{2}+dq+\frac{d^2}{2}-\frac{d}{2} & \frac{d^2}{2}+\frac{d}{2}\\ \frac{q^2}{2}+\frac{q}{2}-dq-d^2+2d-1 & \frac{q^2}{2}-\frac{3q}{2}+dq+\frac{d^2}{2}-\frac{3d}{2}+1 & \frac{d^2}{2}-\frac{d}{2}\end{pmatrix}$$

and

$$R := \frac{z}{q^2}\begin{pmatrix} 0 & 0 & 0\\ 0 & q+d & -d\\ 0 & q+d-1 & -d+1\end{pmatrix}.$$

Note that the matrix B describes the dotted, R the solid edges. We need the quantities

$$\mathcal{R}_{ij}=\sum_{l\ge1}R^l_{ij}=\left((I-R)^{-1}-I\right)_{ij},$$

describing nonempty paths from i to j, using only solid edges. We find

$$\mathcal{R}=\frac{1}{(q-z)(q^2-z)}\begin{pmatrix} 0 & 0 & 0\\ 0 & z(q^2+dq-z) & -zqd\\ 0 & zq(q+d-1) & z(q-dq-z)\end{pmatrix}.$$

Analogously we use the matrix $\mathcal{B}=(I-B)^{-1}-I$, describing nonempty paths from i to j, using only dotted edges. We can decompose each path p in the whole automaton in a unique manner as $\dots p^{\mathrm{B}}p^{\mathrm{R}}p^{\mathrm{B}}\dots$, with nonempty subpaths of either type B or R. The reason to do this is that we want to superimpose a condition on the paths using only solid edges. We only want to allow such (nonempty) paths (of type R, say), of length $\le k$. For that purpose we must compute the matrix $\mathcal{R}^{\le k}$ of such paths of restricted lengths. We explain the procedure for one component, say

$$\frac{zq(q+d-1)}{(q-z)(q^2-z)};$$

the other ones are similar. Write

$$\frac{zq(q+d-1)}{(q-z)(q^2-z)}=\frac{q+d-1}{q-1}\left[\frac{1}{1-z/q}-\frac{1}{1-z/q^2}\right],$$

then it is plain to see that the restricted version is given by

$$\frac{q+d-1}{q-1}\left[\frac{1-(z/q)^{k+1}}{1-z/q}-\frac{1-(z/q^2)^{k+1}}{1-z/q^2}\right].$$

In this way we get the matrix $\mathcal{R}^{\le k}$.

Now we duplicate the states $1,2,3$ to $1B,2B,3B,1R,2R,3R$ and go from state iB to state jR using the entry $\mathcal{B}_{ij}$ and from state iR to state jB using the entry $\mathcal{R}^{\le k}_{ij}$; all other entries are zero. This results in the matrix

$$M:=\begin{pmatrix} 0 & 0 & 0 & \mathcal{B}_{11} & \mathcal{B}_{12} & \mathcal{B}_{13}\\ 0 & 0 & 0 & \mathcal{B}_{21} & \mathcal{B}_{22} & \mathcal{B}_{23}\\ 0 & 0 & 0 & \mathcal{B}_{31} & \mathcal{B}_{32} & \mathcal{B}_{33}\\ \mathcal{R}^{\le k}_{11} & \mathcal{R}^{\le k}_{12} & \mathcal{R}^{\le k}_{13} & 0 & 0 & 0\\ \mathcal{R}^{\le k}_{21} & \mathcal{R}^{\le k}_{22} & \mathcal{R}^{\le k}_{23} & 0 & 0 & 0\\ \mathcal{R}^{\le k}_{31} & \mathcal{R}^{\le k}_{32} & \mathcal{R}^{\le k}_{33} & 0 & 0 & 0 \end{pmatrix}.$$

We can start in the states $1B$ and $1R$ and end anywhere. The empty word will be accepted twice, so that we get eventually for the generating function of all paths where we only use up to k consecutive solid edges,

$$\begin{aligned} G^{\le k}(z)=\sum_{n\ge 0}p_{nk}z^n &= (1,0,0,1,0,0)(I-M)^{-1}(1,1,1,1,1,1)^t-1\\ &= \frac{s_0(z)+(z/q)^k r_1(z)+(z/q^2)^k r_2(z)+(z^2/q^3)^k r_3(z)}{(1-z)s_0(z)+(z/q)^k s_1(z)+(z/q^2)^k s_2(z)+(z^2/q^3)^k s_3(z)}, \end{aligned}$$

where $s_0(z)=-2q^4(q-1)(q^2-z(1-d))(q^2-z(q+d))$. The terms $r_1(z)$, $r_2(z)$, $r_3(z)$, $s_1(z)$, $s_2(z)$, $s_3(z)$ are polynomials in z, q, d which are independent of k. For later use, we record that $s_1(1)=-q^2(q+1)(q-1)^2(q^3+(2d-2)q^2+(2d-1)(d-1)q-d(d-1))$.

2.3. **Asymptotic Analysis.** We have to calculate

$$\begin{aligned} t_n &= \sum_{k\ge 0}k\mathbb{P}_n(t(\mathbf{X},\mathbf{Y})=k)=\sum_{k\ge 0}\mathbb{P}_n(t(\mathbf{X},\mathbf{Y})>k)\\ &= \sum_{k=0}^{1}\mathbb{P}_n(t(\mathbf{X},\mathbf{Y})>k)+\sum_{k\ge 0}(1-p_{nk}). \end{aligned} \tag{12}$$

To evaluate this sum, we can proceed as Knuth [5]. Since we will need the same techniques (bootstrapping) in the next sections also, we collect the relevant results in the following lemma.

Lemma 2.5. *Let p_{nk}, $n,k\ge 0$, be numbers such that*

$$0\le p_{n0}\le\cdots\le p_{nn}$$

with generating function

$$\frac{R_k(z)}{S_k(z)}=\sum_{n\ge 0}p_{nk}z^n.$$

Assume that

$$R_k(z) = r_0(z) + (z/a_1)^k r_{1k}(z), \qquad S_k(z) = (1-z)s_0(z) + (z/a_1)^k s_1(z) + (z/a_2)^k s_{2k}(z),$$

where $r_0(z)$, $s_0(z)$, *and* $s_1(z)$ *are real polynomials in* z *(not depending on* k*),* $s_0(1) \neq 0$, *and* $r_{1k}(z)$ *and* $s_{2k}(z)$ *are real polynomials in* z, $(z/a_1)^k$, $\dots$, $(z/a_l)^k$ *for some* $l \geq 2$ *and some real numbers* $1 < a := a_1 < |a_2| \leq |a_3| \leq \cdots \leq |a_l|$.

Define

$$\delta := s_1(1)/s_0(1), \qquad \rho := \min\left(\log|a_2| / \log a_1, 2\right) - 1.$$

If s_0 *does not have any zero in* $|z| \leq 1$, $r_0(1)/s_0(1) = 1$ *and if* $\delta > 0$, *then*

$$\sum_{k=0}^{n}(1-p_{nk}) = \log_a n + \log_a \delta + \frac{\gamma}{\log a} + \frac{1}{2} + \psi(\log_a n + \log_a \delta) + O\left(\frac{\log^{\rho+3} n}{n^\rho}\right), \tag{13}$$

where $\psi(x)$ *is a periodic function (with period* 1 *and mean value* 0*), given by its Fourier expansion*

$$\psi(x) = -\frac{1}{\log a}\sum_{k\neq 0}\Gamma\Big(-\frac{2k\pi i}{\log a}\Big)e^{2k\pi i x}. \tag{14}$$

Proof. $0 \leq k_1 \leq k_2 \leq k_3$ will denote suitable constants.

For some $C > 0$ such that there is no root of s_0 inside $\{z : |z| \leq 1 + 2C\}$ and such that $(1+C)/a < 1$, we have

$$|S_k(z) - (1-z)s_0(z)| = O\Big(\big((1+C)/a\big)^k\Big) < |(1-z)s_0(z)|$$

for $|z| = 1 + C$ and $k \geq k_1$. By Rouché's Theorem, we conclude that for $k \geq k_1$, $S_k(z)$ has exactly one simple root in the disk $\{z : |z| \leq 1 + C\}$.

Since $\operatorname{sign}(S_k(1)) = \operatorname{sign}(s_1(1))$ and $\operatorname{sign}(S_k(1+1/k)) = -\operatorname{sign}(s_0(1))$ for $k \geq k_2$, the assumption $\delta > 0$ implies that $S_k(z)$ has a real root $z_k = 1 + \varepsilon_k$ with $0 < \varepsilon_k < 1/k$ for $k \geq k_2$. Inserting this in $S_k(1+\varepsilon_k) = 0$ yields $\varepsilon_k = O(1/a^k)$. Using $S_k(1+\varepsilon_k) = 0$ again shows that

$$\varepsilon_k = \frac{\delta}{a^k}\big(1 + O(k/c^k)\big),$$

where $\min\{a, |a_2|/a\} = c := a^\rho > 1$.

Using the residue theorem and the assumption $r_0(1) = s_0(1)$, we get

$$\begin{aligned}
p_{nk} &= \operatorname{Res}\left(\frac{R_k(z)}{z^{n+1}S_k(z)}, z = 0\right) \\
&= \frac{1}{2\pi i}\oint_{|z|=1+C/2}\frac{R_k(z)}{z^{n+1}S_k(z)} - \operatorname{Res}\left(\frac{R_k(z)}{z^{n+1}S_k(z)}, z = 1+\varepsilon_k\right) \\
&= -\frac{R_k(1+\varepsilon_k)}{S_k'(1+\varepsilon_k)}(1+\varepsilon_k)^{-(n+1)} + O((1+C/2)^{-n}) \\
&= \exp(-n\delta/a^k)\big(1 + O(k/a^k) + O(nk/(a^k c^k))\big) + O((1+C/2)^{-n})
\end{aligned}$$

for $k_3 \leq k \leq n$.

Let $t_{nk} = \exp(-n\delta/a^k)$. In the intervals $k_3 \le k \le \log_a(\delta n/4\log n)$, $\log_a(\delta n/4\log n) < k \le 5\log_a n$, and $5\log_a n \le k \le n$, we get $|p_{nk} - t_{nk}| = O(1/n^2)$, $O(\log_a^{\rho+2} n/n^\rho)$, and $O(1/n^3)$, respectively. For $k \le k_3$, we have $|p_{nk} - t_{nk}| \le p_{nk} + |t_{nk}| \le p_{nk_3} + |t_{nk}| = O(1/n^2)$. Noting that $(1 - t_{nk})$ is exponentially small for $k > n$ and adding up the errors, we obtain

$$\sum_{k=0}^{n}(1 - p_{nk}) = \sum_{k=0}^{\infty}\bigl(1 - \exp(-n\delta/a^k)\bigr) + O\left(\frac{\log^{\rho+3} n}{n^\rho}\right).$$

We note that $p_{n0} = O(n^{-2})$.

It is well known (see e. g. [2]), that

$$\sum_{k\ge 0}\left(1 - e^{-x/a^k}\right) = \log_a x + \frac{\gamma}{\log a} + \frac{1}{2} + \psi(\log_a x) + O\left(\frac{1}{x}\right)$$

with the periodic function $\psi(x)$ given in (14). Setting $x = n\delta$, we get (13). □

To apply this lemma, we note that $s_0(1) = -2q^4(q-1)(q^2+d-1)(q^2-q-d) < 0$, $s_1(1) < 0$, $\rho = 1$, and that the roots of s_0 are $q^2/(1-d) > q$ and $q^2/(q+d) > q$. From the combinatorial definition of the p_{nk}, it is clear that $0 \le p_{n0} \le \cdots \le p_{nn} = 1$ holds. From Theorem 2.4, we get $p_{nk} = 0$ for $k > n$. Furthermore, we note that $1 \ge \mathbb{P}_n(t(\mathbf{X}, \mathbf{Y}) > k) \ge (1 - p_{n0}) = 1 + O(1/n^2)$ for $k = 0, 1$. Therefore, we have to add 2 to (13), which amounts to a multiplication of δ by q^2. This leads to the following result.

Theorem 2.6. *The expected number t_n of carry propagations is*

$$t_n = \log_q n + \log_q \delta + \frac{\gamma}{\log q} + \frac{1}{2} + \psi(\log_q n + \log_q \delta) + O\left(\frac{\log^4 n}{n}\right),$$

where

$$\delta = \frac{(q^3 + (2d-2)q^2 + (2d-1)(d-1)q - (d-1)d)(q-1)(q+1)}{2(q^2-q-d)(q^2+d-1)}$$

and $\psi(x)$ is the periodic function given in (14).

We remark that δ is symmetric in $d + (q-1)/2$ and that for $d = 0$ (which we excluded), we get $\delta = (q-1)/2$, which was exactly Knuth's result [5].

3. Symmetric Signed Digit Expansion

Let $q \ge 2$ be even. We call a sequence $\mathbf{x}$ admissible, if

$$x_j \in \{-q/2, \ldots, q/2\}, \qquad j \ge 0, \tag{15a}$$

$$|x_j| = q/2 \Longrightarrow 0 \le \operatorname{sign}(x_j)x_{j+1} \le q/2 - 1, \qquad j \ge 0, \tag{15b}$$

$$x_j \ne 0 \text{ for finitely many } j. \tag{15c}$$

In [4], we proved that all integers x have a unique expansion

$$x = \sum_{j\ge 0} x_j q^j, \qquad \mathbf{x} \text{ admissible.}$$

We will call this expansion the "symmetric signed digit expansion."

Let x and y be two integers with symmetric signed digit expansions $\mathbf{x}$ and $\mathbf{y}$, respectively. We define the partial addition $(\mathbf{z},\mathbf{c}) := \operatorname{add}(\mathbf{x},\mathbf{y})$ in such a way that if admissibility is violated, a carry is triggered:

$$c_0 := 0, \tag{16}$$

$$c_{j+1} := \begin{cases} \operatorname{sign}(x_j+y_j) & \text{if } |x_j+y_j| > q/2, \\ \operatorname{sign}(x_j+y_j) & \text{if } |x_j+y_j| = q/2 \text{ and} \\ & \qquad \big(\operatorname{sign}(x_j+y_j)(x_{j+1}+y_{j+1})\big) \bmod q \geq q/2, \\ 0 & \text{otherwise,} \end{cases} \tag{17}$$

$$z_{j+1} := x_j + y_j - c_{j+1}q. \tag{18}$$

It is clear that $|z_j| \leq q/2$ and $c_j \in \{0,\pm 1\}$ for $j \geq 0$. The relation (3) holds in this case, too. However in general, $\mathbf{z}$ and $\mathbf{c}$ are not admissible. Since we want to iterate the process, we extend the definition of the partial addition to the case where $\mathbf{x}$ and $\mathbf{y}$ are sequences with $|x_j|$, $|y_j| \leq q/2$ for $j \geq 0$ and only finitely many nonzero digits.

It can easily be checked that if $\mathbf{c} = \mathbf{0}$, the sequence $\mathbf{z}$ is the symmetric signed digit expansion of $x+y$.

We define the iterative procedure and the number of carries $t(\mathbf{x},\mathbf{y})$ as in (4) and (5).

3.1. Syntactical Properties.

For $q \geq 4$, the syntactical description of the sequences $\mathbf{x}$, $\mathbf{y}$ with $t(\mathbf{x},\mathbf{y}) = k$ will only depend on (15a) and (15c), but not on (15b).

Therefore, we assume throughout the section that $q \geq 2$ is an even integer, $\mathbf{x}$, $\mathbf{y}$ are sequences of digits of absolute value at most $q/2$ with finitely many nonzero digits, and that $\mathbf{x}$ and $\mathbf{y}$ are admissible if $q=2$. The sequences $(\mathbf{z}^{(k)})_{k\geq 0}$ and $(\mathbf{c}^{(k)})_{k\geq 0}$ are defined by (4).

The conclusions of Lemma 2.1 are still valid, however, the proof has to be modified to deal with the case $|z_j^{(k)} + c_j^{(k)}| = q/2$. Therefore, we restate the Lemma and append two further statements.

Lemma 3.1. *Let $j \geq 0$ and $k \geq 1$.*

1. *If $c_{j+1}^{(k+1)} \neq 0$, then $c_{j+1}^{(k+1)} = c_j^{(k)}$.*
2. *If $c_j^{(k)} = 0$, then $z_j^{(k+1)} = z_j^{(k)}$.*
3. *$c_j^{(j+k)} = 0$.*
4. *Let $c_j^{(k)} \neq 0$ and $l \geq 1$ minimal such that $c_j^{(k+l)} \neq 0$. Then $c_j^{(k+l)} = -c_j^{(k)}$.*
5. *If $c_{j+1}^{(k+1)} \neq c_j^{(k)}$, then $c_{j+1}^{(k+m)} = 0$ for all $m \geq 1$.*
6. *If $|z_j^{(k)}| = q/2$, then $\big(\operatorname{sign}(z_j^{(k)}) z_{j+1}^{(k+1)}\big) \bmod q < q/2$.*
7. *If $|z_j^{(k)}| = q/2$, then $|z_{j+1}^{(k+1)}| < q/2$.*

Proof. Let $t \in \{\pm 1\}$, q be even and l be an integer. Then it is easily checked that

$$tl \bmod q \geq q/2 \iff \big(-t(l+t)\big) \bmod q < q/2. \tag{19}$$

(1) By (17), $c_{j+1}^{(k+1)} \neq 0$ implies $c_{j+1}^{(k+1)}(c_j^{(k)} + z_j^{(k)}) > q/2$ or $(c_{j+1}^{(k+1)}(c_j^{(k)} + z_j^{(k)}) = q/2$ and $\bigl(c_{j+1}^{(k+1)}(c_{j+1}^{(k)} + z_{j+1}^{(k)})\bigr) \bmod q \geq q/2)$. The first case leads to $z_j^{(k)} = c_{j+1}^{(k+1)} q/2$ and $c_j^{(k)} = c_{j+1}^{(k+1)}$ as in Lemma 2.1. We consider the second case. The relation $c_{j+1}^{(k+1)}(c_j^{(k)} + z_j^{(k)}) = q/2$ implies that either $c_{j+1}^{(k+1)} c_j^{(k)} = 1$, which is the required result, or $c_j^{(k)} = 0$ and $z_j^{(k)} = c_{j+1}^{(k+1)} q/2$. We assume the latter. From $z_j^{(k)} = z_j^{(k-1)} + c_j^{(k-1)} - c_{j+1}^{(k)} q$ we conclude that $c_{j+1}^{(k)} \in \{0, -c_{j+1}^{(k+1)}\}$.

Consider first the case $c_{j+1}^{(k)} = 0$. This implies $z_j^{(k)} = z_j^{(k-1)} + c_j^{(k-1)} = c_{j+1}^{(k+1)} q/2$. Therefore, equation (17) yields

$$\bigl(c_{j+1}^{(k+1)}(c_{j+1}^{(k)} + z_{j+1}^{(k)})\bigr) \bmod q = \bigl(c_{j+1}^{(k+1)}(c_{j+1}^{(k-1)} + z_{j+1}^{(k-1)})\bigr) \bmod q < q/2.$$

This is a contradiction to $c_{j+1}^{(k+1)} \neq 0$.

We are left with the case $c_{j+1}^{(k)} = -c_{j+1}^{(k+1)}$. We get $z_j^{(k-1)} + c_j^{(k-1)} = c_{j+1}^{(k)} q/2$, and therefore $\bigl(c_{j+1}^{(k)}(c_{j+1}^{(k-1)} + z_{j+1}^{(k-1)})\bigr) \bmod q \geq q/2$. Then (19) yields a contradiction.

(2) Follows as in Lemma 2.1.

(3) Follows as in Lemma 2.1.

(4) We have $c_j^{(k)} z_{j-1}^{(k)} = c_j^{(k)}(z_{j-1}^{(k-1)} + c_{j-1}^{(k-1)}) - q \leq 0$. Using induction on j as in the proof of Lemma 2.1, we get

$$c_j^{(k)}(z_{j-1}^{(k+l-1)} + c_{j-1}^{(k+l-1)}) = c_j^{(k)} z_{j-1}^{(k)} + \sum_{m=0}^{l-1} c_j^{(k)} c_{j-1}^{(k+m)} \leq 1. \tag{20}$$

If $q \geq 4$, we conclude that $c_j^{(k)}(z_{j-1}^{(k+l-1)} + c_{j-1}^{(k+l-1)}) < q/2$, which implies $c_j^{(k+l)} \neq c_j^{(k)}$, which immediately yields the required relation $c_j^{(k+l)} = -c_j^{(k)}$.

If $q = 2$ and $k \geq 2$, we have $c_j^{(k)} = c_{j-1}^{(k-1)}$ by part 1. This implies that the first nonzero summand $c_j^{(k)} c_{j-1}^{(k+m)}$ in (20) is negative by induction hypothesis. This implies that the sum in (20) is nonpositive which again yields $c_j^{(k+l)} = -c_j^{(k)}$.

Therefore, the only remaining case is $q = 2$, $k = 1$, and $x_{j-1} + y_{j-1} = 2c_j^{(1)}$. From part 3 we conclude $2 \leq 1 + l \leq j$. Since $\mathbf{x}$ and $\mathbf{y}$ are admissible, we have $x_{j-1} = y_{j-1} = c_j^{(1)}$ and $x_{j-2} = y_{j-2} = x_j = y_j = 0$. By definition, we get $c_{j-1}^{(1)} = z_{j-1}^{(1)} = z_{j-2}^{(1)} = 0$. We claim that $z_{j-1}^{(m)} = c_{j-1}^{(m)} = 0$ for $m \geq 1$ and that $z_{j-2}^{(m)} c_{j-2}^{(m)} \in \{0, -1\}$ for $m \geq 0$. For $m \leq 1$, the claim has already been proved.

Assume that the claim has been proved for all $m \leq n-1$ for some $n \geq 2$. Since $|z_{j-2}^{(n-1)} + c_{j-2}^{(n-1)}| \leq 1$ and $c_{j-1}^{(n-1)} + z_{j-1}^{(n-1)} = 0$, we immediately get $c_{j-1}^{(n)} = 0$ and $z_{j-1}^{(n)} = 0$.

If $c_{j-2}^{(m)} = 0$ for $0 \leq m < n$, then we conclude from part 2 that $z_{j-2}^{(m)} = z_{j-2}^{(1)} = 0$ for $0 \leq m \leq n$, and $z_{j-2}^{(n)} c_{j-2}^{(n)} = 0$. Otherwise, there is a maximal $1 \leq n' < n$

such that $c_{j-2}^{(n')} \neq 0$. By induction hypothesis, we have $c_{j-2}^{(n)} = -c_{j-2}^{(n')}$. We obtain $c_{j-2}^{(n)} z_{j-2}^{(n)} = c_{j-2}^{(n)} \big(z_{j-2}^{(n')} + c_{j-2}^{(n')}\big) \leq 0$, which proves the claim.

Since $c_{j-1}^{(m)} = 0$ for $m \geq 1$, we get $c_j^{(m)} = 0$ for $m \geq 2$. This concludes the proof.

(5) As in Lemma 2.1, we only have to consider the case $c_j^{(k+l)} \neq 0$ for some $l \geq 1$. We choose l minimal with this property and have to prove $c_{j+1}^{(k+l+1)} = 0$. As in Lemma 2.1, we get $c_{j+1}^{(k+1)} = \cdots = c_{j+1}^{(k+l)} = 0$ and $z_{j+1}^{(k+1)} = \cdots = z_{j+1}^{(k+l)} = z_{j+1}^{(k+l+1)}$. In particular, we obtain

$$z_{j+1}^{(k+l)} + c_{j+1}^{(k+l)} = z_{j+1}^{(k+1)} \equiv z_{j+1}^{(k)} + c_{j+1}^{(k)} \equiv z_{j+1}^{(k-1)} + c_{j+1}^{(k-1)} + c_{j+1}^{(k)} \pmod q. \tag{21}$$

By part 2, we have $z_j^{(k+1)} = \cdots = z_j^{(k+l)}$, which implies (using part 4)

$$\begin{aligned} z_j^{(k+l)} + c_j^{(k+l)} &= z_j^{(k+1)} - c_j^{(k)} = z_j^{(k)} + c_j^{(k)} - qc_{j+1}^{(k+1)} - c_j^{(k)} \\ &= z_j^{(k)} = z_j^{(k-1)} + c_j^{(k-1)} - c_{j+1}^{(k)} q. \end{aligned}$$

This yields $|z_j^{(k+l)} + c_j^{(k+l)}| = |z_j^{(k)}| \leq q/2$, the only interesting case is therefore $|z_j^{(k+l)} + c_j^{(k+l)}| = q/2$. If $c_{j+1}^{(k)} = 0$, we have $z_j^{(k+l)} + c_j^{(k+l)} = z_j^{(k-1)} + c_j^{(k-1)}$ and $z_{j+1}^{(k+l)} + c_{j+1}^{(k+l)} \equiv z_{j+1}^{(k-1)} + c_{j+1}^{(k-1)} \pmod q$. Therefore, we get $c_{j+1}^{(k+l+1)} = c_{j+1}^{(k)} = 0$. Otherwise, we have $c_{j+1}^{(k)} = t \in \{\pm 1\}$. This implies $z_j^{(k+l)} + c_j^{(k+l)} = -tq/2$ and $z_j^{(k-1)} + c_j^{(k-1)} = tq/2$. By (17), this yields $\big(t(z_{j+1}^{(k-1)} + c_{j+1}^{(k-1)})\big) \bmod q \geq q/2$. By (19), this and (21) result in $\big(-t(z_{j+1}^{(k+l)} + c_{j+1}^{(k+l)})\big) \bmod q < q/2$. Hence $c_{j+1}^{(k+l+1)} = 0$, as requested.

(6) Let $s := \operatorname{sign}(z_j^{(k)})$. Then $sq/2 = z_j^{(k)} = z_j^{(k-1)} + c_j^{(k-1)} - c_{j+1}^{(k)} q$, which implies $c_{j+1}^{(k)} \in \{0, -s\}$. If $c_{j+1}^{(k)} = 0$, we get $z_j^{(k-1)} + c_j^{(k-1)} = sq/2$ and $\big(s(z_{j+1}^{(k-1)} + c_{j+1}^{(k-1)})\big) \bmod q < q/2$. Since $z_{j+1}^{(k+1)} \equiv z_{j+1}^{(k-1)} + c_{j+1}^{(k-1)} + c_{j+1}^{(k)} \pmod q$, the assertion follows. Otherwise, if $c_{j+1}^{(k)} = -s$, we have $z_j^{(k-1)} + c_j^{(k-1)} = -sq/2$ and $\big(-s(z_{j+1}^{(k-1)} + c_{j+1}^{(k-1)})\big) \bmod q \geq q/2$, and the assertion follows from (19).

(7) This is an easy consequence of part 6.

□

The result on finiteness (and its proof) can be transferred literally.

Lemma 3.2. *Let* $J := \max\{j : x_j + y_j \neq 0\}$. *Then* $t(\mathbf{x}, \mathbf{y}) \leq J + 2$.

Proof. The proof of Lemma 2.2 does apply. □

Proposition 3.3. *Let* $k \geq 1$. *Then the following properties are equivalent:*

(1) $t(\mathbf{x}, \mathbf{y}) \geq k + 1$.

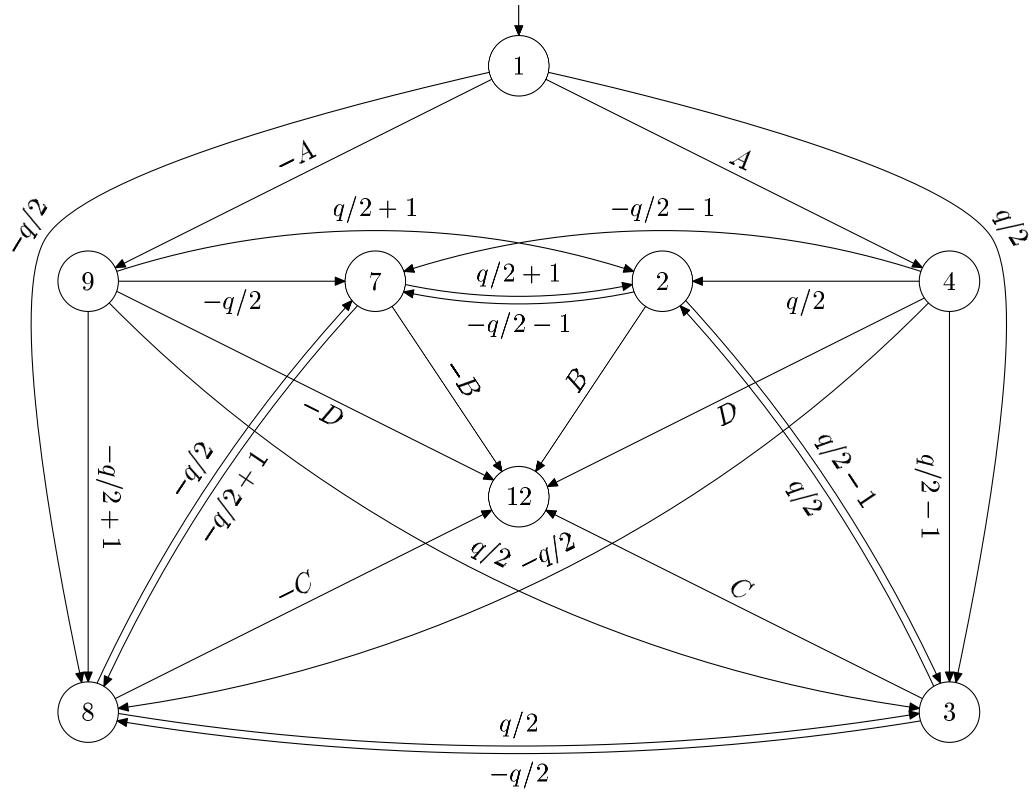
(2) *There is a* $j \geq 0$, *a* $v \in \{\pm 1\}$, *and a sequence* $(s_l)_{1 \leq l \leq k} \in \{\pm 1\}^k$ *such that the following properties hold.*

  (a) $s_1(x_j + y_j) \geq q/2$.

  (b) *If* $s_1(x_j + y_j) = q/2$, *then* $v = s_1$.

(c) $x_{j+l} + y_{j+l} = s_{l+1}q/2 - s_l\,[s_l = (-1)^l v]$ *for* $1 \le l \le k-1$.
(d) $\big((-1)^k v(x_{j+k} + y_{j+k}) - [s_k = -(-1)^k v]\big) \bmod q \le q/2 - 1$.

(3) *There is a* $j \ge 0$ *such that the subsequence* $(x_{j+l} + y_{j+l})_{0 \le l \le k}$ *of length* $k+1$ *is accepted by the finite automaton given in Figure 4.*



$$A = \{q/2+1, \dots, q\}$$
$$B = \{-q, \dots, -q/2-2\} \cup \{0, \dots, q/2-2\} \cup (\{q\} \setminus \{2\})$$
$$C = \{-q/2+1, \dots, -1\} \cup \{q/2+1, \dots, q-1\}$$
$$D = \{-q, \dots, -q/2-2\} \cup \{-q/2+1, \dots, q/2-2\} \cup \{q/2+1, \dots, q\}$$

FIGURE 4. Automaton recognizing subsequences which require $k+1$ carries in the symmetric signed digit expansion.

Proof. We first prove that 1 implies 2. The proof of Proposition 2.3 can be copied literally until equation (8). Similarly, we get

$$z_{j+k}^{(k)} \equiv x_{j+k} + y_{j+k} + \sum_{m=1}^{k-1} c_{j+k}^{(m)} \equiv x_{j+k} + y_{j+k} - \sigma\,[s_k = -\sigma] \pmod{q}. \tag{22}$$

The equation $c_{j+l+1}^{(l+1)} = \sigma$ implies

$$\sigma(z_{j+l}^{(l)} + c_{j+l}^{(l)}) > q/2 \text{ or } \Big(z_{j+l}^{(l)} + c_{j+l}^{(l)} = \sigma q/2 \text{ and } \big(\sigma(z_{j+l+1}^{(l)} + c_{j+l+1}^{(l)})\big) \bmod q \geq q/2\Big) \quad (23)$$

for $0 \leq l \leq k-1$. Noting that $s_1 = \sigma$ and letting $l = 0$, we get relation 2a. Let now $1 \leq l \leq k-1$. Since $q/2 \leq \sigma(z_{j+l}^{(l)} + c_{j+l}^{(l)}) \leq q/2 + 1$ and $c_{j+l}^{(l)} = \sigma$, we obtain $z_{j+l}^{(l)} = \sigma q/2$ or $(z_{j+l}^{(l)} = \sigma(q/2-1)$ and $(\sigma z_{j+l+1}^{(l+1)}) \bmod q \geq q/2)$. From Lemma 3.2, part 7 we conclude that the two alternatives occur alternately. We define $u \in \{0,1\}$ such that $z_{j+1}^{(1)} = \sigma(q/2 - u)$. Then we have $z_{j+l}^{(l)} = \sigma\big(q/2 - ((l-1+u) \bmod 2)\big)$ for $1 \leq l \leq k-1$. Setting $v := (-1)^u s_1$ and combining this with (8), elementary calculations yield relation 2c. Relation 2b follows from (23) for $l = 0$. Finally, relation 2d follows from (22), combined with (23) or Lemma 3.1, part 6, depending on the parity of $k+u$.

We will now prove the other direction. Relations 2a, 2b, and 2c clearly imply $c_{j+1}^{(1)} = s_1$. It can easily be checked that relation 2c implies $c_{j+l+1}^{(1)} = s_{l+1}\,[s_l \neq s_{l+1}]$ and $z_{j+l}^{(1)} = s_l q/2 - s_l\,\big[s_l = (-1)^l v\big]$. Defining m_l as previously, we claim that (10) and (11) are still valid. We proceed by induction on l. As in the case of Proposition 2.3, (10) follows from (11) for $l-1$. To prove (11), we assume that $c_{j+l}^{(m)} \neq 0$ and get analogously to the case of Proposition 2.3

$$z_{j+l}^{(m)} + c_{j+l}^{(m)} = c_{j+l}^{(m)}\left(\frac{q}{2} + \Big[c_{j+l}^{(m)} = (-1)^{l+1}v\Big]\right).$$

If $c_{j+l}^{(m)} = (-1)^{l+1}v$, there is a carry $c_{j+l+1}^{(m+1)} = c_{j+l}^{(m)}$, as requested. Otherwise, we have to check that $\big(c_{j+l}^{(m)}(z_{j+l+1}^{(m)} + c_{j+l+1}^{(m)})\big) \bmod q \geq q/2$. Consider first the case $l < k-1$. Then

$$\begin{aligned}
c_{j+l+1}^{(m)} + z_{j+l+1}^{(m)} &\equiv z_{j+l+1}^{(1)} + \sum_{t=1}^{m} c_{j+l+1}^{(t)} \\
&\equiv \frac{q}{2} - s_{l+1}\,\big[s_{l+1} = (-1)^{l+1}v\big] + c_{j+l+1}^{(1)} + \sum_{t=2}^{m} c_{j+l}^{(t-1)} \\
&= \frac{q}{2} - s_{l+1}\,\big[s_{l+1} = (-1)^{l+1}v\big] + s_{l+1}\,[s_{l+1} \neq s_l] - c_{j+l}^{(m)}\Big[s_l = -c_{j+l}^{(m)}\Big] \\
&= q/2 \pmod{q}.
\end{aligned}$$

If $l = k-1$, we similarly obtain

$$c_{j+k}^{(m)} + z_{j+k}^{(m)} \equiv x_{j+k} + y_{j+k} - c_{j+l}^{(m)}\Big[s_k = -c_{j+l}^{(m)}\Big] \pmod{q}.$$

Relation 2d and (19) yield the required result.

It is clear that (11) implies $t(\mathbf{x}, \mathbf{y}) \geq k+1$.

The equivalence of 2 and 3 follows from the associations given in Table 2. □

As in the case of the (q,d) expansion, we transform the automaton in Figure 4 to an automaton which reads the whole sequence $(x_n + y_n)_{n \geq 0}$ in one run. However, in this case, maximal accepted subsequences may overlap: Assume that we read a digit $a_j = x_j + y_j$ while accepting a subsequence. If $|a_j| < q/2$, then it cannot start a new acceptable subsequence,

node	l	s_l	$(-1)^l v$
1	0		
2	≥ 2	1	1
3	≥ 1	1	-1
4	1	1	
7	≥ 2	-1	-1
8	≥ 1	-1	1
9	1	-1	
12	k		

TABLE 2. Associations between nodes and states for the Automaton in Figure 4.

therefore it may be appended to the current subsequence if possible. If $|a_j| > q/2+1$, then it may serve to reach node 12 in the current subsequence (which ends there) and to start a new acceptable subsequence. Therefore, the appropriate action is to add 1 to the length of the current subsequence (if applicable), reset the counter to 1, and go to nodes 4 or 9.

Assume $a_j = q/2+1$. If it leads us to node 12 in the current accepted subsequence, we proceed as above. Therefore, we assume that a_j leads us to node 2 in the current subsequence, whereas if a_j would start a new acceptable subsequence, we would be in node 4. If $a_{j+1} = q/2-1$, both possibilities lead us to node 3, and it is clear that starting a new acceptable subsequence with a_j would lead to a non-maximal accepted subsequence, which we do not want. However, if $a_{j+1} = q/2$, the old subsequence would stop after a_j and the new subsequence would reach node 2 with a counter of 2. Other values for a_{j+1} and the cases $a_j \in \{-q/2-1, -q/2, q/2\}$ have to be discussed analogously.

The construction of a new automaton is now done in the following way: We agree that we do not count the first 2 digits of an accepted subsequence. To this aim, all edges from 1, 4, 9 have to be dotted. Furthermore, new nodes 5 and 10 are introduced, which inherit all outgoing edges from 3 and 8, respectively, but as dotted edges. The edges $(1,3)$ and $(1,8)$ are replaced by edges $(1,5)$ and $(1,10)$. These changes assure that the first two edges of an acceptable subsequence are not counted. We introduce missing edges as in the (q,d) expansion. For instance, we introduce a solid edge from 3 to 4 for digits $\in \{q/2+1, \ldots, q-1\}$, because such a digit would lead an accepted subsequence to node 12, and it starts a new subsequence, therefore going to 4. The fact that all edges starting in 4 are dotted ensures that the two subsequences are indeed separated by a dotted edge. The situation $(a_j, a_{j+1}) = (q/2+1, q/2)$ sketched above leads to a dotted loop from 2 to 2. Doing all such modifications, we finally arrive at the automaton in Figure 5.

The syntactic properties of carry generating sequences are summed up in the following Theorem.

Theorem 3.4. (1) $t(\mathbf{x}, \mathbf{y}) = 0$ *if and only if* $\mathbf{y} = 0$. *This does not guarantee that* $\mathbf{x}$ *is admissible.*

(2) $t(\mathbf{x}, \mathbf{y}) \leq 1$ *if and only if* $(x_j + y_j)_{j\geq 0}$ *is admissible.*

(3) *Let $k \geq 0$. Then $t(\mathbf{x}, \mathbf{y}) \leq k+2$ if and only if the automaton in Figure 5 does not traverse more than k consecutive solid edges when reading the sequence $(x_j + y_j)_{j \geq 0}$.*

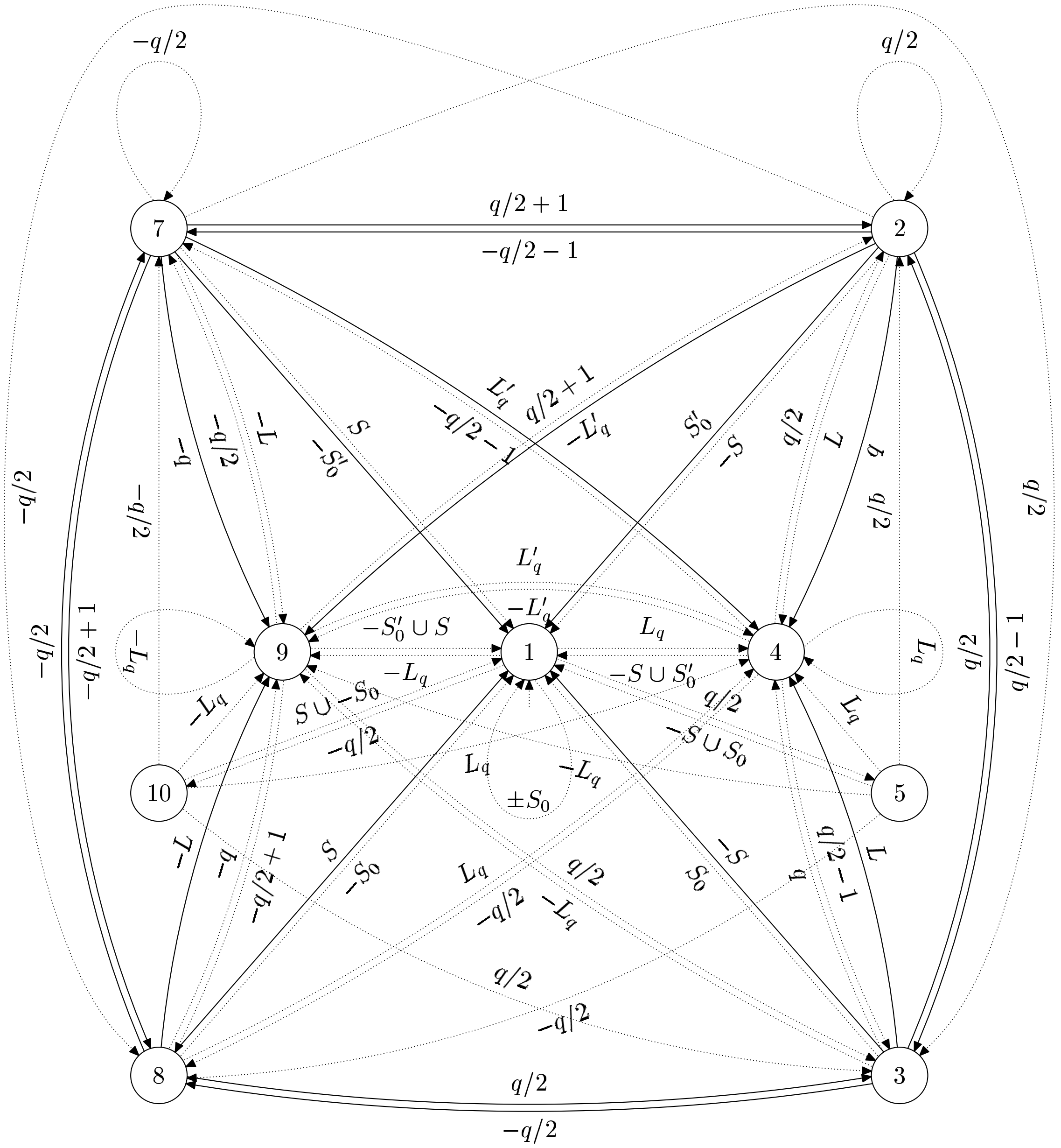
3.2. **Generating Function and Asymptotic Analysis for $q \geq 4$.** Since by definition digits in admissible sequences are not independent, the method in Section 2.2 cannot be applied directly. One possibility to circumvent this problem is to allow a larger class of input. Since for $q \geq 4$, Theorem 3.4 does not assume that $\mathbf{x}$ and $\mathbf{y}$ are admissible, we allow $\mathbf{x}$ and $\mathbf{y}$ to be strings of length n, built from digits $-q/2, \dots, q/2$. However, in order to make our probability model somehow realistic, we put weights onto the digits. It has been proved in [4] that the average frequency $\varpi(i)$ (amongst the numbers $0, \dots, N-1$, say) of respective digits is asymptotically given by

$$\varpi(i) = \begin{cases} \frac{1}{2(q+1)} & \text{for } |i| = \frac{q}{2}, \\ \frac{1}{q} & \text{for } 0 < |i| < \frac{q}{2}, \\ \frac{q+2}{q(q+1)} & \text{for } i = 0, \\ 0 & \text{otherwise.} \end{cases} \tag{24}$$

Now the sum of two digits can be in the range $-q, \dots, q$; the above frequencies translate into the following list of weights $w(i)$ that we are going to use in our automaton and associate generating functions:

$$w(i) = \begin{cases} \frac{1}{4(q+1)^2} & \text{for } |i| = q, \\ \frac{1}{q} - \frac{1}{q^2(q+1)} - \frac{i}{q^2} & \text{for } \frac{q}{2} < |i| < q, \\ \frac{\frac{q^3}{2} + q^2 + \frac{q}{2} - 1}{q^2(q+1)^2} & \text{for } |i| = \frac{q}{2}, \\ \frac{1}{q+1} - \frac{i-1}{q^2} & \text{for } 0 < |i| < \frac{q}{2}, \\ \frac{q^3 + \frac{3q^2}{2} + q + 2}{q^2(q+1)^2} & \text{for } i = 0, \\ 0 & \text{otherwise.} \end{cases}$$

In the automaton in Figure 5 there are symmetries, which lead to the following simplifications when it comes to generating functions. The principle is as follows: If we have states i and i' such that the generating functions of any type (using only bold resp. dotted edges) $f_{ij}(z)$ and $f_{i'j}(z)$ are always equal, then it is sufficient to work with one of them, and reduce the transition matrix by replacing the entries T_{ki} by $T_{ki} + T_{ki'}$. In our example, we have symmetries between states on the left and right. In this way we can write the following transition matrix:



$L := \{q/2+1, \ldots, q-1\}$ $\qquad$ $S := \{1, \ldots, q/2-1\}$

$L_q := L \cup \{q\} = \{q/2+1, \ldots, q\}$ $\qquad$ $S_0 := S \cup \{0\} = \{0, \ldots, q/2-1\}$

$L'_q := L_q \setminus \{q/2+1\} = \{q/2+2, \ldots, q\}$ $\qquad$ $S'_0 := S_0 \setminus \{q/2-1\} = \{0, \ldots, q/2-2\}$

FIGURE 5. $q \geq 2$ even: $t(\mathbf{x}, \mathbf{y}) \leq k+2$ if and only if the automaton traverses at most k consecutive solid edges when reading $(x_j + y_j)_{j \geq 0}$.

$$B = \frac{1}{8q^2(q+1)^2}\times$$
$$\begin{pmatrix} 2q(3q^3+4q^2+q-6) & 0 & 0 & 2(q+2)(q^3-2q^2-q+4) & 8(q^3+2q^2+q-2) \\ (q+1)(q-2)(3q^2+3q+4) & 4(q^3+2q^2+q-2) & 4(q^3+2q^2+q-2) & (q+1)(q-2)(q^2+q-4) & 0 \\ 3q^4+8q^3+7q^2-2q+8 & 0 & 0 & q^4-3q^2+2q+8 & 0 \\ 2(3q^4+2q^3-7q^2-20q-8) & 8(q^3+q^2-2q-3) & 8(q^3+3q^2+4q+1) & 2(q^4-2q^3-5q^2+12q+16) & 0 \\ 2(3q^3+4q^2+q-6)q & 4(q^3+2q^2+q-2) & 4(q^3+2q^2+q-2) & 2(q+2)(q^3-2q^2-q+4) & 0 \end{pmatrix},$$

$$R = \frac{1}{8q^2(q+1)^2}\times$$
$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 3q^4+4q^3-9q^2-30q-8 & 4(q^2-q-4)(q+1) & 4(q^2+3q+4)(q+1) & q^4-4q^3-3q^2+22q+24 & 0 \\ (q+1)(q-2)(3q^2+3q+4) & 4q^3+8q^2+4q-8 & 4q^3+8q^2+4q-8 & (q+1)(q-2)(q^2+q-4) & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The common denominator of the nonzero $\mathcal{R}_{ij}$'s is

$$8(q+1)(-(q+2)(q^3+2q^2+q-2)z^2 - q^2(q+1)(q^3+q^2-2q-3)z + q^4(q+1)^3).$$

The discriminant of this quadratic polynomial in z is

$$64(q^6+6q^5+17q^4+26q^3+18q^2-4q-7)(q+1)^4q^4,$$

which is not a square for any $q \geq 4$. Therefore, the denominators do not factor over the integers. Since the computation of the restrictions $\mathcal{R}_{\bar{i}\bar{j}}^{\leq k}$ involves calculating the partial fraction decomposition of $\mathcal{R}_{ij}$, these restrictions contain $\sqrt{q^6+6q^5+17q^4+26q^3+18q^2-4q-7}$.

In the automaton in Figure 5 we see that there is exactly one (except for symmetry) solid edge for digit 0, namely from 2 to 1. This means that if we are reading a sequence $(x_j+y_j)_{0\leq j\leq n-1}$ we must not end the path $\ldots p^B p^R p^B \ldots$ as described in Section 2.2 with an $\mathcal{R}_{\bar{i}\bar{2}}^{=k}$, because the automaton would then take the edge with digit 0. Therefore, a path not traversing more than $k \geq 1$ consecutive solid edges may end in some vertex iB for $i \neq 2$ or it may end in some vertex jB for some j or it may have the form $\ldots \mathcal{B}_{ij}\mathcal{R}_{\bar{j}\bar{2}}^{\leq k-1}$ for some i, j.

We apply the method described in Section 2.2 with the above transition matrix to obtain

$$G^{\leq k}(z) =$$
$$(1,0,0,0,0,1,0,0,0,0)(I-M)^{-1}(1,0,1,1,1,1+\mathcal{R}_{\bar{1}\bar{2}}^{\leq k-1},1+\mathcal{R}_{\bar{2}\bar{2}}^{\leq k-1},\ldots,1+\mathcal{R}_{\bar{5}\bar{2}}^{\leq k-1})^t - 1$$

for $k \geq 1$, where the "exit vector" has been chosen in accordance with the above discussion on the special role of the node 2.

Since we have to assume $k \geq 1$, we do not get information about p_{n0}. We rewrite (12) as

$$t_n = \sum_{l=0}^{2} \mathbb{P}_n(t(\mathbf{X},\mathbf{Y}) > l) + \sum_{k\geq 0}(1 - p_{n(k+1)}).$$

The calculation and simplification of the generating function took several hours using Maple. Finally we get

$$\begin{aligned} G^{\leq k+1}(z) &= \sum_{n\geq 0} p_{n(k+1)} z^n \\ &= \frac{s_0(z) + (z\alpha)^k r_1(z) + (z\beta)^k r_2(z) + (z^2\alpha\beta)^k r_3(z)}{(1-z)s_0(z) + (z\alpha)^k s_1(z) + (z\beta)^k s_2(z) + (z^2\alpha\beta)^k s_3(z)}, \end{aligned}$$

for $k \geq 0$, where

$$\begin{aligned} \alpha &= \frac{q^3+q^2-2q-3+\sqrt{D}}{2q^2(q+1)^2} = \frac{1}{q} - \frac{1}{q^4} + O\left(\frac{1}{q^5}\right), \\ \beta &= \frac{q^3+q^2-2q-3-\sqrt{D}}{2q^2(q+1)^2} = -\frac{1}{q^2} - \frac{1}{q^3} + \frac{1}{q^4} + O\left(\frac{1}{q^5}\right), \\ s_0(z) &= -4q^{12}(q^6+6q^5+17q^4+26q^3+18q^2-4q-7)(q+1)^9 \times \\ &\qquad \bigl((-q^5-5q^4-11q^3-9q^2+2q+8)z^2+4q^7+12q^6+12q^5+4q^4\bigr), \\ D &= q^6+6q^5+17q^4+26q^3+18q^2-4q-7, \end{aligned}$$

and $r_1(z)$, $r_2(z)$, $r_3(z)$, $s_1(z)$, $s_2(z)$, and $s_3(z)$ are polynomials in z with coefficients in $\mathbb{Z}[q,\sqrt{D}]$.

We note that $\log(-\beta)/\log(\alpha) > 1.85$. The generating function does not give information about $\mathbb{P}_n(t(\mathbf{X},\mathbf{Y}) \leq k)$ for $k \leq 2$, but these quantities can be estimated by $O(p_{n3}) = O(1/n^2)$. We apply Lemma 2.5 to obtain the following theorem.

Theorem 3.5. *The expected value t_n of carry propagations $t(\mathbf{X},\mathbf{Y})$, where $\mathbf{X}$ and $\mathbf{Y}$ are random strings of digits $-q/2,\dots,q/2$ of length n, where the digits are independent and have probabilities as given in* (24)*, is*

$$t_n = \log_{1/\alpha} n + \log_{1/\alpha}\delta + \frac{\gamma}{\log 1/\alpha} + \frac{1}{2} + \psi(\log_{1/\alpha} n + \log_{1/\alpha}\delta) + O\left(\frac{1}{n^{0.85}}\right),$$

where α and δ are given in Table 3 and $\psi(x)$ is the periodic function given in (14).

In theory, the methods presented in the next section for the case $q = 2$ could be used to obtain an exact model for the symmetric signed digit expansions. However, the number of nodes in the automaton would increase to about 13 (after removing symmetric nodes), which would probably make the symbolic computations infeasible.

3.3. **Generating Functions and Asymptotic Analysis for $q = 2$.** If $q = 2$, Theorem 3.4 is only valid for admissible sequences $\mathbf{x}$ and $\mathbf{y}$. Therefore, we have to use an equidistribution measure $\mathbb{P}_n$ on the set $\mathcal{A}_n$ of admissible sequences of length n. Whereas in the previous sections we could assume the digits to be independent, this is certainly not the case in this model, since $\mathbb{P}_n(X_{j+1} \neq 0 \mid X_j \neq 0) = 0$.

As a first step, we determine the number of admissible sequences $|\mathcal{A}_n|$. It is clear that the automaton in Figure 6 accepts a sequence if and only if it is admissible. Labeling edges

$$
\begin{aligned}
\alpha &= \frac{q^3+q^2-2q-3+\sqrt{D}}{2q^2(q+1)^2} = \frac{1}{q} - \frac{1}{q^4} + O\left(\frac{1}{q^5}\right),\\
D &= q^6+6q^5+17q^4+26q^3+18q^2-4q-7,\\
\delta &= \frac{\delta_1\sqrt{D} + (q^6+6q^5+17q^4+26q^3+18q^2-4q-7)\delta_2}{\delta_3}\\
&= \frac{1}{4}q - \frac{1}{8} - \frac{7}{16q} + \frac{75}{32q^2} - \frac{275}{64q^3} + \frac{663}{128}q^4 - \frac{991}{256q^5} + O\left(\frac{1}{q^6}\right),\\
\delta_1 &= 2q^{20}+25q^{19}+139q^{18}+456q^{17}+973q^{16}+1389q^{15}+1244q^{14}+423q^{13}-237q^{12}\\
&\quad+859q^{11}+3769q^{10}+5837q^9+5418q^8+3411q^7+48q^6-2880q^5-1876q^4+472q^3\\
&\quad-240q^2-1568q-768,\\
\delta_2 &= 2q^{17}+19q^{16}+74q^{15}+152q^{14}+190q^{13}+195q^{12}+261q^{11}+352q^{10}+240q^9-198q^8\\
&\quad-767q^7-1124q^6-768q^5+388q^4+968q^3+112q^2-608q-256,\\
\delta_3 &= 4q^2(q+2)(q^3+2q^2+q-2)(4q^7+12q^6+11q^5-q^4-11q^3-9q^2+2q+8)\\
&\quad\times(q^6+6q^5+17q^4+26q^3+18q^2-4q-7)(q+1)^3.
\end{aligned}
$$

TABLE 3. Constants for Theorem 3.5.

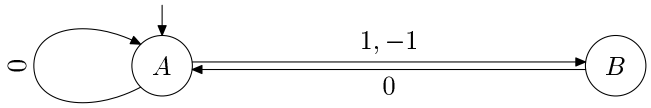


FIGURE 6. Admissible sequences for $q=2$.

in the automaton with the variable z, we get the generating function

$$A(z) := \sum_{n\geq 0} |\mathcal{A}_n|\, z^n = \frac{1+2z}{1-(z+2z^2)} = \frac{4}{3}\frac{1}{1-2z} - \frac{1}{3}\frac{1}{1+z}.$$

This yields

$$|\mathcal{A}_n| = \frac{4}{3}2^n - \frac{(-1)^n}{3}.$$

Furthermore, we calculate that for $1 \leq j \leq n-1$ we have

$$\mathbb{P}_n(X_j = 0 \mid X_{j-1} = 0) = \frac{|\mathcal{A}_{n-j-1}|}{|\mathcal{A}_{n-j}|} = \frac{1}{2} + \frac{3}{2}(-1)^{n-j}\frac{1}{2^{n-j+2}-(-1)^{n-j}}.$$

We cannot handle this by an automaton, since this expression depends on j. However, we can take the main term $1/2$ and estimate the error afterwards.

Therefore, we define another measure $\tilde{W}_n$ by Table 4. Then an admissible sequence $(x_0,\ldots,x_{n-2},0)$ with s nonzero entries gets weight $4^{-s}2^{-(n-2s)} = 2^{-n}$ and an admissible sequence $(x_0,\ldots,x_{n-1},x_n)$ with $x_n \in \{\pm 1\}$ with $s+1$ nonzero entries gets weight $4^{-s}2^{-(n-1-2s)}4^{-1} = 2^{-n-1}$. Defining "exit weights" $e(0) := 3/4$, $e(\pm 1) := 3/2$ and $W_n(\mathbf{X}) =$

x_{j-1}	$x_j=-1$	$x_j=0$	$x_j=1$
0	1/4	1/2	1/4
1 or -1	0	1	0

TABLE 4. $\tilde{W}_n(X_j = x_j \mid X_{j-1} = x_{j-1})$ depending on x_{j-1} and x_j.

$e(X_{n-1})\tilde{W}_n(\mathbf{X})$, we get a new measure on $\mathcal{A}_n$ which assigns the same weight $(3/4)2^{-n}$ to every admissible sequence. We get $W_n(\mathcal{A}_n) = (3/4)2^{-n}\,|\mathcal{A}_n| = 1-(-1)^n 2^{-(n+2)}$, which yields

$$W_n = W_n(\mathcal{A}_n)\mathbb{P}_n = \left(1-(-1)^n 2^{-(n+2)}\right)\mathbb{P}_n. \tag{25}$$

A pair $(\mathbf{x},\mathbf{y})$ of admissible sequences is recognized by the automaton in Figure 7. We

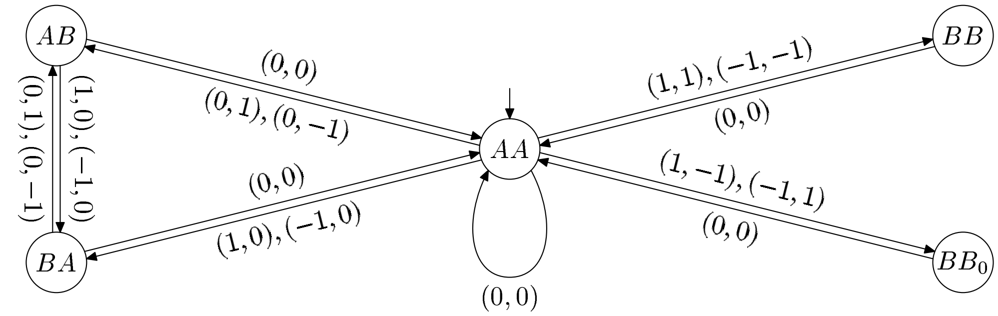


FIGURE 7. Pairs of admissible sequences for $q = 2$.

consider now a pair of (independent) random sequences $(\mathbf{X},\mathbf{Y})$.

The conditional weights $\tilde{W}_n((X_j,Y_j)\in M_j \mid (X_{j-1},Y_{j-1})\in M_{j-1})$ for various sets M_{j-1} and M_j are given in Table 5. Since the automaton in Figure 5 only needs to know (X_j+Y_j)

M_{j-1}	$M_j=$ $\{(0,0)\}$	$\{(1,-1),(-1,1)\}$	$\{(s,0),(0,s)\}$	$\{(s,s)\}$
$\{(0,0)\}$	1/4	1/8	1/4	1/16
$\{(1,-1),(-1,1)\}$	1	0	0	0
$\{(t,0),(0,t)\}$	1/2	0	1/4	0
$\{(t,t)\}$	1	0	0	0

TABLE 5. $\tilde{W}_n((X_j,Y_j)\in M_j \mid (X_{j-1},Y_{j-1})\in M_{j-1})$ depending on M_{j-1} and M_j, where $s,t\in\{\pm 1\}$.

and not the exact pairs, we only listed some sets M_{j-1} and M_j in Table 5. However, the case of $X_j+Y_j=0$ needs special care, as it is shown in the table. So we modify the automaton in Figure 5 for our counting purposes.

As a first step, we note that the sets L, L'_q, S, and S'_0 are empty, so the corresponding edges can be deleted.

Then we note that if node 4 (or 9) is reached, it has been reached with $x_j + y_j = 2$ (or $= -2$). Therefore, these nodes can only be left with $(0,0)$. This leads to deleting of several edges, for instance the edge $(9,2)$. But 2 can only be reached with $x_j + y_j \geq 1$, therefore, the edge $(2,7)$ (and analogously $(7,2)$) has to be deleted. This implies that node 2 (or 7) can be reached with $x_j + y_j = 1$ (or $= -1$) only. Similarly, nodes 5 and 10 are reached with $x_j + y_j = 1$ and $= -1$, respectively. Nodes 3 and 8 can be reached via $x_j + y_j \in \{0,1\}$ and $\in \{0,-1\}$. Since we have to know exactly what happened, we split node 3 into nodes 3 and 6, where 6 inherits the sum-zero inbound edges, and 3 the others. The outbound edges are copied, some of them have to be deleted due to the usual restrictions.

Finally, we have to deal with the input $(x_j, y_j) = (\pm 1, \mp 1)$. Such pairs can only be read if a sum-zero edge has been read. This can happen in nodes 1, 6, and 11 only. Such a pair would then lead to node 1. Therefore, we split node 1 into nodes 1 and 13, where 13 inherits the inbound edges $(\pm 1, \mp 1)$, whereas the others remain with 1. So, we finally arrived at the automaton in Figure 8, and we have proved the following theorem.

Theorem 3.6. *Let $q = 2$ and $\mathbf{x}$ and $\mathbf{y}$ be admissible.*

(1) $t(\mathbf{x}, \mathbf{y}) = 0$ *if and only if* $\mathbf{y} = 0$.
(2) $t(\mathbf{x}, \mathbf{y}) \leq 1$ *if and only if* $(x_j + y_j)_{j \geq 0}$ *is admissible.*
(3) *Let* $k \geq 0$. *Then* $t(\mathbf{x}, \mathbf{y}) \leq k + 2$ *if and only if the automaton in Figure 8 does not traverse more than k consecutive solid edges when reading the sequence* $(x_j, y_j)_{j \geq 0}$.

We define t_n to be the expected value of $t(\mathbf{X}, \mathbf{Y})$, where $\mathbf{X}, \mathbf{Y} \in \mathcal{A}_n$ are independent random sequences. Furthermore, we define $w_{nk} := W_n(t(\mathbf{x}, \mathbf{y}) \leq k + 2)$.

Then it is clear that

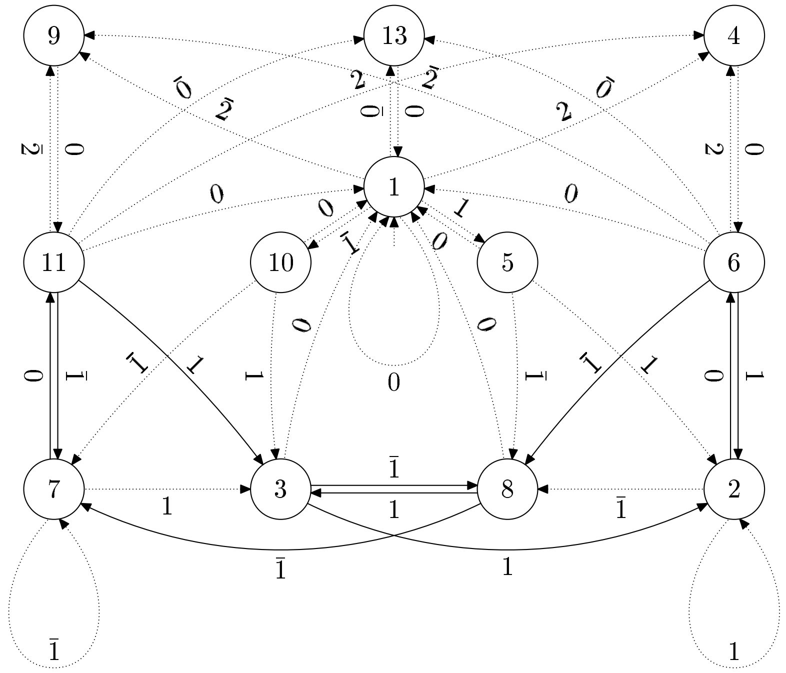
$$\begin{aligned} t_n &= \sum_{k \geq 0} \mathbb{P}_n(t(\mathbf{X}, \mathbf{Y}) > k) = 3 + \sum_{k=0}^{n} \left(1 - \frac{w_{n(k+1)}}{W_n^2(\mathcal{A}_n)}\right) + O\left(\frac{w_{n1}}{W_n^2(\mathcal{A}_n)}\right) \\ &= 3 + \sum_{k=0}^{n} (1 - w_{n(k+1)}) + O(w_{n1}) + O(n 2^{-n}), \end{aligned}$$

where (25) has been used in the last step.

By Theorem 3.6, w_{nk} is the sum of weights of those admissible sequences $(\mathbf{x}, \mathbf{y})$ which are read by the automaton in Figure 8 traversing at most k consecutive solid edges.

As in Section 3.2, we can make use of symmetry: Nodes i and $i+5$ can be identified for $2 \leq i \leq 6$. Using Table 5, we get the following transition matrices

$$B = \frac{1}{8} \begin{pmatrix} 2 & 0 & 0 & 1 & 4 & 0 & 1 \\ 0 & 2 & 2 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 8 & 0 \\ 4 & 2 & 2 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 & 0 & 0 & 1 \\ 8 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad R = \frac{1}{4} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$



$$0 = (0,0) \qquad \bar{0} = (1,-1), (-1,1)$$
$$1 = (1,0), (0,1) \qquad \bar{1} = (-1,0), (0,-1)$$
$$2 = (1,1) \qquad \bar{2} = (-1,-1)$$

FIGURE 8. $q = 2$: $t(\mathbf{x}, \mathbf{y}) \le k + 2$ if and only if the automaton traverses at most k consecutive solid edges when reading $(x_j, y_j)_{j\ge 0}$.

The only solid zero edge is $(2, 6)$. We adjust the exit vector as in Section 3.2 to forbid paths ending on $\mathcal{R}_{i2}^{=k}$. Furthermore, we have to use the extra weights $e(X_{n-1})$, $e(Y_{n-1})$ determined by the last digits. So we end up with the exit vector

$$\frac{1}{16}(9, 0, 18, 36, 18, 9, 36; 9, 18, 18, 36, 18, 9, 36)^t \\ + \frac{9}{8}(0, 0, 0, 0, 0, 0, 0; \mathcal{R}_{\bar{1}2}^{\le k-1}, \mathcal{R}_{\bar{2}2}^{\le k-1}, \mathcal{R}_{\bar{3}2}^{\le k-1}, \mathcal{R}_{\bar{4}2}^{\le k-1}, \mathcal{R}_{\bar{5}2}^{\le k-1}, \mathcal{R}_{\bar{6}2}^{\le k-1}, \mathcal{R}_{\bar{7}2}^{\le k-1})^t.$$

The resulting generating function is

$$G^{\le k+1}(z) = \sum_{n\ge 0} w_{n(k+1)} z^n = \frac{s_0(z) + (z/2)^k r_1(z) + (-z/4)^k r_2(z) - 27(-z^2/8)^k z^6}{(1-z)s_0(z) + (z/2)^k s_1(z) + (-z/4)^k s_2(z) + 12(-z^2/8)^k z^7},$$

where

$$r_0(z) = 864(z^2 - 8)(z^2 - 3z - 2), \qquad s_0(z) = 384(z + 2)(z - 4)(z^2 - 8),$$
$$r_1(z) = -72z^3(z^2 + 2z + 16), \qquad s_1(z) = 32z^3(z + 2)(z^2 - 4z + 16),$$
$$r_2(z) = -18z^3(3z^3 - z^2 - 14z - 4), \qquad s_2(z) = 8z^3(z - 1)(3z^3 + 2z^2 - 20z - 16).$$

By Lemma 2.5, we get the final result.

Theorem 3.7. *The expected number t_n of carry propagations $t(\mathbf{X}, \mathbf{Y})$ where $\mathbf{X}$ and $\mathbf{Y}$ are random admissible sequences to base 2 of length n is*

$$t_n = \log_2 n + \log_2 \frac{26}{63} + \frac{\gamma}{\log 2} + \frac{1}{2} + \psi\left(\log_2 n + \log_2 \frac{26}{63}\right) + O\left(\frac{\log^4 n}{n}\right),$$

where $\psi(x)$ is the periodic function given in (14).

References

1. A. W. Burks, H. H. Goldstine, and J. von Neumann, *Preliminary Discussion of the Logical Design of an Electronic Computing Instrument*, 2 ed., Institute for Advanced Study, Princeton, N. J., 1947, See also [8, p. 34].
2. Ph. Flajolet, X. Gourdon, and Ph. Dumas, *Mellin transforms and asymptotics: Harmonic sums*, Theoret. Comput. Sci. **144** (1995), 3–58.
3. R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete mathematics. A foundation for computer science*, second ed., Addison-Wesley, 1994.
4. C. Heuberger and H. Prodinger, *On minimal expansions in redundant number systems: Algorithms and quantitative analysis*, Computing **66** (2001), 377–393.
5. D. E. Knuth, *The average time for carry propagation*, Nederl. Akad. Wetensch. Indag. Math. **40** (1978), 238–242.
6. ———, *Seminumerical algorithms*, third ed., The Art of Computer Programming, vol. 2, Addison-Wesley, 1998.
7. G. W. Reitwiesner, *Binary arithmetic*, Advances in computers, vol. 1, Academic Press, New York, 1960, pp. 231–308.
8. J. von Neumann, *Collected works. Vol. V: Design of computers, theory of automata and numerical analysis*, The Macmillan Co., New York, 1963.

Institut für Mathematik, Technische Universität Graz, Steyrergasse 30, A-8010 Graz, Austria

E-mail address: clemens.heuberger@tugraz.at

URL: http://www.opt.math.tu-graz.ac.at/~cheub/

The John Knopfmacher Centre for Applicable Analysis and Number Theory, School of Mathematics, University of the Witwatersrand, P. O. Wits, 2050 Johannesburg, South Africa

E-mail address: helmut@gauss.cam.wits.ac.za

URL: http://www.wits.ac.za/helmut/index.htm