Discr. Math. 145 (1995), 307-313

An Effective Additive Basis for the Integers

Mihail N. Kolountzakis
Department of Mathematics, Stanford University, Stanford, CA 94305
E-mail: kolount@cauchy.stanford.edu

May 1993; revised August 1993

Abstract

We give an algorithm for the enumeration of a set E of nonnegative integers with the property that each nonnegative integer x can be written as a sum of two elements of E in at least $C_1 \log x$ and at most $C_2 \log x$ ways, where C_1, C_2 are positive constants. Such a set is called a basis and its existence has been established by Erdős. Our algorithm takes time polynomial in n to enumerate all elements of E not greater than n. We accomplish this by derandomizing a probabilistic proof which is slightly different than that given by Erdős.

Mathematics Subject Classification: 11Y16, 68Q99

1 Introduction

A set E of nonnegative integers is called a basis if every nonnegative integer can be written as a sum of two elements of E. We write $r(x) = r_E(x)$ for the number of representations of x as $a + b$, with $a, b \in E$ and $a \leq b$. In what follows C denotes an arbitrary positive constant, not necessarily the same in all its occurences, and $\mathbf{N} = \{1, 2, 3, \ldots\}$ denotes the set of all positive integers. The mean value of a random variable X is denoted by $\mathbf{E}X$.

Erdős [2, 3] has proved that there is a basis E such that

$$C \log x \leq r(x) \leq C \log x \tag{1}$$

for all positive integers x (see also [1, p. 106] and [4, Ch. 3]). The most widely known proof (in [1, 3, 4]) is probabilistic. It is proved that if we let $x \in E$ with a certain probability p_x, independently for all x, then the random set E is an asymptotic basis (that is (1) is true eventually) with probability 1. Since the probability space used is infinite, the question of whether such a basis exists which is also computable is not addressed by this proof.

The original [2] proof though, which has been stated using counting arguments and not probability, uses an existential argument on a finite interval at a time and can thus be readily turned into a construction by examining all possible intersections of E with the interval. But the algorithm which we get this way takes time exponential in n to decide whether n is in E or not.

In this paper, we give an algorithm which produces the elements of E one by one and in increasing order, and which takes time polynomial in n in order to produce all the elements of E not greater than n. We use the so called method of conditional probabilities [1, p. 223] in order to "derandomize" a modified proof. The method is not directly applicable to Erdős's probabilistic proof. We will only care for (1) to hold for x large enough, since, then, with the addition of a finite number of elements to the set E we can have it hold true for all positive x.

In Section 2 we give a probabilistic proof of the existence of a basis with certain properties. In Section 3 we apply the method of conditional probabilities to derandomize the proof and arrive to our algorithm.

2 Probabilistic Proof of Existence

We define the modified representation function $r'(x) = r'_E(x)$ as the number of representations of the nonegative integer x as a sum $a + b$, with $a, b \in E$, $g(x) \leq a \leq b$, where $g(x) = (x \log x)^{1/2}$. (This is our main difference from Erdős's proof. By doing this modification we have achieved that the presence or absence of a certain number n in our set E affects $r'(x)$ for only a finite number of nonnegative integers x.)

Theorem 1 *There are positive constants c_1, c_2, c_3, with $c_2 < c_3$, and a set E of positive integers such that*

$$c_2 \log x \leq r'(x) \leq c_3 \log x$$

and

$$|E \cap [x - g(x), x]| \leq c_1 \log x$$

for all large enough $x \in \mathbf{N}$.

Proof: In what follows x is assumed to be sufficiently large. We define the random set E by letting

$$\Pr(x \in E) = p_x = K \cdot \left(\frac{\log x}{x}\right)^{1/2}$$

independently for all $x \in \mathbf{N}$, where K is a positive constant that will be specified later. We are going to show that with positive probability (in fact almost surely but we do not need this here) the random set E satisfies Theorem 1. Let

$$\mu = \mathbf{E}r'(x) = \sum_{t=g(x)}^{x/2} p_t p_{x-t}.$$

Define also

$$s(x) = |E \cap [x - g(x), x]|$$

and

$$\nu = \mathbf{E}s(x) = \sum_{t=x-g(x)}^{x} p_t.$$

First we estimate μ and ν for large x. We have

$$\begin{aligned}\mu &\geq \sum_{t=x/\log x}^{x/2} p_t p_{x-t} \\ &\geq K^2 \log\frac{x}{\log x} \sum_{t=x/\log x}^{x/2} (t(x-t))^{-1/2} \\ &= (1+o(1))IK^2 \log x,\end{aligned}$$

where $I = \int_0^{1/2} (s(1-s))^{-1/2} ds$, and

$$\begin{aligned}\mu &\leq \sum_{1}^{x/2} p_t p_{x-t} \\ &\leq K^2 \log\frac{x}{2} \sum_{1}^{x/2} (t(x-t))^{-1/2} \\ &= (1+o(1))IK^2 \log x,\end{aligned}$$

which proves $\mu = (1+o(1))IK^2 \log x$.

For ν we have

$$Kg(x)\left(\frac{\log(x-g(x))}{x}\right)^{1/2} \leq \nu \leq Kg(x)\left(\frac{\log x}{x-g(x)}\right)^{1/2},$$

which implies

$$\nu = (1+o(1))K\log x.$$

We define the "bad" events

$$\begin{aligned}A_x &= \{|r'(x)-\mu| > \epsilon\mu\} \\ B_x &= \{s(x)-\nu > \epsilon\nu\}\end{aligned}$$

for a positive constant ϵ. To bound their probabilities we need the following Lemma [1, p. 239].

Lemma 1 *If $Y = X_1 + \cdots + X_k$, and the X_j are independent indicator random variables, then for all $\epsilon > 0$*

$$\Pr(|Y - \mathbf{E}Y| > \epsilon \mathbf{E}Y) \leq 2e^{-c_\epsilon \mathbf{E}Y},$$

where $c_\epsilon > 0$ is a function of ϵ alone.

Since both $r'(x)$ and $s(x)$ are sums of independent indicator random variables we can use Lemma 1 to get

$$\Pr(A_x) \leq 2e^{-c_\epsilon \mu} \leq 2e^{-\frac{1}{2}c_\epsilon IK^2 \log x} = 2x^{-\alpha}$$

and

$$\Pr(B_x) \leq 2e^{-c_\epsilon \nu} \leq 2e^{-\frac{1}{2}c_\epsilon K \log x} = 2x^{-\beta}$$

where $\alpha = \frac{1}{2}c_\epsilon IK^2$ and $\beta = \frac{1}{2}c_\epsilon K$. We now let $\epsilon = 1/2$ and choose K large enough to make both α and β greater than 1.

Then

$$\sum_{x=1}^{\infty} \Pr(A_x) + \Pr(B_x) < \infty$$

which implies the existence of $n_0 \in \mathbf{N}$ such that, with positive probability, none of the events A_x and B_x, $x \geq n_0$, holds. In particular there exists a set E for which $\mu/2 \leq r'(x) \leq 3\mu/2$ and $s(x) \leq 3\nu/2$, for all $x \geq n_0$. This implies the conclusion of Theorem 1 with $c_1 = \frac{1}{2}K$, $c_2 = \frac{1}{2}IK^2$ and $c_3 = \frac{3}{2}IK^2$. **QED**

Observe that $r'(x) \leq r(x) \leq r'(x) + s(x)$. We deduce that for the set E of Theorem 1 we have

$$c_2 \log x \leq r(x) \leq (c_1 + c_3) \log x$$

so that (1) is true for E.

3 Derandomization of the Proof

We keep the notation of the previous section. We showed that for some $n_0 \in \mathbf{N}$ the complement of the "bad" event $B = \bigcup_{x \geq n_0}(A_x \cup B_x)$ has positive probability, by establishing the inequality

$$\sum_{x \geq n_0} \Pr(A_x) + \Pr(B_x) < 1.$$

This implies the existence of a point E in our probability space $\{0,1\}^{\mathbf{N}}$ which is not in B (there is a natural identification between points in the probability space and subsets of $\mathbf{N}$). In this section we are going to show how to construct efficiently such a point E. We give an algorithm which at the n-th step outputs 0 or 1 to denote the absence or presence of n in our set E.

Denote by $\chi \in \{0,1\}^{\mathbf{N}}$ a generic element in our space and by $R(a_1, \ldots, a_k)$ the event $\chi_1 = a_1, \ldots, \chi_k = a_k$, where $a_1, \ldots, a_k \in \{0,1\}$. It is obvious that for any event $D \subseteq \{0,1\}^{\mathbf{N}}$

$$\begin{aligned} &\Pr(D \mid R(a_1, \ldots, a_{n-1})) = \\ &\quad p_n \Pr(D \mid R(a_1, \ldots, a_{n-1}, 1)) + (1 - p_n)\Pr(D \mid R(a_1, \ldots, a_{n-1}, 0)). \end{aligned} \tag{2}$$

We are going to define the sequence $a_n \in \{0,1\}$ so that the function

$$b_n = b_n(a_1, \ldots, a_n) = \sum_{x \geq n_0} \Pr(A_x \mid R(a_1, \ldots, a_n)) + \Pr(B_x \mid R(a_1, \ldots, a_n))$$

is non-increasing in n. (Notice that the function $\Pr(A_x \mid R(a_1, \ldots, a_n))$ is constant in n when $n > x$, and is equal to either 0 or 1. The same is true for the events B_x.) Since $b_0 = \sum_{x \geq n_0} \Pr(A_x) + \Pr(B_x) < 1$, the monotonicity of b_n implies that

$$\sum_{x \geq n_0} \Pr(A_x \mid R(a_1, \ldots, a_n, \ldots)) + \Pr(B_x \mid R(a_1, \ldots, a_n, \ldots)) < 1.$$

The probabilities above are either 0 or 1, so they are all 0, and the point $E = (a_1, \ldots, a_n, \ldots)$ is not in B.

So all that remains to be done is to ensure that b_n does not increase. Adding up (2) we get

$$b_{n-1}(a_1,\ldots,a_{n-1}) = p_n b_n(a_1,\ldots,a_{n-1},1) + (1-p_n)b_n(a_1,\ldots,a_{n-1},0),$$

which implies that at least one of $b_n(a_1,\ldots,a_{n-1},1)$, $b_n(a_1,\ldots,a_{n-1},0)$ is not greater than $b_{n-1}(a_1,\ldots,a_{n-1})$. We let $a_n = 1$ if the first number is smaller than the latter, otherwise we let $a_n = 0$.

Notice that

$$\begin{aligned}\Delta &= b_n(a_1,\ldots,a_{n-1},1) - b_n(a_1,\ldots,a_{n-1},0)\\ &= \sum_{x=n}^{G(n)} \Pr(A_x \mid R(a_1,\ldots,a_{n-1},1)) - \Pr(A_x \mid R(a_1,\ldots,a_{n-1},0)) +\\ &\quad +\Pr(B_x \mid R(a_1,\ldots,a_{n-1},1)) - \Pr(B_x \mid R(a_1,\ldots,a_{n-1},0)),\end{aligned}$$

where $G(n) = (1+o(1))n^2/\log n$ is the greatest integer k such that $g(k) \leq n$. This is so because the events A_x and B_x, with $x > G(n)$ are independent of $\chi_1,\ldots,\chi_n$ and their probabilities cancel out in the difference above. We have to decide in time polynomial in n whether $\Delta \geq 0$. This is indeed possible since the expression for Δ has $(4+o(1))n^2/\log n$ terms, each of which can be computed in polynomial time as the following Lemma claims.

Lemma 2 *Let $X_k = \xi_1 + \cdots + \xi_k$ be a sum of k independent indicator random variables with $\Pr(\xi_j = 1) = p_j$, $j = 1,\ldots,k$. Then the distribution of X_k can be computed in time polynomial in k.*

Proof: The distribution of X_k is a vector of length $k+1$, where the j-th coordinate in the vector, $j = 0,\ldots,k$, is equal to $\Pr(X_k = j)$. To compute the distribution of X_k from that of X_{k-1} we use the obvious formulas

$$\Pr(X_k = j) = p_k \Pr(X_{k-1} = j-1) + (1-p_k)\Pr(X_{k-1} = j), \quad \text{for } j = 1,\ldots,k-1,$$

$\Pr(X_k = 0) = (1-p_k)\Pr(X_{k-1} = 0)$ and $\Pr(X_k = k) = p_k \Pr(X_{k-1} = k-1)$. It is obvious now that the computation of the distribution of X_k can be carried out in time polynomial in k. (Here we are really assuming that arithmetic operations on the numbers p_j can be done in time polynomial in k. See the Remarks at the end of the section for a justification of this assumption.) **QED**

Thus all probabilities of the form $\Pr(\alpha < X_k < \beta)$ can be efficiently computed. Observe that having fixed $\chi_1 = a_1,\ldots,\chi_n = a_n$ we have

$$\begin{aligned}r'(x) &= \sum_{t=g(x)}^{x/2} \chi_t \chi_{x-t}\\ &= \sum_{g(x)}^{n} a_t \chi_{x-t} + \sum_{n+1}^{x/2} \chi_t \chi_{x-t}\end{aligned}$$

for $x - g(x) > n$, otherwise $r'(x)$ has already been completely determined by the assigned values of $\chi_1,\ldots,\chi_n$. This means that $r'(x)$ is a sum of independent indicator random variables and so is $s(x)$. Thus the probabilities of A_x and B_x conditioned on $R(a_1,\ldots,a_{n-1},1)$ and $R(a_1,\ldots,a_{n-1},0)$ can be efficiently computed and $\Delta \geq 0$ can be decided in polynomial time, as we had to show.

Remarks:

1. Our definition of the probabilities $p_x = K(\log x/x)^{1/2}$ has to be modified so that the numbers p_x can be represented with a number of digits polynomial in x and can also be computed in polynomial time, given x. One such modification is to use the probabilities $q_x = K2^{-\lfloor L/2 \rfloor}S$, where $L = \lfloor \log_2 x \rfloor$ and $S = \lfloor \sqrt{L} \rfloor$. The number S can for example be computed in time polynomial in $\log L$ (and in particular in x) using a simple binary search of the interval $[0, L]$. Since $p_x < Cq_x < Cp_x$ one can easily prove asymptotic estimates of the form $CIK^2 < \mu < CIK^2$ and $CK \log x < \nu < CK \log x$, which is all our existential proof needs.

2. Ignoring polylogarithmic factors, the time our algorithm needs to decide whether $n \in E$, having already found the set E up to $n-1$, is $O(n^6)$. This is so since the distribution of X_k in Lemma 2 can be computed in time $O(k^2)$. So the computation of any probability of the form $\Pr(\alpha < X_k < \beta)$ can be computed in time $O(k^2)$. For the computation of Δ we need to evaluate $O(n^2)$ such probabilities with $k = O(n^2)$, thus the total time is $O(n^6)$.

References

[1] N. Alon and J. H. Spencer, *The Probabilistic Method*, Wiley-Interscience Series in Discrete Math. and Optimization, 1992.

[2] P. Erdős, *On a Problem of Sidon in Additive Number Theory*, Acta Sci. Math. (Szeged), 15 (1953-54), 255-259.

[3] P. Erdős, *Problems and Results in Additive Number Theory*, Colloque sur la Théorie des Nombres (CBRM, Bruxelles), 127-137.

[4] H. Halberstam and K. F. Roth, *Sequences*, 2nd ed., Springer-Verlag, Berlin, 1983.