PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 71, Number 1, August 1978

THE BINARY DIGITS OF A POWER

KENNETH B. STOLARSKY

ABSTRACT. Let $B(m)$ denote the number of ones in the binary expansion of the integer $m > 1$ and let $r_h(m) = B(m^h)/B(m)$ where h is a positive integer. The maximal order of magnitude of $r_h(m)$ is $c(h)(\log m)^{(h-1)/h}$ where $c(h) > 0$ depends only on h. That this is best possible follows from the Bose-Chowla theorem. The minimal order of magnitude of $r_2(m)$ is at most $c(\log\log m)^2/\log m$ where $c > 0$ is an absolute constant.

1. Introduction. It seems difficult to say anything about the distribution of ones in the binary expansion of a surd such as $\sqrt{2}$ (but see P. Erdös [**6**, p. 215, Theorem 2] and J. Samborski [**11**]). We study the easier yet somehow related problem of digital distribution in powers of integers. Let $B(m)$ denote the number of ones in the binary expansion of m. It is known that $B(m)$ and $h^{-1}B(m^h)$, for a fixed integer h, have the same average order of magnitude, namely $(\log m)/(2\log 2)$. In fact, stronger results for base 10 are proved in H. Davenport and P. Erdös [**3**]; see also A. Besicovitch [**1**]. Here we investigate the *pointwise* relationship of these quantities.

Throughout, logarithms are to the base 2 unless otherwise specified.

DEFINITION. Let

$$r_h(m) = B(m^h)/B(m). \tag{1.1}$$

THEOREM 1. *Let m and h be positive integers greater than* 1. *Then*

$$r_h(m) \leqslant 2(h\log m)^{1-1/h}, \tag{1.2}$$

and this is best possible in that there is a constant $c(h) > 0$, depending only on h, such that

$$r_h(m) > c(h)(\log m)^{1-1/h} \tag{1.3}$$

infinitely often.

THEOREM 2. *Let m be a positive integer greater than* 1. *Then (trivial estimate) we have*

$$r_2(m) \geqslant \{[\log m] + 1\}^{-1}.$$

On the other hand, there are infinitely many integers m such that

$$r_2(m) \leqslant 4(\log\log m)^2/\log m. \tag{1.4}$$

Received by the editors January 31, 1978.
AMS (MOS) subject classifications (1970). Primary 10A35, 10A40, 10L99.

It is well known that

$$B(ab) \leqslant B(a)B(b) \tag{1.5}$$

for positive integers a and b, and examples such as

$$(111)(100100) = (111\ 111)$$

show it is best possible. However, (1.5) with $a = b = m$ is usually far weaker than (1.2) with $h = 2$, since $(\log m)^{1/2}$ is usually much less than $B(m)$. For very precise statements of the value distribution of $B(m)$ see I. Kátai and J. Mogyoródi [8].

An extensive bibliography for the function $B(n)$, together with a historical survey, is given in [12]; see also [13], [14].

2. Proof of Theorem 1. Let $x = B(m)$ and

$$r_h(m) = B(m^h)/B(m). \tag{2.1}$$

Then by (1.5) and the trivial estimate

$$B(m) \leqslant [\log m] + 1, \tag{2.2}$$

where $[u]$ denotes the greatest integer in u, we have

$$r_h(m) \leqslant x^{-1}\min\{h \log m + 1, x^h\}. \tag{2.3}$$

For $x^h \geqslant h \log m$ we have

$$r_h(m) \leqslant (h \log m)^{1-1/h} + 1. \tag{2.4}$$

Otherwise

$$r_h(m) \leqslant x^{h-1} < (h \log m)^{1-1/h} \tag{2.5}$$

and (1.2) follows.

Our proof of (1.3) uses a notable result of Bose and Chowla.

THEOREM 3 (BOSE-CHOWLA). *Let $h \geqslant 2$ be an integer. Then there are infinitely many integers M for which there exist integers $a_1, \ldots, a_{M+1}$ such that*

$$1 \leqslant a_1 < a_2 < \cdots < a_{M+1} = M^h, \tag{2.6}$$

while every sum of the form

$$a_{j_1} + \cdots + a_{j_h}, \qquad 1 \leqslant j_1 \leqslant \cdots \leqslant j_h \leqslant M + 1 \tag{2.7}$$

is distinct.

PROOF. See either [2] or [7, pp. 81–83].

We shall refer to this property of the a_i as the *distinct sums property*.

Let $k = [\log h!] + 1$. Choose $M \geqslant 3(k + 1)$ and $a_1, \ldots, a_{M+1}$ so that the conclusion of Theorem 3 holds. Let $C(i)$ be the class of all a_j such that

$$a_j \equiv i \bmod(k + 1), \qquad 0 \leqslant i \leqslant k. \tag{2.8}$$

For some i_0, the corresponding $C(i_0)$ has at least

$$[(M + 1)/(k + 1)] = N + 1 \tag{2.9}$$

elements. Subtract i_0 from each element of $C(i_0)$, remove the smallest (which

might be zero), and label the elements of the transformed set as $y_1, \ldots, y_N$ in increasing order. Thus

$$1 \leqslant y_1 < y_2 < \cdots < y_N \leqslant M^h \leqslant \{(N+2)(k+1)\}^h, \tag{2.10}$$

and the y_i evidently have the distinct sums property.

Define m by

$$m = \sum_{i=1}^{N} 2^{y_i}. \tag{2.11}$$

Then

$$m^h = \sum{}' C(h; h_1, \ldots, h_N) 2^{y_1 h_1 + \cdots + y_N h_N} \tag{2.12}$$

where the $C(h; h_1, \ldots, h_N)$ are the usual multinomial coefficients, bounded above by 2^k, and the summation is over all

$$\binom{N+h-1}{N-1}$$

vectors $(h_1, \ldots, h_N)$ satisfying

$$h_1 + \cdots + h_N = h. \tag{2.13}$$

By writing the multinomial coefficients in binary, we obtain

$$C(h; h_1, \ldots, h_N) = \sum_{j=1}^{J} 2^{b(j; h_1, \ldots, h_N)} \tag{2.14}$$

where $J = J(h_1, \ldots, h_N)$, and

$$0 \leqslant b(j; h_1, \ldots, h_N) \leqslant k, \qquad 1 \leqslant j \leqslant J. \tag{2.15}$$

Upon combining (2.12) and (2.14) we obtain

$$m^h = \sum{}' \sum_{j} 2^{y_1 h_1 + \cdots + y_N h_N + b(j; h_1, \ldots, h_N)}. \tag{2.16}$$

To see that the exponents on the right of (2.16) are distinct, examine them modulo $k+1$. Since

$$y_i \equiv 0 \bmod (k+1), \tag{2.17}$$

the equality of two exponents implies that the corresponding $b(j; \cdot)$ terms are congruent modulo $k+1$, and hence, by (2.15), are equal. But then the values of $(h_1, \ldots, h_N)$ must be the same for both exponents by the distinct sums property. Finally, (2.14) shows that the values of j are identical, since the binary expansion of a number is unique. Hence

$$N^{h-1}/h! \leqslant N(N+1)\cdots(N+h-1)/h! N \leqslant B(m^h)/B(m). \tag{2.18}$$

On the other hand, from (2.10) and (2.11), we have

$$\log m \leqslant y_N + 1 \leqslant \{(N+2)(k+1)\}^h + 1 \leqslant 2^{h+1} N^h (k+1)^h. \tag{2.19}$$

Upon raising both sides of (2.19) to the power $(h-1)/h$ and combining with (2.18), the result follows.

3. Proof of Theorem 2. We begin by observing that

$$B(2^a - 2^b) = a - b, \qquad a \geqslant b. \tag{3.1}$$

From this it is easy to deduce that for

$$A > a_1 > a_2 > \cdots > a_q \geqslant 0$$

we have

$$B(2^A - 2^{a_1} - 2^{a_2} - \cdots - 2^{a_q}) = 1 + (A - a_1 - 1) + (a_1 - a_2 - 1) + \cdots + (a_{q-1} - a_q - 1) = A + 1 - a_q - q. \tag{3.2}$$

Now let $q \geqslant 1$, set $a(t) = 2^t$ and

$$S = S_q = \sum_{j=1}^{q} 2^{a(q+1)-a(j)+1}, \tag{3.3}$$

and define

$$m = 2^{a(q+1)} - S. \tag{3.4}$$

Then from (3.2) we have

$$B(m) = 2^{q+1} + 1 - (2^{q+1} - 2^q + 1) - q = 2^q - q. \tag{3.5}$$

Now

$$m^2 = 2^{2a(q+1)} - 2^{a(q+1)+1}S + S^2. \tag{3.6}$$

The first $q - 1$ squared terms from S^2 cancel out the first two terms on the right of (3.6), so

$$m^2 = 2^{a(q+1)+2} + \sum_{i=1}^{Q} 2^{e_i}, \quad Q = q(q-1)/2, \tag{3.7}$$

where each $e_i \geqslant 0$ is an integer. Clearly

$$B(m^2) \leqslant 1 + \left[q(q-1)/2\right]; \tag{3.8}$$

it is easily seen (though not needed here) that equality holds. Since

$$2^q \leqslant \log m \leqslant 2^{q+1}, \tag{3.9}$$

the result follows.

By slightly perturbing the exponents in (3.3), we can create a wider (but still rather "thin") class of integers with small values of $r_2(m)$.

4. Remarks. It seems reasonable to expect that

$$\liminf r_h(m) = 0 \tag{4.1}$$

for every fixed $h \geqslant 2$, but I do not see how to prove this. Set

$$R_h(T) = T^{-1} \sum_{m=1}^{T} r_h(m). \tag{4.2}$$

I conjecture that $R_h(T) \to h'$ as $T \to \infty$, where $1 < h' \leqslant h$, and that

$$R(2^n) \leqslant R(2^{n+1}), \tag{4.3}$$

at least for all sufficiently large n.

References

1. A. S. Besicovitch, *The asymptotic distribution of the numerals in the decimal representation of the squares of the natural numbers*, Math. Z. **39** (1934), 146–156.

2. R. C. Bose and S. Chowla, *Theorems in the additive theory of numbers*, Comm. Math. Helv. **37** (1962/63), 141–147.

3. H. Davenport and P. Erdös, *Note on normal decimals*, Canad. J. Math. **4** (1952), 58–63.

4. H. Delange, *Sur la fonction sommatoire de la fonction "somme des chiffres"*, Enseignement Math. (2) **21** (1975), 31–47.

5. M. P. Drazin and J. S. Griffith, *On the decimal representation of integers*, Proc. Cambridge Philos. Soc. (4) **48** (1952), 555–565.

6. P. Erdös, *On the irrationality of certain series*, Nederl. Akad. Wetensch. Proc. Ser. A. **60** (1957), 212–219.

7. H. Halberstam and K. F. Roth, *Sequences*, vol. I, Clarendon Press, London, 1966.

8. I. Kátai and J. Mogyoródi, *On the distribution of digits*, Publ. Math. Debrecen **15** (1968), 57–68.

9. D. J. Newman and M. Slater, *Binary digit distribution over naturally defined sequences*, Trans. Amer. Math. Soc. **213** (1975), 71–78.

10. I. Shiokawa and S. Uchiyama, *On some properties of the dyadic Champernowne numbers*, Acta Math. Acad. Sci. Hungar. **26** (1975), 9–27.

11. J. R. Samborski, Problem E2667, Amer. Math. Monthly **84** (1977), 567.

12. K. B. Stolarsky, *Power and exponential sums of digital sums related to binomial coefficient parity*, SIAM J. Appl. Math. **32** (1977), 717–730.

13. K. B. Stolarky and J. B. Muskat, *The number of binary digits in multiples of n* (in prep.).

14. K. B. Stolarsky, *Integers whose multiples have anomalous digital frequencies*, Acta Arith. (to appear).

Department of Mathematics, University of Illinois, Urbana, Illinois 61801