Forschungsschwerpunkt

Algorithmen und mathematische Modellierung

Graz University of Technology

Hamming Weight of the Non-Adjacent-Form under Various Input Statistics

Clemens Heuberger and Helmut Prodinger

Project Area(s):

Analysis of Digital Expansions with Applications in Cryptography

Institut für Optimierung und Diskrete Mathematik (Math B)

Report 2007-1, April 2007

HAMMING WEIGHT OF THE NON-ADJACENT-FORM UNDER VARIOUS INPUT STATISTICS

CLEMENS HEUBERGER AND HELMUT PRODINGER

Abstract. The Hamming weight of the non-adjacent form is studied in relation to the Hamming weight of the standard binary expansion. In particular, we investigate the expected Hamming weight of the NAF of a n-digit binary expansion with k ones where k is either fixed or proportional to n. The expected Hamming weight of NAFs of binary expansions with large ($\geq n/2$) Hamming weight is studied. Finally, the covariance of the Hamming weights of the binary expansion and the NAF is computed. Asymptotically, these Hamming weights become independent and normally distributed.

1. Introduction

Signed digit expansions of low Hamming weight are important in various branches of Mathematics and Computer Science, such as efficient arithmetic [16], coding theory [18], and cryptography [15]. A prominent example is the so-called Non-Adjacent-Form (NAF) which uses the digits 0, 1, and -1 and base 2:

$$m = \sum_{j=0}^{n} \varepsilon_j 2^j$$

with $\varepsilon_j \varepsilon_{j+1} = 0$ for all j. It is well-known [16] that every integer admits exactly one such representation and that it minimises the Hamming weight (the number of non-zero digits) over all representations of the same integer with digit 0, 1, -1 (but without imposing the syntactic restriction).

The expected Hamming weight of a non-negative integer less than 2^n is known to be $\frac{1}{3}n + O(1)$, cf. for instance [2, 15, 11]. A more detailed analysis can be found in [17], [8], and [9].

The aim of this paper is to study the expected Hamming weight under more refined input models, for instance: Does the expected Hamming weight increase, if the input is known

Date: April 12, 2007.

2000 *Mathematics Subject Classification.* 11A63; 68W40 68Q45 05A16 05A15.

Key words and phrases. Non-adjacent form; binary expansion; Hamming weight; transducer; generating function; Omega operator; singularity analysis; quasi-power theorem; multivariate asymptotics.

This paper was written while C. Heuberger was a visitor at the Center of Experimental Mathematics at the University of Stellenbosch. He thanks the center for its hospitality. He is also supported by the Austrian Science Foundation FWF, project S9606, that is part of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory."

H. Prodinger is supported by the NRF grant 2053748 of the South African National Research Foundation and by the Center of Experimental Mathematics of the University of Stellenbosch.

to have a binary expansion of large Hamming weight? How big is the correlation between the Hamming weights of the binary expansion and the NAF? Are they independent?

Obviously, the non-negative integers less than 2^n are exactly those with standard binary expansion of length at most n. We study the expected Hamming weight of the NAF of such an integer under the assumption that its binary expansion has Hamming weight k for k/n in a certain range (Theorem 1). For instance, if $k/n \approx \alpha$, the expected Hamming weight is asymptotically equal to

$$\frac{1-4\left(\alpha-\frac{1}{2}\right)^2}{3+4\left(\alpha-\frac{1}{2}\right)^2}n.$$

For $\alpha = 1/2$, this equals $n/3$ as in the unrestricted case, otherwise, the expected Hamming weight is smaller.

If k is fixed and only n tends to infinity, Theorem 2 states that the expected Hamming weight is $k + O(1/n^2)$. The intuitive explanation is that for k small with respect to n, i.e., the ones in the binary expansion are sparse, the NAF tends to agree with the binary expansion.

In Theorem 3, we study the expected Hamming weight under the assumption that the Hamming weight of the binary expansion is “large”, i.e., at least $n/2$. So these are the worst cases of the binary expansion. The NAF, however, is quite immune: the expected Hamming weight is still asymptotic to

$$\frac{n}{3} + \frac{4}{9} + \frac{2\sqrt{2}\,(7+(-1)^n)}{9\pi}\cdot\frac{1}{\sqrt{n}} + O\left(\frac{1}{n}\right).$$

The difference to the unrestricted input model only occurs in the coefficient of $1/\sqrt{n}$.

Finally, we consider the Hamming weight of the binary expansion and the Hamming weight of the NAF as a random vector and study their covariance as well as its limiting distribution (Theorem 4). The covariance is

$$\frac{2}{3} + O\left(\frac{n}{2^n}\right),$$

which is an order of magnitude smaller than the variances, but still non-zero. Asymptotically, however, the coordinates of the random vector become independent and normally distributed.

The methods used include transducer automata and generating functions, in particular bivariate rational generating functions. Asymptotics in the central region are derived via Bender and Richmond’s [3, 4] method, in the case of fixed k by singularity analysis as introduced by Flajolet and Odlyzko [6], cf. also the forthcoming book of Flajolet and Sedgewick [7]. For the large input Hamming weight case, MacMahon’s Omega operator [14] is used to select the relevant terms of the generating function, cf. also [1]. The coefficients are again estimated by singularity analysis. Finally, the limiting distribution of the random vector outlined above is derived via a variant of Hwang’s [13] quasi-power theorem, cf. [10].

Acknowledgement. The authors thank S. Wagner for fruitful discussions on Theorem 1.

2. Generating Functions

As usual, the *unsigned (or standard) binary expansion* of an integer m is the unique sequence ε_j, $j \geq 0$, with $\varepsilon_j \in \{0,1\}$ such that $m = \sum_{j\geq 0} \varepsilon_j 2^j$. We will sometimes omit the words "unsigned" or "standard" and just speak about the "binary expansion". The *non-adjacent-form (NAF)* of an integer m is the unique sequence ε_j, $j \geq 0$, with $\varepsilon_j \in \{-1,0,1\}$ such that $m = \sum_{j\geq 0} \varepsilon_j 2^j$ and $\varepsilon_j \varepsilon_{j+1} = 0$ for $j \geq 0$. Existence and uniqueness of the NAF have been proved in [16]. The *Hamming weight* of an expansion ε_j, $j \geq 0$, is the number of nonzero ε_j.

Let $a_{k\ell n}$ be the number of nonnegative integers less than 2^n whose unsigned binary expansion has Hamming weight k and whose NAF has Hamming weight ℓ. We consider the generating function

$$G(x,y,z) = \sum_{k,\ell,n\geq 0} a_{k,\ell,n} x^k y^\ell z^n.$$

To compute $G(x,y,z)$, we use the transducer automaton mapping the unsigned binary expansion of an integer to its NAF. It is shown in Figure 1 (for instance, it is equivalent to the transducer in [12, Figure 2]). The labels of the states correspond to carries. Note that input and output are read resp. written from right to left. An edge with input Hamming weight k and output Hamming weight ℓ corresponds to an entry $x^k y^\ell z$ in the transition matrix M of this transducer:

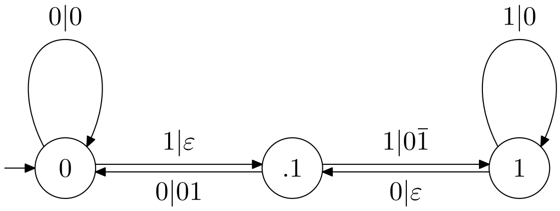

Figure 1. Transducer mapping a binary expansion of an integer to its NAF.

$$M = \begin{pmatrix} z & xz & 0 \\ yz & 0 & xyz \\ 0 & z & xz \end{pmatrix}.$$

Here, the states have been ordered as 0, .1, 1. Given an integer m less than 2^n, the transducer runs from the initial state 0 to some state reading the n-digit unsigned binary input. If this run ends in some state $\neq 0$ (representing some carry), the output is not yet finished: If ending in state .1 or 1, there is an additional output 01 (corresponding to a contribution y) in both cases. Therefore, the generating function G is given by

$$G(x,y,z) = (1,0,0)(I-M)^{-1}(1,y,y)^t,$$

where the superscript t indicates transposition of the vector. This can be evaluated to

$$G(x,y,z) = \frac{x^2y^2z^2 - x^2yz^2 - xyz^2 - xz + xyz + 1}{x^2yz^3 + xyz^3 + xz^2 - 2xyz^2 - xz - z + 1}.$$

We are interested in

$$b_{kn} := \sum_{\ell \geq 0} \ell a_{k\ell n},$$

which corresponds (after division by the mass $M_{kn} = \sum_{\ell \geq 0} a_{k\ell n}$) to the expected Hamming weight of the NAF of an nonnegative integer less than 2^n with Hamming weight k of its unsigned binary expansion.

The generating function $\sum_{k,n \geq 0} b_{kn} x^k z^n$ can be obtained by differentiating $G(x, y, z)$ with respect to y and setting $y = 1$:

$$G_y(x, 1, z) = \sum_{k,n \geq 0} b_{kn} x^k z^n = \frac{xz\,(x^2z^2 + xz^2 - 1)}{(xz + z - 1)^2\,(xz^2 - 1)}. \tag{1}$$

The mass $M_{kn} = \sum_{\ell \geq 0} a_{k\ell n}$ is the number of n-digit unsigned binary expansions with Hamming weight k, thus

$$M_{kn} = \binom{n}{k}.$$

Of course, this corresponds to

$$\sum_{k,n \geq 0} M_{kn} x^k z^n = G(x, 1, z) = \frac{1}{1 - z - xz}$$

which is the generating function of the binomial coefficients by the recursion of Pascal's triangle.

In Section 3, we need a quite trivial lower bound for b_{kn}, which shall be derived at this point.

Lemma 2.1. *For $n \geq 2k - 1$, the estimate $b_{kn} \geq k(n - 2k + 2)$ holds.*

Proof. Consider the number

$$m_j = (\underbrace{0 \ldots 0}_{n-j-2k+1 \text{ digits}} \; 1 \underbrace{0 \ldots 0}_{j \text{ digits}} \underbrace{0101 \ldots 0101}_{2k-2 \text{ digits}})_2$$

for $0 \leq j \leq n - 2k + 1$ given by its unsigned binary expansion. The unsigned binary expansion has Hamming weight k and equals the NAF of m_j. Thus the m_j, $0 \leq j \leq n - 2k + 1$, contribute $(n - 2k + 2)k$ to b_{kn}. □

3. Asymptotics of b_{kn}

The aim of this section is to derive an asymptotic expression for b_{kn}/M_{kn}.

Theorem 1. *Let $0 < c < d < 1$ be real numbers. Then the expected Hamming weight of the NAF of a nonnegative integer less than 2^n with unsigned binary digit expansion of Hamming weight k is asymptotically*

$$\frac{b_{kn}}{M_{kn}} \sim \frac{1 - 4\left(\frac{k}{n} - \frac{1}{2}\right)^2}{3 + 4\left(\frac{k}{n} - \frac{1}{2}\right)^2} n, \tag{2}$$

uniformly for $c \leq k/n \leq d$.

Remark 3.1. If $k/n \sim \alpha$ for a fixed α in the interval $(0,1)$, then the expected Hamming weight of the NAF of a nonnegative integer less than 2^n with unsigned binary digit expansion of Hamming weight k is asymptotically

$$\frac{b_{kn}}{M_{kn}} \sim \frac{1-4\left(\alpha-\frac{1}{2}\right)^2}{3+4\left(\alpha-\frac{1}{2}\right)^2} n. \tag{3}$$

Remark 3.2. The coefficient

$$\frac{1-4\left(\alpha-\frac{1}{2}\right)^2}{3+4\left(\alpha-\frac{1}{2}\right)^2} \tag{4}$$

attains its maximum $1/3$ for $\alpha = 1/2$. Note that the average Hamming weight of a NAF of an integer less than 2^n (without restrictions on the input Hamming weight) is also $n/3+O(1)$. The intuitive explanation for that is that $M_{\alpha n,n}$ obviously attains its maximum at $\alpha = 1/2$, and the decrease of $M_{\alpha n,n}$ is sufficient such that all other $b_{\alpha n,n}/M_{\alpha n,n}$ do not influence the overall outcome too much anyway.

It is also worth noting that the expression (4) is independent of the sign of $(\alpha - 1/2)$, i.e.,

$$\frac{b_{\alpha n,n}}{M_{\alpha n,n}} \sim \frac{b_{(1-\alpha)n,n}}{M_{(1-\alpha)n,n}}.$$

On the level of generating functions, this corresponds to

$$\sum_{k,n\geq 0} (b_{kn} - b_{n-k,n}) x^k z^n = G_y(x,1,xz) - G_y(1/x,1,xz) = \frac{(x-1)z(xz+z+1)}{(xz+z-1)(xz^2-1)}.$$

Comparing this with (1), we note that in the denominator, the factor $(xz+z-1)$ only occurs once instead of twice.

The main part of the proof relies the following lemma formulated by Drmota [5], which is a combination of results of Bender [3] and Bender and Richmond [4]. Note that the letters k and n have been switched in comparison to [5].

Lemma 3.3. *Let $c(x,z) = \sum_{k,n\geq 0} c_{kn} x^k z^n$ be a generating function of non-negative numbers c_{kn} and let $a < b$ be positive real numbers such that $c(x, b+\varepsilon)$ has positive radius of convergence (as a function in x) for some $\varepsilon > 0$. Suppose that*

$$\varphi_k(z) = \sum_{n\geq 0} c_{kn} z^n \sim a_k g(z) \lambda(z)^k \qquad (k \to \infty)$$

holds uniformly in $R(a,b,\phi) = \{z : a \leq |z| \leq b, |\arg(z)| \leq \phi\}$ for some $\phi > 0$, where $a_k > 0$, $g(z)$ is continuous and non-zero and $\lambda(z)$ is non-zero and has bounded third derivative for $z \in R(a,b,\phi)$. Furthermore suppose that $\frac{d^2}{ds^2} \log \lambda(e^s)|_{e^s=z} \neq 0$ for $z \in [a,b]$ and that there exists a $\delta > 0$ such that $c(x,z)$ is analytic and bounded for $|z| \in [a,b], z \notin R(a,b,\phi)$, and $|x| \leq (1+\delta)/\lambda(|z|)$. Then $\frac{d^2}{ds^2} \log \lambda(e^s)|_{e^s=z} > 0$ and we have

$$c_{kn} \sim \frac{a_k}{\sqrt{2\pi k}} \frac{g(h(n/k))}{\sigma(h(n/k))} \frac{\lambda(h(n/k))^k}{h(n/k)^n}$$

uniformly for $n/k \in [\mu(a), \mu(b)]$, where

$$\mu(z) = \frac{d}{ds} \log \lambda(e^s)|_{e^s=z},$$
$$\sigma(z) = \left(\frac{d^2}{ds^2} \log \lambda(e^s)|_{e^s=z} \right)^{1/2},$$

and $h(t)$ is the inverse function of $\mu(z)$.

Proof of Theorem 1. We split $G_y(x,1,z)$ into two summands separating the coprime factors depending on x in its denominator:

$$\begin{aligned}
G_y(x,1,z) &= G^{(1)}(x,z) + G^{(2)}(x,z),\\
G^{(1)}(x,z) &= \frac{-xz^5 + 2xz^4 - 3xz^3 + z^3 + 2xz^2 - 2z^2 - xz + 3z - 2}{(1-z+z^2)^2\,(1-xz^2)},\\
G^{(2)}(x,z) &= -\frac{xz^5 + z^5 - 4xz^4 - 4z^4 + 6xz^3 + 8z^3 - 6xz^2 - 10z^2 + 2xz + 7z - 2}{(1-z+z^2)^2\,(1-xz-z)^2}.
\end{aligned}$$

These auxiliary functions are generating functions of some numbers $b_{kn}^{(1)}$ and $b_{kn}^{(2)}$, respectively, i.e.,

$$G^{(j)}(x,z) = \sum_{k,n\ge 0} b_{kn}^{(j)} x^k z^n$$

for $j \in \{1,2\}$.

Our first aim is to show that the contributions $b_{kn}^{(1)}$ are asymptotically smaller than $b_{kn}^{(2)}$ and, in particular, that the $b_{kn}^{(2)}$ are nonnegative, as required by Lemma 3.3.

For fixed z with $|z| < 1$, the function $G^{(1)}(x,z)$ has a simple pole at $x = 1/z^2$ as a function in x, thus the coefficient of x^k of $G^{(1)}(x,z)$ is the negative residue of $G^{(1)}(x,z)/x^{k+1}$ at $x = 1/z^2$, and we obtain

$$[x^k]G^{(1)}(x,z) = -\frac{z^{2k-1}}{(1-z+z^2)^2}$$

for $k \ge 1$. Extracting the coefficient of z^n in this expansion amounts to summing up the contribution of the poles of $1/(1-z+z^2)^2$. Since these are double poles, we obtain

$$b_{kn}^{(1)} := [z^n][x^k]G^{(1)}(x,z) = -[z^{n-2k+1}]\frac{1}{(1-z+z^2)^2} = O(n-2k) \tag{5}$$

for $n \ge 2k-1 \ge 1$. Together with Lemma 2.1 we conclude that $b_{nk}^{(2)} := [x^k][z^n]G^{(2)}(x,z) \ge 0$ for all $n \ge 0$ for sufficiently large k (a precise evaluation of $b_{kn}^{(1)}$ would show that $k \ge 1$ is sufficient, but we do not need this in order to use Lemma 3.3). Furthermore, we see that $b_{kn}^{(1)} = o(b_{kn})$ for $k \to \infty$.

For the analysis of $b_{nk}^{(2)}$, we want to apply Lemma 3.3 on $G^{(2)}(x,z)$. We set $b = 1-c$ and $a = 1-d$, respectively. This means $0 < a < b < 1$. From this we see that $G^{(2)}(x, b+\varepsilon)$

has a positive radius of convergence, if we choose $0 < \varepsilon < 1 - b$. Extracting the coefficient of x^k in $G^{(2)}(x, z)$ can be done by routine calculations yielding

$$\varphi_k(z) = \sum_{n\geq 0} b^{(2)}_{kn} z^n = \frac{\left(\frac{z}{1-z}\right)^k (z^4 + kz^3 - 3z^3 - kz^2 + 5z^2 + kz - 5z + 2)}{(1-z)\,(1-z+z^2)^2}. \tag{6}$$

Setting $\lambda(z) = z/(1 - z)$ and

$$g(z) = \frac{z}{(1-z)\,(1-z+z^2)}$$

yields

$$\varphi_k(z) \sim kg(z)\lambda(z)^k \qquad (k \to \infty)$$

uniformly for $a < |z| < b$. We note that $g(z)$ is non-zero and continuous for $z \in [a, b]$ and $\lambda(z) \in \mathcal{C}^\infty[a, b]$. We have

$$\frac{d^2}{ds^2} \log \lambda(e^s)|_{e^s=z} = \frac{z}{(1-z)^2} \neq 0$$

for $z \in [a, b]$. Thus the assumptions of Lemma 3.3 are satisfied with $\phi = \pi$ (thus the assumption on $|z| \in [a, b]$, $z \notin R(a, b, \phi)$ is empty). The quantities involved are

$$\mu(z) = \frac{1}{1-z},$$
$$\sigma(z) = \frac{\sqrt{z}}{1-z},$$
$$h(t) = \frac{t-1}{t}.$$

We obtain

$$b^{(2)}_{kn} \sim \frac{n^{3/2}\sqrt{n-k}\sqrt{k}}{\sqrt{2\pi}(n^2 - nk + k^2)} \left(\frac{n-k}{k}\right)^k \left(\frac{n}{n-k}\right)^n \tag{7}$$

uniformly for $n/k \in [\frac{1}{1-a}, \frac{1}{1-b}] = [\frac{1}{d}, \frac{1}{c}]$.

An asymptotic formula for the mass M_{kn} can be obtained from Stirling's formula:

$$M_{kn} \sim \left(\frac{n}{k}\right)^k \left(\frac{n}{n-k}\right)^{n-k} \sqrt{\frac{n}{2\pi k(n-k)}} \tag{8}$$

Dividing (7) by (8) yields (2), since $b_{kn} \sim b^{(2)}_{kn}$. □

4. Asymptotics of b_{kn} for fixed k

In Theorem 1, the asymptotics of b_{kn} were derived under the assumption that k and n both tend to infinity at the same speed. The purpose of this section is to derive the same statement for fixed k.

Theorem 2. *Let k be a fixed positive integer. Then the expected Hamming weight of the NAF of a nonnegative integer less than 2^n with unsigned binary digit expansion of Hamming weight k is asymptotically*

$$\frac{b_{kn}}{M_{kn}} = k - \frac{k(k^2-3k+2)}{n^2} + O\left(\frac{1}{n^3} + \frac{1}{n^{k-1}}\right), \tag{9}$$

whereas the expected Hamming weight of the NAF of a nonnegative integer less than 2^n with unsigned binary digit expansion of Hamming weight $(n-k)$ is asymptotically

$$\frac{b_{n-k,n}}{M_{n-k,n}} = (k+2) - \frac{2k}{n} - \frac{(k-1)k(k+2)}{n^2} + O\left(\frac{1}{n^3} + \frac{1}{n^{k-1}}\right). \tag{10}$$

Proof of Theorem 2. We only prove (9). The proof of (10) runs along the same lines, it suffices to replace $G_y(x,1,z)$ by $G_y(1/x,1,xz)$.

By (5), we have

$$b_{kn} = [z^n]\varphi_k(z) + O(n) = [z^{n-k}]\frac{(z^4+kz^3-3z^3-kz^2+5z^2+kz-5z+2)}{(1-z)^{k+1}\left(1-z+z^2\right)^2} + O(n),$$

where $\varphi_k(z)$ is given in (6). We extract the asymptotics of b_{kn} by singularity analysis, see Flajolet and Odlyzko [6] and the forthcoming book of Flajolet and Sedgewick [7]. The simple poles at $z=(1\pm\sqrt{-3})/2$ give a contribution of $O(1)$. Expanding around the pole at $z=1$ gives

$$b_{kn} = O(n) + [z^{n-k}]\left(k(1-z)^{-k-1} + (2-k)(1-z)^{1-k} + O(1-z)^{2-k}\right).$$

We have

$$\begin{aligned}[z^n](1-sz)^\alpha = \frac{s^n n^{-\alpha-1}}{\Gamma(-\alpha)}\Bigg(1 &+ \frac{\alpha(\alpha+1)}{2n} + \frac{\alpha(\alpha+1)(\alpha+2)(3\alpha+1)}{24n^2} \\ &+ \frac{\alpha^2(\alpha+1)^2(\alpha+2)(\alpha+3)}{48n^3} + O\left(\frac{1}{n^4}\right)\Bigg)\end{aligned} \tag{11}$$

for $\alpha\notin\{0,1,2,\ldots\}$ by [6, Eqn. (2.2)]. The function hidden in the O-term is meromorphic, thus its contribution to b_{kn} does not exceed $O(n^{k-2-1})$ by [6, Theorem 1]. We obtain

$$b_{kn} = \frac{(n-k)^k}{(k-1)!}\left(1+\frac{k(k+1)}{2n} + \frac{3k^4+14k^3-15k^2+70k-48}{24n^2} + O\left(\frac{1}{n^3}\right)\right) + O(n).$$

On the other hand, the mass M_{kn} can be estimated as

$$M_{kn} = \frac{(n-k)^k}{k!}\left(1+\frac{k(k+1)}{2n} + \frac{3k^4+14k^3+9k^2-2k}{24n^2} + O\left(\frac{1}{n^3}\right)\right).$$

This yields (9). □

5. Binary Expansions of Large Weight

In this section, we focus on the NAFs of integers with unsigned binary expansions of high weight, in particular, with a weight greater or equal half of the length of the binary expansion.

We set

$$c_n := \sum_{k\geq n/2} b_{kn}, \qquad M_n := \sum_{k\geq n/2} M_{kn},$$

and we are interested in the asymptotic behaviour of c_n/M_n.

Theorem 3. *The expected Hamming weight of a nonnegative integer less than 2^n with unsigned binary expansion of weight $\geq n/2$ equals*

$$\frac{c_n}{M_n} = \frac{n}{3} + \frac{4}{9} + \frac{2\sqrt{2}\,(7+(-1)^n)}{9\pi}\cdot\frac{1}{\sqrt{n}} - \frac{16\,(1+(-1)^n)}{9\pi}\cdot\frac{1}{n} + O\left(\frac{1}{n^{3/2}}\right). \tag{12}$$

The expected Hamming weight of a nonnegative integer less than 2^n with unsigned binary expansion of weight $\leq n/2$ equals

$$\frac{n}{3} - \frac{(1+(-1)^n)\sqrt{2}}{3\sqrt{\pi}}\sqrt{n} + \frac{4}{9} + \frac{2+2(-1)^n}{3\pi} - \frac{8+8(-1)^n+23\pi+7(-1)^n\pi}{6\sqrt{2}\sqrt{n}\pi^{3/2}} + O\left(\frac{1}{n}\right). \tag{13}$$

Remark 5.1. If the assumption on the weight of the unsigned binary expansion is removed, then the expected Hamming weight of a nonnegative integer less than 2^n equals

$$\frac{n}{3} + \frac{4}{9} + O(2^{-n}).$$

This means that only the third order term is influenced by the additional assumption $k \geq n/2$, but for even n, the influence of the assumption $k \leq n/2$ is much larger.

Proof of Theorem 3. We focus on the proof of (12). The proof of (13) is quite similar, cf. the comments at the end of this proof.

We consider

$$G_y(\lambda^2, 1, z/\lambda) = \sum_{k,n\geq 0} b_{kn}\lambda^{2k-n}z^n = \frac{\lambda^3 z(\lambda^2 z^2 + z^2 - 1)}{(z-1)(z+1)(z\lambda^2 - \lambda + z)^2},$$

where z and λ are in neighbourhoods of 0 and 1, respectively. We want to extract those summands of the power series with $2k - n \geq 0$, i.e., nonnegative exponents of λ, and setting $\lambda = 1$ afterwards. This amounts to applying MacMahon's [14] Omega operator $\underset{\geq}{\Omega}$ (cf. Andrews, Paule and Riese [1]) to $G_y(\lambda^2, 1, z/\lambda)$:

$$\underset{\geq}{\Omega} G_y(\lambda^2, 1, z/\lambda) = \sum_{\substack{k,n\geq 0\\ 2k-n\geq 0}} b_{kn}z^n = \sum_{n\geq 0} c_n z^n.$$

However, the Mathematica® package described in [1] cannot handle this type of generating function, so we have to apply the Omega operator manually.

We factorise the quadratic term in λ in the denominator of $G_y(\lambda^2,1,z/\lambda)$ and perform a partial fraction decomposition (in λ) to obtain

$$\begin{aligned}G_y(\lambda^2,1,z/\lambda) =&\frac{\lambda z+2}{(z-1)(z+1)}\\&+\frac{16z^6-24wz^4-40z^4+13wz^2+17z^2-2w-2}{(z-1)(z+1)(2z-1)^2(2z+1)^2(w-2\lambda z+1)}\\&-\frac{2\left(2z^2-w-1\right)z^2}{(z-1)(z+1)(2z-1)(2z+1)(w-2\lambda z+1)^2}\\&-\frac{16z^6+24wz^4-40z^4-13wz^2+17z^2+2w-2}{(z-1)(z+1)(2z-1)^2(2z+1)^2(w+2\lambda z-1)}\\&-\frac{2\left(2z^2+w-1\right)z^2}{(z-1)(z+1)(2z-1)(2z+1)(w+2\lambda z-1)^2},\end{aligned}\tag{14}$$

where the abbreviation $w:=\sqrt{1-4z^2}$ has been used. We now examine every summand in order to see which contributes to non-negative powers of λ. We rewrite the denominators as

$$\begin{aligned}\frac{1}{w-2\lambda z+1}&=\frac{1}{(1+w)\left(1-\frac{2\lambda z}{1+w}\right)}=\sum_{m\ge0}\frac{(2\lambda z)^m}{(1+w)^{m+1}},\\\frac{1}{w+2\lambda z-1}&=\frac{1}{2\lambda z\left(1-\frac{1-w}{2\lambda z}\right)}=\sum_{m\ge0}\frac{(1-w)^m}{(2\lambda z)^{m+1}},\end{aligned}$$

keeping in mind that

$$\frac{2\lambda z}{1+w}\sim z,\qquad \frac{1-w}{2\lambda z}\sim\frac{2z^2}{2z}=z$$

for $z\to0$ and $\lambda\to1$. This implies that $\underset{\ge}{\Omega}$ deletes the last two summands in (14) since these obviously only contribute negative powers of λ, whereas the first three summands are kept with λ replaced by 1. Thus we have

$$\begin{aligned}\underset{\ge}{\Omega}G_y(\lambda^2,1,z/\lambda)=\sum_{n\ge0}c_nz^n=&\frac{z+2}{(z-1)(z+1)}\\&+\frac{16z^6-24wz^4-40z^4+13wz^2+17z^2-2w-2}{(z-1)(z+1)(2z-1)^2(2z+1)^2(w-2z+1)}\\&-\frac{2\left(2z^2-w-1\right)z^2}{(z-1)(z+1)(2z-1)(2z+1)(w-2z+1)^2}\\=&\frac{(3z-1)\left(z^2+z-1\right)}{(z-1)(z+1)(2z-1)^2}-\frac{2z^4-4z^3-4z^2+z+1}{(z-1)(z+1)\left(1-4z^2\right)^{3/2}}.\end{aligned}$$

We extract the asymptotics of c_n by singularity analysis. The dominant singularities are at $z = \pm 1/2$. The local expansions are

$$\sum_{n\geq 0} c_n z^n = \frac{1}{6(1-2z)^2} + \frac{1}{12\sqrt{2}(1-2z)^{3/2}} + \frac{1}{18(1-2z)} + \frac{241}{144\sqrt{2}(1-2z)^{1/2}} - \frac{58}{27} - \frac{3337(1-2z)^{1/2}}{3456\sqrt{2}} + \frac{158(1-2z)}{81} + \frac{46889(1-2z)^{3/2}}{41472\sqrt{2}} - \frac{490(1-2z)^2}{243} + O\left((1-2z)^{5/2}\right) \tag{15}$$

for $z \to 1/2$ and

$$\sum_{n\geq 0} c_n z^n = \frac{1}{12\sqrt{2}(1+2z)^{3/2}} + \frac{49}{144\sqrt{2}(1+2z)^{1/2}} - \frac{25}{24} + \frac{3191(1+2z)^{1/2}}{3456\sqrt{2}} + \frac{5(1+2z)}{18} - \frac{15127(1+2z)^{3/2}}{41472\sqrt{2}} - \frac{415(1+2z)^2}{864} + O\left((1+2z)^{5/2}\right) \tag{16}$$

for $z \to -1/2$.

Furthermore, the function hidden in the O-terms is analytic in a "camembert-region", whence their contribution to c_n does not exceed $O(n^{-7/2})$ by [6, Theorem 1]. The contributions of the two poles can be added, cf. [7, Theorem VI.5]. Applying (11) to (15) and (16) yields

$$c_n = 2^n \left(\frac{n}{6} + \left(\frac{1}{6\sqrt{2\pi}} + \frac{(-1)^n}{6\sqrt{2\pi}} \right) \sqrt{n} + \frac{2}{9} + \frac{\frac{125}{72\sqrt{2\pi}} + \frac{29(-1)^n}{72\sqrt{2\pi}}}{\sqrt{n}} + \frac{\frac{457}{1728\sqrt{2\pi}} - \frac{887(-1)^n}{1728\sqrt{2\pi}}}{n^{3/2}} + \frac{\frac{7213}{6912\sqrt{2\pi}} - \frac{3059(-1)^n}{6912\sqrt{2\pi}}}{n^{5/2}} + O\left(\frac{1}{n^{7/2}}\right)\right). \tag{17}$$

We now compute the total mass M_n. We have

$$\begin{aligned} 2M_n &= \sum_{k\geq n/2} 2\binom{n}{k} = 2\binom{n}{n/2}[n \text{ even}] + \sum_{k>n/2}\left(\binom{n}{k} + \binom{n}{n-k}\right) \\ &= \binom{n}{n/2}[n \text{ even}] + \sum_{k\geq 0}\binom{n}{k} = \binom{n}{n/2}[n \text{ even}] + 2^n. \end{aligned}$$

We estimate the binomial coefficient by Stirling's formula and obtain

$$M_n = 2^{n-1}\left(1 + \frac{1+(-1)^n}{2\sqrt{2\pi}}\left(\frac{2}{n^{1/2}} - \frac{1}{2n^{3/2}} + \frac{1}{16n^{5/2}} + \frac{5}{64n^{7/2}} + O\left(\frac{1}{n^{9/2}}\right)\right)\right). \tag{18}$$

Dividing c_n by M_n yields (12).

For proving (13), the operator $\underset{\leq}{\Omega}$ has to be applied, which amounts to removing the second and the third summand in (14). The remaining calculation until (17) is very similar, the only difference being that every square root is replaced by its negative. On division by M_n as estimated in (18), however, the term of order $\sqrt{n}$ does not cancel, and this yields (13). □

6. Limit Distribution

In the previous sections, we studied b_{kn}, i.e., we considered the length n and the weight k of the binary expansion as parameters and studied the (average) weight of the corresponding NAFs.

In this section, however, we only consider n as a parameter, and we study the two random variables $H(\mathsf{Binary}(X_n))$ and $H(\mathsf{NAF}(X_n))$, where X_n is a random nonnegative integer less than 2^n, $\mathsf{Binary}(m)$ and $\mathsf{NAF}(m)$ denote the binary expansion and the NAF of m, respectively, and $H(\,\cdot\,)$ denotes the Hamming weight of an expansion.

We are interested in the limiting distribution of the random vector

$$\mathbf{V}_n := (H(\mathsf{Binary}(X_n)), H(\mathsf{NAF}(X_n)))$$

after appropriate rescaling. We use boldface letters for vectors, the components of a vector $\mathbf{x}$ are (x_1, x_2), for instance. Inequalities for vectors have to be taken component-wise.

Theorem 4. *With the notations above, we have*

$$\begin{aligned}
\mathbb{E}(H(\mathsf{Binary}(X_n))) &= \frac{n}{2},\\
\mathbb{E}(H(\mathsf{NAF}(X_n))) &= \frac{n}{3} + \frac{4}{9} + O(2^{-n}),\\
\operatorname{Var}(H(\mathsf{Binary}(X_n))) &= \frac{n}{4},\\
\operatorname{Var}(H(\mathsf{NAF}(X_n))) &= \frac{2n}{27} + \frac{14}{81} + O(n2^{-n}),\\
\operatorname{Cov}(H(\mathsf{Binary}(X_n)), H(\mathsf{NAF}(X_n))) &= \frac{2}{3} + O(n2^{-n}).
\end{aligned}$$

The random vector $\mathbf{V}_n$ is asymptotically normal, i.e.

$$\mathbb{P}\left(\frac{\mathbf{V}_n - \binom{1/2}{1/3}n}{\sqrt{n}} \le \mathbf{x}\right) = \frac{1}{54}\Phi(2x_1)\Phi\left(\frac{3\sqrt{3}}{\sqrt{2}}x_2\right) + O\left(\frac{1}{\sqrt{n}}\right), \tag{19}$$

where

$$\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}\,dt$$

is the distribution function of the standard normal distribution.

This means that although $H(\mathsf{Binary}(X_n))$ and $H(\mathsf{NAF}(X_n))$ are correlated, they are asymptotically independent. Their limiting distribution is the product of two normal distributions.

Proof of Theorem 4. The joint probability $\mathbb{P}(\mathbf{V}_n = (k,\ell))$ is simply $a_{k\ell n}/2^n$ in the terminology of Section 2, thus the probability generating function can be computed as

$$\begin{aligned} P(x,y,z) &= \sum_{k,\ell,n\geq 0} \mathbb{P}(\mathbf{V}_n = (k,\ell))x^k y^\ell z^n \\ &= \sum_{k,\ell,n\geq 0} a_{k,\ell,n} x^k y^\ell \left(\frac{z}{2}\right)^n = G(x,y,z/2) \\ &= \frac{2\left(x^2y^2z^2 - x^2yz^2 - xyz^2 - 2xz + 2xyz + 4\right)}{x^2yz^3 + xyz^3 + 2xz^2 - 4xyz^2 - 4xz - 4z + 8}. \end{aligned}$$

The denominator of $P(1,1,z)$ factors as $2(2-z)(1-z)(2+z)$, thus there are analytic functions $\rho_j(x,y)$, $j \in \{1,2,3\}$, in a neighbourhood of $(x,y) = (1,1)$ such that the denominator of $P(x,y,z)$ exactly vanishes for $z = \rho_j$, $j \in \{1,2,3\}$, and we have

$$\rho_1(1,1) = 1, \qquad \rho_2(1,1) = 2, \qquad \rho_3(1,1) = 3.$$

The moment generating function of $\mathbf{V}_n$ can be obtained by extracting the coefficient of z^n in $P(e^{s_1}, e^{s_2}, z)$ and has the form

$$\mathbb{E}(e^{\langle \mathbf{V}_n, \mathbf{s}\rangle}) = \sum_{k,\ell\geq 0} \mathbb{P}(\mathbf{V}_n = (k,\ell))e^{ks_1+\ell s_2} = e^{u(\mathbf{s})n+v(\mathbf{s})}(1+O(\kappa_n^{-1}))$$

with

$$\begin{aligned} u(s_1,s_2) &= -\log\rho_1, \\ v(s_1,s_2) &= \log\left(-\frac{2\left(-e^{s_1+s_2}\rho_1^2 - e^{2s_1+s_2}\rho_1^2 + e^{2s_1+2s_2}\rho_1^2 - 2e^{s_1}\rho_1 + 2e^{s_1+s_2}\rho_1 + 4\right)}{\rho_1\left(3e^{s_1+s_2}\rho_1^2 + 3e^{2s_1+s_2}\rho_1^2 + 4e^{s_1}\rho_1 - 8e^{s_1+s_2}\rho_1 - 4e^{s_1} - 4\right)}\right), \\ \kappa_n &= 2^{n(1-\epsilon)}, \end{aligned}$$

where $\rho_1 = \rho_1(e^{s_1}, e^{s_2})$ for s_1, s_2 in a neighbourhood of the origin and $\varepsilon > 0$ with $\min\{|\rho_2(e^{s_1}, e^{s_2})|, |\rho_2(e^{s_1}, e^{s_2})|\} \geq 2^{1-\varepsilon}$.

Differentiating $e^{u(\mathbf{s})n+v(\mathbf{s})}$ and setting $(s_1,s_2) = (0,0)$ yields (up to a term $O(2^{-n})$) the means

$$\mathbb{E}(\mathbf{V}_n)^t = \left(\frac{n}{2}, \frac{n}{3} + \frac{4}{9}\right)^t + O(2^{-n})$$

and the matrix of second moments

$$\mathbb{E}(\mathbf{V}_n\mathbf{V}_n^t) = \begin{pmatrix} \frac{n^2}{4} + \frac{n}{4} & \frac{n^2}{6} + \frac{2n}{9} + \frac{2}{3} \\ \frac{n^2}{6} + \frac{2n}{9} + \frac{2}{3} & \frac{n^2}{9} + \frac{10n}{27} + \frac{10}{27} \end{pmatrix} + O(n2^{-n}).$$

Thus the variance-covariance matrix equals

$$\mathbb{E}(\mathbf{V}_n\mathbf{V}_n^t) - \mathbb{E}(\mathbf{V}_n)\mathbb{E}(\mathbf{V}_n)^t = \begin{pmatrix} \frac{n}{4} & \frac{2}{3} \\ \frac{2}{3} & \frac{2n}{27} + \frac{14}{81} \end{pmatrix} + O(n2^{-n}).$$

By a two-dimensional analogue [10] of Hwang's quasi-power theorem [13], we obtain the central limit law (19). □

References

1. G. E. Andrews, P. Paule, and A. Riese, *MacMahon's partition analysis: the Omega package*, European J. Combin. **22** (2001), 887–904.
2. S. Arno and F. S. Wheeler, *Signed digit representations of minimal hamming weight*, IEEE Trans. Comp. **42** (1993), 1007–1010.
3. E. A. Bender, *Central and local limit theorems applied to asymptotic enumeration*, J. Combinatorial Theory Ser. A **15** (1973), 91–111.
4. E. A. Bender and L. B. Richmond, *Central and local limit theorems applied to asymptotic enumeration. II. Multivariate generating functions*, J. Combin. Theory Ser. A **34** (1983), 255–265.
5. M. Drmota, *Asymptotic distributions and a multivariate Darboux method in enumeration problems*, J. Combin. Theory Ser. A **67** (1994), 169–184.
6. Ph. Flajolet and A. Odlyzko, *Singularity analysis of generating functions*, SIAM J. Discrete Math. **3** (1990), 216–240.
7. Ph. Flajolet and R. Sedgewick, *Analytic combinatorics*, in preparation, preprint available at `http://algo.inria.fr/flajolet/Publications/`.
8. P. J. Grabner, C. Heuberger, and H. Prodinger, *Subblock occurrences in signed digit representations*, Glasg. Math. J. **45** (2003), 427–440.
9. P. J. Grabner, C. Heuberger, H. Prodinger, and J. Thuswaldner, *Analysis of linear combination algorithms in cryptography*, ACM Trans. Algorithms **1** (2005), 123–142.
10. C. Heuberger, *Hwang's quasi-power-theorem in dimension two*, in preparation.
11. C. Heuberger and H. Prodinger, *On minimal expansions in redundant number systems: Algorithms and quantitative analysis*, Computing **66** (2001), 377–393.
12. ———, *Analysis of alternative digit sets for nonadjacent representations*, Monatsh. Math. **147** (2006), 219–248.
13. H.-K. Hwang, *On convergence rates in the central limit theorems for combinatorial structures*, European J. Combin. **19** (1998), 329–343.
14. P. A. MacMahon, *Combinatory analysis*, Cambridge University Press, Cambridge, 1915–1916, (Reprinted: Chelsea, New York, 1960).
15. F. Morain and J. Olivos, *Speeding up the computations on an elliptic curve using addition-subtraction chains*, RAIRO Inform. Théor. Appl. **24** (1990), 531–543.
16. G. W. Reitwiesner, *Binary arithmetic*, Advances in computers, vol. 1, Academic Press, New York, 1960, pp. 231–308.
17. J. M. Thuswaldner, *Summatory functions of digital sums occurring in cryptography*, Period. Math. Hungar. **38** (1999), 111–130.
18. J. H. Van Lint, *Introduction to coding theory*, 2nd ed., Graduate Texts in Mathematics, vol. 86, Springer, 1992.

Institut für Mathematik B, Technische Universität Graz, Austria
E-mail address: `clemens.heuberger@tugraz.at`

Department of Mathematics, University of Stellenbosch, South Africa
E-mail address: `hproding@sun.ac.za`