The digit generating function of a polynomial

Helmut Prodinger[1]

Department of Mathematical Sciences
Stellenbosch University
7602 Stellenbosch
South Africa

Stephan Wagner

Department of Mathematical Sciences
Stellenbosch University
7602 Stellenbosch
South Africa

Abstract

The average frequency of 1 occurring as the kth digit in the binary expansion of squares, cubes, and generally the values of a polynomial is studied. In particular, it turns out that the generating function of these frequencies is rational for the important special cases of powers, linear and quadratic polynomials. For higher degree polynomials, the behaviour seems to be much more chaotic in general, which is exhibited by two examples of cubic polynomials.

Key words: digit frequency, integer polynomial, generating function, Hensel's Lemma

1 Introduction

If one writes down a list of the binary expansions of the first few integers, then one observes the obvious pattern 01010... in the last column, 00110011... in the penultimate, and so on; in this case, it is clear that the "average frequency" of ones, say, is $\frac{1}{2}$ for each of the columns and therefore also in total. If one

Email addresses: hproding@sun.ac.za (Helmut Prodinger), swagner@sun.ac.za (Stephan Wagner).

[1] Supported by the South African Science Foundation NRF, grant 2053748.

sums all the digits (equivalently, counts all the ones) of the first integers (from 0 to $N-1$, say), then there is a celebrated theorem due to Delange [1] that expresses this sum explicitly as

$$\frac{N}{2}\log_2 N + NF(\log_2 N),$$

where $F(x)$ is a periodic function of period 1. The regularity of the pattern for individual digits would only be enough to obtain the main term of order $N \log N$.

Following Delange, a vast literature has developed, dealing with problems of the sum-of-digits function in various contexts. One recent contribution is due to Drmota and Rivat [2] who consider the distribution of the sum of digits of squares, which is inspired by a problem of Gelfond [4]; even more recently, their results were improved by Mauduit and Rivat [6]. It is also a natural question to look for patterns in the sequence of kth digits (from the right) in the sequence of squares, cubes, etc. Clearly, a periodic pattern can always be observed if the values of a polynomial are considered, but the frequency of 1 as the kth digit is not necessarily always $\frac{1}{2}$. One observes for instance that the penultimate digit of a square is always 0. However, if a_n denotes the average frequency of 1 as the nth digit from the right in the sequence of squares, one finds, first empirically, that the generating function of the a_n's is *rational*; this phenomenon persists if one considers the sequence of cubes, or generally arbitrary powers.

This paper is devoted to the study of the generating function of the digit frequencies, which we simply call the *digit generating function*. Indeed, an explicit form of this generating function can be given for arbitrary powers.

Now it is tempting to study—instead of just powers—general polynomials. And for linear and quadratic polynomials, we will show that the generating functions of the frequencies of digits are still rational. In the case of linear polynomials, this is still pretty trivial, but quadratic polynomials already show more interesting behaviour. However, for polynomials of higher degree the behaviour appears to be more "chaotic." We found an example of a cubic polynomial whose digit generating function is (most probably) not rational; if it was, the degree of the denominator polynomial would be in the range of 10^5 at least.

We will first present some preliminaries, then prove explicit formulas for linear and quadratic polynomials as well as powers, and consider cubic polynomials, with the aforementioned example. Furthermore, we show that the "main term" of the digit generating function is the same for all non-constant polynomials. A list of questions and possible extensions finishes the paper.

A key ingredient of our analysis is *Hensel's Lemma* [3,8], a classical result which is (in a sense) an analogue of Newton's method to solve equations.

2 Preliminaries

Definition 1. Let $p(x) \in \mathbb{Z}[x]$ be a polynomial. For positive integers n, we define

$$f(p(x), n) = \frac{|\{0 \le x < 2^n : p(x) \equiv y \mod 2^n \text{ for some } 2^{n-1} \le y < 2^n\}|}{2^n}$$

to be the relative frequency of values x for which the n-th digit (from the right) in the binary representation of $p(x)$ is 1 (assuming that the value of $p(x)$ is positive). Then the *digit generating function* of $p(x)$ is given by

$$D(p(x), z) = \sum_{n \ge 1} f(p(x), n) z^{n-1}.$$

Remark 2. Let us remark that $f(p(x), n)$ can also be defined as the limit

$$f(p(x), n) = \lim_{N \to \infty} \frac{|\{0 \le x < N : p(x) \equiv y \mod 2^n \text{ for some } 2^{n-1} \le y < 2^n\}|}{N}.$$

Furthermore, it is clear that shifts do not alter the digit generating function, i.e.,

$$D(p(x+c), z) = D(p(x), z)$$

holds for an arbitrary integer constant c.

Next, we are going to state some elementary properties of the digit generating function.

Lemma 3. *For an arbitrary polynomial $p(x)$, we have*

$$D(p(x), z) = \frac{1}{2}\Big(D(p(2x), z) + D(p(2x+1), z)\Big),$$

$$D(2p(x), z) = zD(p(x), z),$$

and

$$D(2p(x)+1, z) = 1 + zD(p(x), z).$$

Proof. For the first identity, simply note that

$$\begin{aligned}
f(p(x),n) &= \frac{|\{0 \le x < 2^n \,:\, p(x) \equiv y \mod 2^n \text{ for some } 2^{n-1} \le y < 2^n\}|}{2^n} \\
&= \frac{|\{0 \le x < 2^{n-1} \,:\, p(2x) \equiv y \mod 2^n \text{ for some } 2^{n-1} \le y < 2^n\}|}{2^n} \\
&\quad + \frac{|\{0 \le x < 2^{n-1} \,:\, p(2x+1) \equiv y \mod 2^n \text{ for some } 2^{n-1} \le y < 2^n\}|}{2^n} \\
&= \frac{|\{0 \le x < 2^n \,:\, p(2x) \equiv y \mod 2^n \text{ for some } 2^{n-1} \le y < 2^n\}|}{2^{n+1}} \\
&\quad + \frac{|\{0 \le x < 2^n \,:\, p(2x+1) \equiv y \mod 2^n \text{ for some } 2^{n-1} \le y < 2^n\}|}{2^{n+1}} \\
&= \frac{1}{2}\Big(f(p(2x),n) + f(p(2x+1),n)\Big).
\end{aligned}$$

For the second and third statement, all we need is the identity

$$\begin{aligned}
f(2p(x),n) &= \frac{|\{0 \le x < 2^n \,:\, 2p(x) \equiv y \mod 2^n \text{ for some } 2^{n-1} \le y < 2^n\}|}{2^n} \\
&= \frac{|\{0 \le x < 2^n \,:\, p(x) \equiv y \mod 2^{n-1} \text{ for some } 2^{n-2} \le y < 2^{n-1}\}|}{2^n} \\
&= f(p(x),n-1)
\end{aligned}$$

for $n > 1$ (and the analogous identity for $f(2p(x)+1,n)$). Furthermore, it is obvious that $f(2p(x),1) = 0$ and $f(2p(x)+1,1) = 1$. □

The final ingredient we will need is based on Hensel's Lemma: recall that $p'(0) \equiv 1 \mod 2$ implies that the congruence $p(0) \equiv a \mod 2$ can be "lifted" to higher powers of 2: i.e., for every $a' \equiv a \equiv p(0) \mod 2$, we can find $x \equiv 0 \mod 2$ such that

$$p(x) \equiv a' \mod 2^n,$$

and x is unique modulo 2^n. An analogous statement holds if $p'(1) \equiv 1 \mod 2$. Therefore, if $p'(0) \equiv 1 \mod 2$, one has

$$f(p(2x),n) = \frac{1}{2}$$

for all $n > 1$ and $f(p(2x),1) = [p(0) \equiv 1 \mod 2]$ (here, we use Iverson's notation, i.e., $[P] = 1$ if P is true and $[P] = 0$ otherwise). Likewise, if $p'(1) \equiv 1 \mod 2$, one has

$$f(p(2x+1),n) = \frac{1}{2}$$

for all $n > 1$ and $f(p(2x+1),1) = [p(1) \equiv 1 \mod 2]$. Let us summarise this in the following lemma, which restates the above formulas in terms of the digit generating functions:

Lemma 4. *If* $p'(0) \equiv 1 \mod 2$*, then*

$$D(p(2x), z) = [p(0) \equiv 1 \mod 2] + \frac{z}{2(1-z)}.$$

Analogously, if $p'(1) \equiv 1 \mod 2$*, then*

$$D(p(2x+1), z) = [p(1) \equiv 1 \mod 2] + \frac{z}{2(1-z)}.$$

Example 5. Let us use these lemmas to compute the digit generating function in the special case that $p(x) = x^3 + 2x^2 + 3x + 4$: note that $p'(0)$ is odd, and that $p(2x+1) = 8x^3 + 20x^2 + 20x + 10$. This gives us

$$\begin{aligned}
D(x^3+2x^2+3x+4, z) &= \frac{1}{2}\left(\frac{z}{2(1-z)} + D(8x^3+20x^2+20x+10, z)\right) \\
&= \frac{1}{2}\left(\frac{z}{2(1-z)} + z \cdot D(4x^3+10x^2+10x+5, z)\right) \\
&= \frac{1}{2}\left(\frac{z}{2(1-z)} + z\left(1 + z \cdot D(2x^3+5x^2+5x+2, z)\right)\right) \\
&= \frac{z}{4(1-z)} + \frac{z}{2} + \frac{z^2}{2} D(2x^3+5x^2+5x+2, z) \\
&= \frac{z}{4(1-z)} + \frac{z}{2} + \frac{z^2}{2} \cdot \frac{z}{2(1-z)} \\
&= \frac{z(3-2z+z^2)}{4(1-z)} = \frac{1}{2(1-z)} - \frac{1}{2} + \frac{z}{4} - \frac{z^2}{4}.
\end{aligned}$$

It is not very surprising to see that this is essentially $\frac{1}{2(1-z)}$, and looking at this example, it is also tempting to conjecture that the digit generating function is always rational. We will find that this is (probably) not always the case, but we can prove explicit formulas in certain special cases.

3 Explicit formulas

In this section we will provide general results for linear and quadratic polynomials as well as for powers. Let us start with the explicit formula for linear polynomials whose trivial proof is left to the reader.

Theorem 6. *Let* $p(x) = ax + b$ *be a linear polynomial, let* $\ell = \nu_2(a)$ *(i.e.,* 2^ℓ *is the largest power of* 2 *that divides* a*), and let*

$$b = \sum_{j \geq 0} \beta_j 2^j$$

be the base-2 expansion of b (only finitely many β_j are nonzero). Then

$$D(p(x),z) = \frac{z^\ell}{2(1-z)} + \sum_{j=0}^{\ell-1} \beta_j z^j.$$

Remark 7. Note also that the digit generating function of a constant is exactly

$$D(b,z) = \sum_{j\geq 0} \beta_j z^j,$$

where the β_j's are chosen as in the above theorem. Constant polynomials are the only instances for which the digit generating function is a polynomial. Generally, it is also obvious that if the coefficients of a sequence p_k of polynomials converge to those of a polynomial p in the 2-adic sense, $D(p_k(x),z)$ tends to $D(p(x),z)$ as well.

For quadratic polynomials, the situation is already more intricate; we have the following theorem:

Theorem 8. *Let $p(x) = ax^2 + bx + c$ be a quadratic polynomial. If $\nu_2(a) \geq \nu_2(b)$, then there is a polynomial $r(z)$ such that*

$$D(p(x),z) = \frac{1}{2(1-z)} + r(z).$$

If on the other hand $\nu_2(a) < \nu_2(b)$, then there are a positive integer ℓ and polynomials $q(z)$ and $r(z)$ such that

$$D(p(x),z) = z^{\nu_2(a)} \left(\frac{1}{2(1-z)(2-z^2)} + \frac{q(z)}{1-(z^2/2)^\ell} \right) + r(z).$$

The integer ℓ satisfies $2^\ell - 1 \equiv 0 \mod \frac{a}{\gcd(a,b)}$.

Proof. If $\nu_2(a) \geq \nu_2(b) = \nu$, then apply Lemma 3 repeatedly to find that

$$D(p(x),z) = z^\nu D\left(2^{-\nu}ax^2 + 2^{-\nu}bx + \lfloor 2^{-\nu}c \rfloor, z\right) + r_1(z)$$

for some polynomial $r_1(z)$. Now, $2^{-\nu}b$ is odd, implying that the derivative of the polynomial $2^{-\nu}ax^2 + 2^{-\nu}bx + \lfloor 2^{-\nu}c \rfloor$ is always odd. Therefore,

$$D(p(x),z) = z^\nu \left(\frac{z}{2(1-z)} + r_2 \right) + r_1(z),$$

where r_2 is a constant (either 0, 1, or $\frac{1}{2}$). Noticing that

$$\frac{z^{\nu+1}}{2(1-z)} = \frac{1}{2(1-z)} - \frac{1}{2}\left(1 + z + \ldots + z^\nu\right),$$

the theorem follows immediately in this case.

Now we consider the case $\nu = \nu_2(a) < \nu_2(b)$. Since we can apply the same initial step as in our first case, we may assume without loss of generality that a is odd. Then we have

$$\begin{aligned} &D(ax^2+bx+c,z) \\ &\quad = \frac{1}{2}\Big(D(4ax^2+2bx+c,z) + D(4ax^2+(2b+4a)x+(a+b+c),z)\Big) \\ &\quad = \frac{z^2}{2}\left(D\Big(ax^2+\tfrac{b}{2}x+\lfloor\tfrac{c}{4}\rfloor,z\Big) + D\Big(ax^2+\tfrac{b+2a}{2}x+\lfloor\tfrac{a+b+c}{4}\rfloor,z\Big)\right) + r(z) \end{aligned}$$

for a certain linear polynomial $r(z)$ (that depends on a, b, c). Now note that one of $\frac{b}{2}$ and $\frac{b+2a}{2}$ is even, while the other is odd. Therefore, we have

$$D(ax^2+bx+c,z) = \frac{1}{4(1-z)} + r'(z) + \frac{z^2}{2}D(ax^2+b'x+c',z),$$

where

$$b' = \begin{cases} \frac{b}{2} & \frac{b}{2} \text{ even,} \\ \frac{b}{2}+a & \frac{b}{2} \text{ odd,} \end{cases} \qquad \text{and} \qquad c' = \begin{cases} \lfloor\frac{c}{4}\rfloor & \frac{b}{2} \text{ even,} \\ \lfloor\frac{a+b+c}{4}\rfloor & \frac{b}{2} \text{ odd,} \end{cases}$$

and $r'(z)$ is a quadratic polynomial. Now set $b_0 = b$, $c_0 = c$ and

$$b_{k+1} = \begin{cases} \frac{b_k}{2} & \frac{b_k}{2} \text{ even,} \\ \frac{b_k}{2}+a & \frac{b_k}{2} \text{ odd,} \end{cases} \qquad \text{and} \qquad c_{k+1} = \begin{cases} \lfloor\frac{c_k}{4}\rfloor & \frac{b_k}{2} \text{ even,} \\ \lfloor\frac{a+b_k+c_k}{4}\rfloor & \frac{b_k}{2} \text{ odd,} \end{cases}$$

and let $r_k(z)$ be the polynomial for which

$$D(ax^2+b_kx+c_k,z) = \frac{1}{4(1-z)} + r_k(z) + \frac{z^2}{2}D(ax^2+b_{k+1}x+c_{k+1},z).$$

Furthermore, we write $p_k(x) = ax^2+b_kx+c_k$ as an abbreviation. Then a simple induction shows that

$$D(p_0(x),z) = \frac{1}{4(1-z)}\sum_{i=0}^{\ell-1}\frac{z^{2i}}{2^i} + \sum_{i=0}^{\ell-1}\frac{z^{2i}}{2^i}r_i(z) + \frac{z^{2\ell}}{2^\ell}D(p_\ell(x),z)$$

and more generally

$$D(p_k(x),z) = \frac{1}{4(1-z)}\sum_{i=0}^{\ell-1}\frac{z^{2i}}{2^i} + \sum_{i=0}^{\ell-1}\frac{z^{2i}}{2^i}r_{k+i}(z) + \frac{z^{2\ell}}{2^\ell}D(p_{k+\ell}(x),z).$$

Both b_k and c_k are bounded (one has $|b_k| \leq \max(|b|, 2|a|)$ and $|c_k| \leq \max(|a|,|b|,|c|)$, as can easily be seen by induction), and so there will be some k and ℓ such that $p_k(x) = p_{k+\ell}(x)$. This implies

$$D(p_k(x), z) = \frac{1}{2(1-z)(2-z^2)} + \frac{s_1(z)}{1-(z^2/2)^\ell},$$

where $s_1(z)$ is used as an abbreviation for the sum

$$\sum_{i=0}^{\ell-1} \frac{z^{2i}}{2^i} r_{k+i}(z).$$

Now we use

$$D(p_0(x), z) = \frac{1}{4(1-z)} \sum_{i=0}^{k-1} \frac{z^{2i}}{2^i} + \sum_{i=0}^{k-1} \frac{z^{2i}}{2^i} r_i(z) + \frac{z^{2k}}{2^k} D(p_k(x), z)$$

and find that

$$D(p_0(x), z) = \frac{1}{2(1-z)(2-z^2)} + \frac{z^{2k}}{2^k} \cdot \frac{s_1(z)}{1-(z^2/2)^\ell} + s_2(z),$$

where

$$s_2(z) = \sum_{i=0}^{k-1} \frac{z^{2i}}{2^i} r_i(z).$$

This proves the second part of the theorem. □

In the following section, we will see that the behaviour for cubic polynomials can be quite unpredictable; before that, we state a general formula for powers:

Theorem 9. *The digit generating function of a power $p(x) = x^k$ is given by*

$$D(x^k, z) = \begin{cases} \dfrac{2-z}{2(1-z)(2-z^k)} & k \text{ odd,} \\ \dfrac{2-2z+z^{\ell+2}}{2(1-z)(2-z^k)} & k \text{ even,} \end{cases}$$

where in the latter case $\ell = \nu_2(k)$.

Proof. If k is odd, then $p'(1) \equiv 1 \mod 2$, and we obtain

$$\begin{aligned} D(x^k, z) &= \frac{1}{2}\Big(D((2x)^k, z) + D((2x+1)^k, z)\Big) \\ &= \frac{1}{2}\Big(z^k D(x^k, z) + 1 + \frac{z}{2(1-z)}\Big). \end{aligned}$$

Solving for $D(x^k, z)$ yields the desired result. If on the other hand k is even, we consider $(2x+1)^k$. Note that all coefficients of $(2x+1)^2 = 4x^2+4x+1$, except for the constant one, are divisible by 4, and it is just an easy induction to show that all coefficients of $(2x+1)^{2^\ell}$, except for the constant one, are divisible by $2^{\ell+1}$. The same statement follows immediately for $(2x+1)^k$ whenever 2^ℓ divides k. Therefore, the polynomial

$$q_k(x) = \frac{(2x+1)^k - 1}{2^{\ell+1}}$$

is an integer polynomial, and its derivative

$$q_k'(x) = \frac{k}{2^\ell}(2x+1)^{k-1}$$

is odd for every integer x, so that we can make use of Hensel's Lemma (note also that $q_k(0) = q_k(-1) = 0$, so that $q_k(x)$ is always even). Now we may progress as in the first case to obtain

$$\begin{aligned} D(x^k, z) &= \frac{1}{2}\Big(D((2x)^k, z) + D((2x+1)^k, z)\Big) \\ &= \frac{1}{2}\Big(D((2x)^k, z) + 1 + z^{\ell+1} D(q_k(x), z)\Big) \\ &= \frac{1}{2}\left(z^k D(x^k, z) + 1 + \frac{z^{\ell+2}}{2(1-z)}\right), \end{aligned}$$

proving our theorem in the case that k is even. □

4 Cubic polynomials

Let us consider cubic polynomials now; our initial example was an instance of a cubic polynomial with a very simple rational digit generating function. However, it seems that generally the digit generating function can be much more complicated and also difficult to predict. We will exhibit this by considering the two seemingly similar polynomials $p(x) = 4x^3 + 7x^2 + 4x$ and $p(x) = 4x^3 + 5x^2 + 4x$. Generally, for a polynomial of the form $2^k x^3 + ax^2 + bx + c$, where $k \geq 2$, a is odd and b is even, we have

$$\begin{aligned} &D(2^k x^3 + ax^2 + bx + c, z) \\ &= \frac{1}{2}\Big(D\Big(2^{k+3}x^3 + (4a + 3\cdot 2^{k+2})x^2 + (4a + 2b + 3\cdot 2^{k+1})x + (a+b+c+2^k), z\Big) \\ &\quad + D\Big(2^{k+3}x^3 + 4ax^2 + 2bx + c, z\Big)\Big) \\ &= \frac{z^2}{2}\Big(D\Big(2^{k+1}x^3 + (a + 3\cdot 2^k)x^2 + \left(\tfrac{b}{2} + a + 3\cdot 2^{k-1}\right)x + 2^{k-2} + \lfloor\tfrac{a+b+c}{4}\rfloor, z\Big) \\ &\quad + D\Big(2^{k+1}x^3 + ax^2 + \tfrac{b}{2}x + \lfloor\tfrac{c}{4}\rfloor, z\Big)\Big) + r(c,z) + r(a+b+c, z), \end{aligned}$$

where $r(m,z)$ is defined by

$$r(m,z)=\begin{cases}0 & m\equiv 0 \mod 4,\\ 1 & m\equiv 1 \mod 4,\\ z & m\equiv 2 \mod 4,\\ 1+z & m\equiv 3 \mod 4.\end{cases}$$

Now note that either $\frac{b}{2}$ or $\frac{b}{2}+a+3\cdot 2^{k-1}$ is even again, while the other is odd, which also leads to an odd derivative. As in the case of quadratic polynomials, this gives rise to a sequence of polynomials $p_k(x)=2^kx^3+a_kx^2+b_kx+c_k$ that is defined by

$$a_{k+1}=\begin{cases}a_k & \frac{b_k}{2} \text{ even},\\ a_k+3\cdot 2^k & \frac{b_k}{2} \text{ odd},\end{cases}$$

$$b_{k+1}=\begin{cases}\frac{b_k}{2} & \frac{b_k}{2} \text{ even},\\ \frac{b_k}{2}+a_k+3\cdot 2^{k-1} & \frac{b_k}{2} \text{ odd},\end{cases}$$

and

$$c_{k+1}=\begin{cases}\lfloor\frac{c_k}{4}\rfloor & \frac{b_k}{2} \text{ even},\\ \lfloor\frac{a_k+b_k+c_k}{4}\rfloor+2^{k-2} & \frac{b_k}{2} \text{ odd}.\end{cases}$$

With these definitions, we can write our recursion as

$$D(p_k(x),z)=\frac{z^2}{2}D(p_{k+1}(x),z)+\frac{z^3}{4(1-z)}+\frac{1}{2}\Big(r(c_k,z)+r(a_k+b_k+c_k,z)\Big)+\frac{s_kz^2}{2},$$

where

$$s_k=\begin{cases}0 & \frac{b_k}{2} \text{ even and } \lfloor\frac{a_k+b_k+c_k}{4}\rfloor+2^{k-2} \text{ even},\\ 1 & \frac{b_k}{2} \text{ even and } \lfloor\frac{a_k+b_k+c_k}{4}\rfloor+2^{k-2} \text{ odd},\\ 0 & \frac{b_k}{2} \text{ odd and } \lfloor\frac{c_k}{4}\rfloor \text{ even},\\ 1 & \frac{b_k}{2} \text{ odd and } \lfloor\frac{c_k}{4}\rfloor \text{ odd}.\end{cases}$$

Iterating the recursion yields, as in the case of quadratic polynomials,

$$D(p_k(x),z)=\frac{z^3}{4(1-z)}\sum_{i=0}^{\ell-1}\frac{z^{2i}}{2^i}+\sum_{i=0}^{\ell-1}\frac{z^{2i}}{2^i}q_{k+i}(z)+\frac{z^{2\ell}}{2^\ell}D(p_{k+\ell}(x),z),$$

where

$$q_k(z)=\frac{r(c_k,z)+r(a_k+b_k+c_k,z)+s_kz^2}{2}.$$

This time, it is not guaranteed that $p_k=p_{k+\ell}$ will ever occur. However, we can take the formal limit $\ell\to\infty$ in this formula to find

$$D(p_k(x),z)=\frac{z^3}{2(1-z)(2-z^2)}+\sum_{i=0}^{\infty}\frac{z^{2i}}{2^i}q_{k+i}(z).$$

This is a rational function if and only if the sequence $q_i(z)$ is periodic. This is sometimes the case, but apparently not always, as our examples show. Consider the case of the polynomial $p(x) = p_2(x) = 4x^3 + 7x^2 + 4x$ first, i.e., $a_2 = 7$, $b_2 = 4$ and $c_2 = 0$. An easy induction shows that

$$a_k = \begin{cases} 2^{k+1} - 1 & k \text{ even,} \\ 2^k - 1 & k \text{ odd,} \end{cases} \qquad b_k = \begin{cases} \frac{4}{3}(2^k - 1) & k \text{ even,} \\ \frac{2}{3}(2^{k-1} - 1) & k \text{ odd,} \end{cases}$$

and

$$c_k = \begin{cases} \left\lfloor \frac{4}{27}(2^{k+1} - 3) \right\rfloor & k \text{ even,} \\ \left\lfloor \frac{1}{27}(2^k - 3) \right\rfloor & k \text{ odd.} \end{cases}$$

The periodicity of the q_i follows immediately, even though the period is long: one has $q_{i+18} = q_i$ for all $i > 2$ (which is proved by straightforward modular arithmetic). Finally, we get

$$\begin{aligned} D(4x^3 + 7x^2 + 4x, z) = \frac{1}{2(1-z)} &+ \frac{z^2}{2(z^2-2)(z^4+2z^2+4)(z^{12}+8z^6+64)} \\ &\times \Big(z^{18} + z^{16} + 2z^{14} - 4z^{13} - 4z^{12} - 8z^{11} - 8z^{10} + 16z^9 \\ &\quad - 16z^8 + 32z^6 - 64z^4 + 128z^2 + 256z - 256\Big). \end{aligned}$$

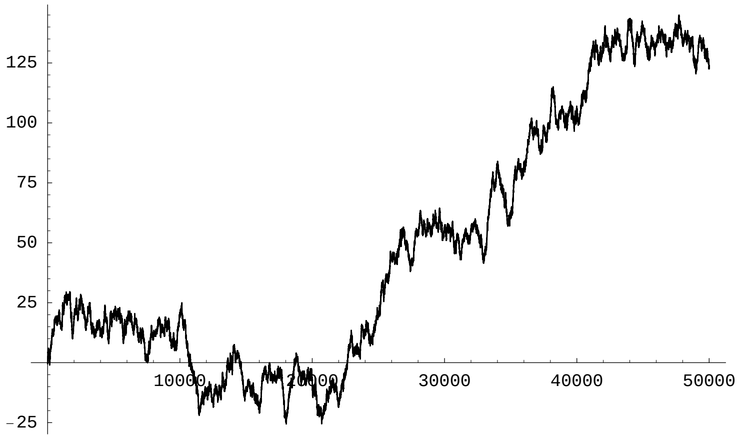
The situation is totally different in the case of the polynomial $p(x) = p_2(x) = 4x^3+5x^2+4x$, i.e., $a_2 = 5$, $b_2 = 4$ and $c_2 = 0$. We were not able to prove that the sequence q_i is not periodic in this case, but computational evidence suggests that this is the case. In the following two graphs, we show the cumulative sums of the linear and quadratic coefficient of q_i respectively (it is easy to see that the constant coefficient is always $\frac{1}{2}$), reduced by the linear drift, i.e. the plots show

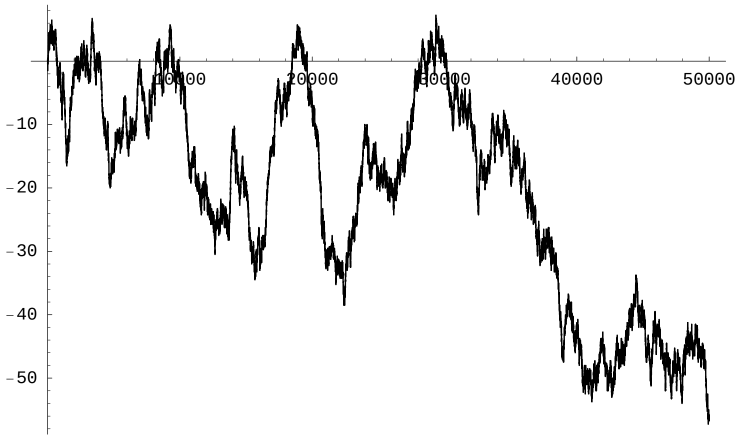
$$\sum_{i=2}^{N+1} [z^1] q_i(z) - \frac{N}{2}$$

and

$$\sum_{i=2}^{N+1} [z^2] q_i(z) - \frac{N}{4},$$

respectively. The resulting graphs are reminiscent of the typical shape of a random walk. This seemingly erratic behaviour makes it unlikely that the digit generating function is rational in this example. Judging from computer experiments, we also conjecture that it is not even algebraic or D-finite.





5 The main term

From the results obtained so far, it is tempting to conjecture that

$$f(p(x), n) = \frac{1}{2} + o(1)$$

for every non-constant polynomial p. Indeed, this can be proved by means of exponential sums. Note first that

$$\begin{aligned} f(p(x), n) &= \frac{|\{0 \le x < 2^n \,:\, p(x) \equiv y \mod 2^n \text{ for some } 2^{n-1} \le y < 2^n\}|}{2^n} \\ &= 2^{-n} \left| \left\{ 0 \le x < 2^n \,:\, \left\{ 2^{-n} p(x) \right\} \ge \frac{1}{2} \right\} \right|, \end{aligned}$$

where $\{u\}$ is the fractional part of u, and recall that the discrepancy of a set $X = \{x_1, x_2, \ldots, x_N\} \subseteq [0, 1)$ is defined by

$$D(x_1, x_2, \ldots, x_N) = \sup_I \left| \frac{|X \cap I|}{N} - \lambda(I) \right|,$$

where the supremum is taken over all subintervals of $[0,1)$, $|X \cap I|$ is the number of elements of X that fall into I, and $\lambda(I)$ is the Lebesgue measure of I. From this definition, it follows immediately that

$$\left|f(p(x),n) - \frac{1}{2}\right| \le D\left(2^{-n}p(0), 2^{-n}p(1), \ldots, 2^{-n}p(2^n-1)\right).$$

Now we apply the Erdős-Turán inequality (see [5]): there is an absolute constant C such that for any integer m,

$$D(x_1, x_2, \ldots, x_N) \le C\left(\frac{1}{m} + \sum_{h=1}^{m} \frac{1}{h}\left|\frac{1}{N}\sum_{j=1}^{N} e^{2\pi i h x_j}\right|\right).$$

In our case, $N = 2^n$, and $x_j = 2^{-n}p(j-1) = p(j-1)/N$. Therefore,

$$D(x_1, x_2, \ldots, x_N) \le C\left(\frac{1}{m} + \sum_{h=1}^{m} \frac{1}{h}\left|\frac{1}{N}\sum_{j=0}^{N-1} e^{2\pi i h p(j)/N}\right|\right). \tag{1}$$

The exponential sum can be estimated by means of Weyl's inequality ([9], see also [7] for instance): assume that $k = \deg p > 1$ (the case $k = 1$ is trivial in view of Theorem 6); if $g(x) = \alpha x^k + \ldots$ is an arbitrary polynomial of degree k such that $|\alpha - \frac{a}{q}| \le \frac{1}{q^2}$ for coprime integers a and q, then

$$\sum_{n=0}^{N-1} e^{2\pi i g(n)} \ll N^{1+\epsilon}(N^{-1} + q^{-1} + N^{-k}q)^{1/K}$$

for $K = 2^{k-1}$ and arbitrary $\epsilon > 0$, where the implied constant only depends on ϵ and k. We apply Weyl's inequality with $g(x) = hp(x)/N$. If b is the leading coefficient of $p(x)$, then $\alpha = \frac{hb}{N} = \frac{a}{q}$ for certain integers a and q, and $N/h \ll q \ll N$. Now we use this in (1) to obtain

$$\begin{aligned}
D(x_1, x_2, \ldots, x_N) &\ll \frac{1}{m} + \sum_{h=1}^{m} \frac{1}{h}\left|\frac{1}{N}\sum_{j=0}^{N-1} e^{2\pi i h p(j)/N}\right| \\
&\ll \frac{1}{m} + \sum_{h=1}^{m} \frac{1}{h} N^{\epsilon}(N^{-1} + hN^{-1} + N^{1-k})^{1/K} \\
&\ll \frac{1}{m} + \sum_{h=1}^{m} \frac{1}{h} N^{\epsilon}(hN^{-1})^{1/K} \\
&\ll \frac{1}{m} + N^{\epsilon - 1/K}\sum_{h=1}^{m} h^{1/K-1} \\
&\ll \frac{1}{m} + N^{\epsilon-1/K} m^{1/K}.
\end{aligned}$$

Choosing $m \sim N^{1/(K+1)}$ finally yields

$$D(x_1, x_2, \ldots, x_N) \ll N^{\epsilon - 1/(K+1)}.$$

Putting everything together, we arrive at the following theorem:

Theorem 10. *If $p(x)$ is a polynomial of degree $k > 1$, then*

$$f(p(x), n) = \frac{1}{2} + O\left(2^{-n(1/(2^{k-1}+1)-\epsilon)}\right)$$

for any $\epsilon > 0$. This implies that

$$D(p(x), z) - \frac{1}{2(1-z)}$$

has radius of convergence $\geq 2^{1/(2^{k-1}+1)}$.

The exponent in this bound is probably not best possible. In view of our general theorem for power functions (Theorem 9), the best error term one can hope for is

$$f(p(x), n) = \frac{1}{2} + O\left(2^{-n/k}\right),$$

and for $k = 2$ this estimate holds indeed in view of Theorem 8, but generally there is a substantial gap between $\frac{1}{k}$ and $\frac{1}{2^{k-1}+1}$. It might be a challenging problem to determine the best possible error term for general k.

6 Conclusion

Several open problems remain, and of course our considerations can be generalised in many directions. For instance, it would be interesting to characterise all polynomials with a rational digit generating function (or those with an algebraic/D-finite digit generating function, ...).

Instead of binary expansions, one could also consider arbitrary bases, Gray code representations, or “exotic” number systems such as linear recursive number systems (the Zeckendorf expansion is a well-known example of this type). If other digits than 0 and 1 are allowed, one can define several digit generating functions, one for each possible digit (in the binary case, the generating functions for the frequencies of 0 and 1 are connected by an obvious relation). Finally, it might also be interesting to consider blocks of digits rather than single digits only (Theorem 10 can be generalised immediately, for instance).

Acknowledgment

The authors are highly indebted to an anonymous referee for pointing out the proof of Theorem 10.

References

[1] H. Delange. Sur la fonction sommatoire de la fonction“somme des chiffres”. *Enseignement Math. (2)*, 21(1):31–47, 1975.

[2] M. Drmota and J. Rivat. The sum-of-digits function of squares. *J. London Math. Soc. (2)*, 72(2):273–292, 2005.

[3] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[4] A. O. Gel′fond. Sur les nombres qui ont des propriétés additives et multiplicatives données. *Acta Arith.*, 13:259–265, 1967/1968.

[5] L. Kuipers and H. Niederreiter. *Uniform distribution of sequences*. Wiley-Interscience [John Wiley & Sons], New York, 1974.

[6] C. Mauduit and J. Rivat. La somme des chiffres des carrés. Acta Mathematica, to appear.

[7] M. B. Nathanson. *Additive number theory*, volume 164 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[8] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.

[9] H. Weyl. Über die Gleichverteilung von Zahlen mod. Eins. *Math. Ann.*, 77(3):313–352, 1916.