数理解析研究所講究録
第 334 巻 1978 年 27-30

A THEOREM ON BINARY DIGITS

UNIVERSITY OF COLORADO WOLFGANG M. SCHMIDT

Let $B(n)$ denote the number of digits 1 in the representation of a natural number n in the binary scale. It is well known that for most n, the number $B(n)$ is about half the total number of digits, so that $B(n)$ is roughly equal to $\frac{1}{2}\nu$, where $\nu = \nu(n) = \log_2 n$, with $\log_2$ denoting the logarithm to the base 2. In fact it follows from the Central Limit Theorem of probability theory that the numbers n with

$$\frac{B(n) - \frac{1}{2}\nu}{\sqrt{\nu}} \leqq \xi$$

have density

$$\varphi(\xi) = \sqrt{\frac{2}{\pi}} \int_{-\infty}^{\xi} e^{-2t^2} dt .$$

Here we say that a set S of natural numbers has <u>density</u> φ if the number $S(x)$ of elements $n \in S$, $n \leqq x$ satisfies the asymptotic relation $S(x) \sim \varphi x$ as $x \to \infty$.

Stolarsky was the first to compare $B(n)$ and $B(kn)$ where $k > 1$ is a fixed odd integer. He called a number k-<u>sturdy</u> if $B(n) \leqq B(kn)$, and simply sturdy if it is k-sturdy for every k. Stolarsky proved that the 3-sturdy numbers have density $\frac{1}{2}$. Here we are going to sketch a proof that for any odd $k > 1$, the k-sturdy numbers have density $\frac{1}{2}$. The interest in the proof lies in the fact that it uses Markov Chains. The main result is as follows.

THEOREM. Let $k_1, \ldots, k_s$ be distinct odd integers. The matrix $M = (\mu_{ij})$ with entries $\mu_{ij} = k_i^{-1} k_j^{-1} (\gcd(k_i, k_j))^2$ $(1 \leq i, j \leq s)$ has an inverse $Q = (q_{ij})$, and the quadratic form $Q(\underline{t}) = Q(t_1, \ldots, t_s) = \sum_{i,j=1}^{s} q_{ij} t_i t_j$ is positive definite. Hence

$$\varphi(\xi_1, \ldots, \xi_s) = (2/\pi)^{s/2} (\det M)^{-1/2} \int_{-\infty}^{\xi_1} \cdots \int_{-\infty}^{\xi_s} dt_1 \ldots dt_s$$

is well defined for $(\xi_1, \ldots, \xi_s) \in \mathbb{R}^s$. The main assertion now is that the natural numbers n having simultaneously

$$\frac{B(k_i n) - \frac{1}{2}\nu}{\sqrt{\nu}} \leq \xi_i \qquad (i = 1, \ldots, s)$$

have density $\varphi(\xi_1, \ldots, \xi_s)$.

A corollary is that for distinct odd integers k_1, k_2, the numbers n with $B(k_1 n) - B(k_2 n) \leq \eta \sqrt{\nu}$ have density

$$\psi(\eta) = (\pi(1-\mu))^{-1/2} \int_{-\infty}^{\eta} e^{-t^2/(1-\mu)} dt$$

with $\mu = k_1^{-1} k_2^{-1} (\gcd(k_1, k_2))^2$. In particular, numbers n with $B(k_1 n) \leq B(k_2 n)$ have density $\psi(0) = \frac{1}{2}$. Another corollary is that the sturdy numbers have density 0.

Let Ω be the ring of 2-adic integers

$$\mathcal{N} = a_1 + 2a_2 + 2^2 a_3 + \dots \quad ,$$

with each "digit" a_t either 0 or 1. The triple $(\Omega, \mathcal{F}, \underline{P})$, where $\underline{P}$ is the Haar measure on Ω, and $\mathcal{F}$ consists of $\underline{P}$-measurable subsets of Ω, is a probability triple. Write $B_h(\mathcal{N})$ for the number of digits 1 among $a_1, \dots, a_h$. Given distinct odd $k_1, \dots, k_s$, put

$S_h^{(i)} = B_h(k_i \mathcal{N}) - \frac{1}{2} h \quad (i = 1, \dots, s)$, and write

$$\underline{\underline{R}}_h(\xi_1, \dots, \xi_s) = \underline{P}\left\{ h^{-1/2} S_h^{(i)} \le \xi_i \quad (i = 1, \dots, s) \right\}.$$

The theorem can be shown to be a consequence of the

PROPOSITION. $\lim\limits_{h \to \infty} \underline{\underline{R}}_h(\xi_1, \dots, \xi_s) = \varphi(\xi_1, \dots, \xi_s)$.

Write $k_i \mathcal{N} = b_1^{(i)} + 2 b_2^{(i)} + \dots$, and put $y_t^{(i)} = \begin{cases} \frac{1}{2} & \text{if } b_t^{(i)} = 1 \\ -\frac{1}{2} & \text{if } b_t^{(i)} = 0. \end{cases}$

Then $S_h^{(i)} = y_1^{(i)} + \dots + y_h^{(i)}$. For given i, the random variables $y_1^{(i)}, y_2^{(i)}, \dots$ are independent. But the random vectors $\underline{\underline{y}}_1, \underline{\underline{y}}_2, \dots$, where $\underline{\underline{y}}_t = (y_t^{(1)}, \dots, y_t^{(s)})$, are *not* independent. Hence we cannot use the Central Limit Theorem for sums of independent random variables.

Call a vector $\underline{\underline{x}} = (x_1, \dots, x_s)$ *admissible*, if there is a real number α in $0 \le \alpha < 2$ with $x_i = [k_i \alpha] \quad (i = 1, \dots, s)$, where $[\ ]$ denotes the integer part. There are finitely many admissible vectors. The vector $\underline{\underline{0}} = (0, \dots, 0)$ is admissible, and if $\underline{\underline{x}}$ is admissible, then both $\underline{\underline{x}}^0 = ([x_1/2], \dots, [x_s/2])$ and $\underline{\underline{x}}^1 = ([x_1/2] + k_1, \dots, [x_s/2] + k_s)$ are admissible.

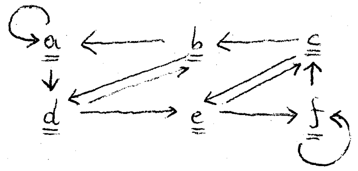
Given $\mathcal{N}$ as above, put $\mathcal{N}_t = a_1 + 2a_2 + \dots + 2^{t-1} a_t$. Put $\underline{\underline{x}}_0 = \underline{\underline{0}}$

and $\underline{\underline{x}}_t = \underline{\underline{x}}_t(n) = \left([2^{-t+1}k_1 n_t], \ldots, [2^{-t+1}k_s n_t]\right)$ $(t=1,2,\ldots)$. Then $\underline{\underline{x}}_0, \underline{\underline{x}}_1, \ldots$ are (vector valued) random variables. Clearly $\underline{\underline{x}}_t(n)$ is always admissible, and conversely if $\underline{\underline{x}}$ is admissible, then there is an n and a t with $\underline{\underline{x}}_t(n) = \underline{\underline{x}}$. It is now easy to prove the

LEMMA. *The random variables $\underline{\underline{x}}_0, \underline{\underline{x}}_1, \ldots$ form a Markov Chain.* The transition probabilities are given by the rule that for given $\underline{\underline{x}}_t$, we have $\underline{\underline{x}}_{t+1}$ either equal to $\underline{\underline{x}}_t^0$, or to $\underline{\underline{x}}_t^1$, each with probability $\frac{1}{2}$.

We now observe that the random variable $\underline{\underline{y}}_t$ is a "functional" of $\underline{\underline{x}}_t$: We have $y_t^{(i)} = f^{(i)}(\underline{\underline{x}}_t)$, where $f^{(i)}(\underline{\underline{x}}) = \frac{1}{2}$ if x_i is odd, $f^{(i)}(\underline{\underline{x}}) = -\frac{1}{2}$ if x_i is even. Hence the machinery of Markov Chains can be used to complete the proof of our theorem.

In the special case when $s=2$, $k_1=1$, $k_2=3$, there are 6 admissible vectors: $\underline{\underline{a}}=(0,0)$, $\underline{\underline{b}}=(0,1)$, $\underline{\underline{c}}=(0,2)$, $\underline{\underline{d}}=(1,3)$, $\underline{\underline{e}}=(1,4)$, $\underline{\underline{f}}=(1,5)$. The transition probabilities are given by the following diagram, where each arrow represents a probability of $\frac{1}{2}$:



References

[Hung. (To appear)

W. M. Schmidt. The Joint Distribution of the digits of certain integer s-tuples. Acta Math.

K.B. Stolarsky. Integers whose multiples have anomalous digital frequencies. Acta Arith. (To appear).