INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 6 (2006), #A25

SOME OBSERVATIONS ON SUBSET SUM REPRESENTATIONS

Donald Mills

Department of Mathematics, Rose-Hulman Institute of Technology, Terre Haute, IN 47803-3999

mills@rose-hulman.edu

Received: 9/22/05, Revised: 5/31/06, Accepted: 9/24/06, Published: 10/06/06

Abstract

Moulton and Develin have investigated the notion of representing various sets S of positive integers, of size m say, as subset sums of smaller sets. The *rank* of a given set S is the smallest positive integer $rk(S) \leq m$ such that S is represented by an integer set of size $rk(S)$. In this note, we primarily consider sets of the form $\{1, 2^m, 3^m, \ldots\}$ for positive integer $m \geq 2$. Given a positive integer k, we ask for the smallest M such that $\{1, 2^m, 3^m, \ldots, k^m\}$ is independent for all $m \geq M$, and provide some answers. We then use a result of Sprague to show that any nondecreasing positive integer sequence $\mathbf{a} = \{a_1, a_2, \ldots\}$ that grows polynomially, and in particular the set $\{1, 2^m, 3^m, \ldots\}$ for fixed exponent m, has limiting rank zero.

1. Introduction

The concept of representing sets of positive integers, and more generally sets of rationals, in an "efficient" manner according to the operation of addition, has received some attention in recent years, specifically in a pair of companion papers published in 2001 by Moulton [5] and Develin [1]. Lev [4] and Ilie and Salomaa [2] have also considered questions related to subset sums.

By efficient representation, we mean the following, as illustrated by way of example. The set of powers of 2 given by $S = \{1, 2, 4, 8, 16\}$ can be represented by $P = \{-5, 1, 7, 9\}$, for $1 \in P$, $2 = -5 + 7$, $4 = -5 + 9$, $8 = 1 + 7$, and $16 = 7 + 9$. Thus S has a *subset sum representation* given by P. As the cardinality of P, denoted $|P|$, is less than $|S|$, S is said to be *dependent*.

We give some definitions that will be useful later. The terms given below, with the exception of total dependence, are taken from [5].

Definition 1.1 (Span, Representation) *The span of a set B, denoted by $sp(B)$, is the set of all sums of subsets of B. In other words, $sp(B) = \{\sum_{b\in A} b : A \subseteq B, A \neq \emptyset\}$. Hence, B represents P, when $P \subseteq sp(B)$.*

Definition 1.2 (Rank, Optimal Set) *For any set P the rank of P, denoted by $rk(P)$, is the smallest size of a set representing P. Any set representing P with size $rk(P)$ is said to be optimal.*

Moulton shows that $\{-5, 1, 7, 9\}$ is one of the 19 optimal representing sets of $S = \{1, 2, 4, 8, 16\}$. Hence, $rk(S) = 4$ here. In general, it is clear that $rk(P) \leq |P|$.

Definition 1.3 (Independent Set) *A set P for which $rk(P) = |P|$ is an independent set. Else, P is said to be dependent.*

Definition 1.4 (Limiting Rank, Total Dependence) *For any infinite set of distinct positive integers $A = \{a_n\}_{n\geq 1}$ with $A_m = \{a_1, a_2, \ldots, a_m\}$ for each m, we define the limiting rank of A by*

$$\rho(A) = \lim_{m\to\infty} \frac{rk(A_m)}{m},$$

provided said limit exists. Thus, if $\rho(A) = 1$, A is an independent set, while A is dependent if $\rho(A) < 1$. If $\rho(A) = 0$ we will say that A is totally dependent.

In Section 2 we consider the following problem: For sets of the form $A_{(k,m)} = \{1, 2^m, 3^m, \ldots, k^m\}$, where k, $m \geq 2$ are positive integers and k is fixed, find the smallest M such that $A_{(k,m)}$ is independent for all $m \geq M$. In Section 3, we use a result of Sprague to show that, for fixed exponent m, the set $P_m = \{1, 2^m, 3^m, \ldots\}$ has limiting rank zero. This is, so far as the author knows, the first class of sets for which the limiting rank is known.

2. Independent Sets of nth Powers

In contrast to Moulton and Develin, who are interested in sets of the form $\{1, r, r^2, \ldots, r^n\}$ for integer (Moulton) and rational (Develin) r, we are interested in sets of the form $A_{(k,m)} = \{1, 2^m, 3^m, \ldots, k^m\}$ for integral $m \geq 2$. In this section, we determine, for certain sets $A_{(k,m)}$ with fixed size k, the minimum M such that $A_{(k,m)}$ is independent for all $m \geq M$. Contrastingly, in Section 3 we show that for fixed m, $\lim_{k\to\infty} \frac{rk(A_{(k,m)})}{k} = 0$.

First, consider $m = 2$. A simple argument shows that $A_{(3,2)} = \{1, 4, 9\}$ is independent, while the set $\{1, 4, 9, 16\}$ can be represented by $S_4 = \{-3, 4, 12\}$, and hence $A_{(k,2)}$ is dependent for all $k \geq 4$.

Next, consider $m = 3$. It is easy to show that $A_{(3,3)} = \{1, 8, 27\}$ is independent, and an adaptation of Moulton's arguments for powers of 2 (Proposition 2 of [5]) shows that $A_{(4,3)} = \{1, 8, 27, 64\}$ is also independent. However, $\{1, 8, 27, 64, 125\}$ can be represented by $\{-34, 8, 27, 98\}$ or $\{-26, 27, 34, 90\}$, and so $A_{(k,3)}$ is dependent for all $k \geq 5$.

As the first three squares and the first four cubes are independent, we ask the following.

Question 2.1 *For $k \geq 3$, is $A_{(k,m)}$ independent for $m \geq k - 1$? More generally, given k and m, what is necessary to guarantee the independence of $A_{(k,m)}$?*

We make progress below towards answering this. First, we note the following.

Theorem 2.2 *$A_{(3,m)}$ is an independent set for $m \geq 2$.*

Proof. The case $m = 2$ is resolved (see above). For $m \geq 3$, we note that, if a set $P = \{a, b\}$, $a < b$, represents $A_{(3,m)}$, then we must have $a = 1$ and $b = 2^m$. But then $a + b = 3^m$, which cannot happen by Fermat's Last Theorem. □

Theorem 2.3 *$A_{(4,m)}$ is an independent set for $m \geq 3$.*

Proof. The method of proof is like that of Proposition 2 in Moulton's paper. Suppose by way of contradiction that $S = \{a, b, c\}$ represents $A_{(4,m)}$. Note that each element of $A_{(4,m)}$ is equal to one of a, b, c, $a + b$, $a + c$, $b + c$, or $a + b + c$. We have four possibilities.

- Case 1: All three of a, b, c belong to $A_{(4,m)}$. Then $A_{(4,m)} = \{a, b, c, d\}$ for some d, and so d is the sum of either two of a, b, and c, or the sum of all three. For the first case, we have an integer solution to the Diophantine equation

$$x^m + y^m = z^m, \tag{1}$$

an impossibility by Fermat's Last Theorem. If $d = a + b + c$ then we have an integer solution to $x^m + y^m + z^m = w^m$. One observes that the only possibility is $1 + 2^m + 3^m = 4^m$, that is, $3^m = 4^m - 2^m - 1$. As $m \geq 3$, we have

$$4^m - 2^m - 1 \;\; \geq \;\; \left(\frac{55}{64}\right) 4^m$$

where the fraction $\frac{55}{64}$ is obtained by setting $m = 3$. Hence by the above, we conclude $\left(\frac{4}{3}\right)^m \leq \frac{64}{55}$, which is impossible.

- Case 2: Exactly two of a, b, c belong to $A_{(4,m)}$. Suppose without loss of generality that a, $b \in A_{(4,m)}$, so that $A_{(4,m)} = \{a, b, d_1, d_2\}$. Observe that both d_1 and d_2 require c as a summand, otherwise we have an integer solution to (1), a contradiction. By appealing to (1), we are able to eliminate the cases $(d_1, d_2) = (a+b+c, a+c)$ and $(d_1, d_2) = (a+b+c, b+c)$ as possibilities, and thus $A_{(4,m)} = \{a, b, a+c, b+c\}$. Thus we have an integer solution to the equation $x^m + y^m = z^m + w^m$, and in particular we must have $2^m + 3^m = 4^m + 1$. Equivalently, $3^m = 4^m - 2^m + 1$. We then argue as in Case 1 to conclude that such a scenario is impossible.

- Case 3: Exactly one of a, b, c is in $A_{(4,m)}$. Suppose without loss of generality that $a \in A_{(4,m)}$. There are four possibilities for the remaining elements of $A_{(4,m)}$, and of these only the following two are viable: $A_{(4,m)} = \{a, a+b, a+c, a+b+c\}$ and $A_{(4,m)} = \{a, a+b, a+c, b+c\}$. The reason that these are the only two acceptable choices for $A_{(4,m)}$ is that, with $a \in A_{(4,m)}$, $b+c$ and $a+b+c$ cannot both belong to $A_{(4,m)}$, otherwise there exists a pair of positive integers s, u such that $s^m + a = u^m$, a contradiction to Fermat's Last Theorem as $m \geq 3$.

  For the first representation, we see that the sum of the first and fourth elements equals the sum of the second and third elements in $A_{(4,m)}$, and we are led to the same contradiction as in Case 2. If the second representation is possible, we have integral solutions to the set of equations

$$\begin{aligned} x^m + b &= w^m, \\ x^m + c &= z^m, \text{and} \\ b + c &= y^m, \end{aligned}$$

  which in turns yields an integral solution to $2x^m + y^m = z^m + w^m$. As $m \geq 3$, the only possibility is $2 + 4^m = 2^m + 3^m$, that is, $3^m = 4^m - 2^m + 2$. An argument similar to that given in Case 1 shows that such a scenario is impossible.

- Case 4: None of a, b, c lie in $A_{(4,m)}$. Thus, $A_{(4,m)} = \{a+b, a+c, b+c, a+b+c\}$. Since $(a+b) + (a+c) + (b+c) = 2(a+b+c)$, we must have an integer solution to $2x^m = y^m + z^m + w^m$. The only possibility is $2(4^m) = 3^m + 2^m + 1$, that is, $2^{2m+1} - 2^m - 1 = 3^m$. Since $2^{2m+1} - 2^m - 1 \geq \left(\frac{119}{64}\right) 4^m$, we have $\left(\frac{4}{3}\right)^m \leq \frac{64}{119}$, which is a contradiction. This completes the proof.

□

Remark. As we have made reference to Moulton's Proposition 2, we should also note that his proof has a small hole, which is easily corrected. Namely, Moulton states that the set $\{a, a+b, a+c, b+c\}$ has the property that the sum of two of its elements equals the sum of the other two, but a quick check denies this assertion. However, one can still verify the claim of independence for $\{1, 2, 4, 8\}$ in this case by way of contradiction. Specifically, if $a = 1$,

then $1+b=2^{m_1}$, $1+c=2^{m_2}$, and $b+c=2^{m_3}$, where we assume WLOG $m_1<m_2$. A little work shows, however, that m_1 must then be 1, so that $a=b=1$, contradiction. If $a=2^n$ for $1\leq n\leq 3$, then we have the equations $2^n+b=1$, $2^n+c=d$, and $b+c=e$, where $(d,e)\in\{(2,4),(4,2),(2,8),(8,2),(4,8),(8,4)\}$. Each of these cases can be easily shown to be impossible.

Theorem 2.3 serves as a "base case" in the following sense. We recall Lemma 3 from Moulton:

Lemma 2.4 *If $P=\{p_1,\ldots,p_n\}$ is a set such that $P\setminus\{p_n\}$ is independent and p_n satisfies*

$$|p_n| \;>\; \Delta_{n-1}\sum_{j=1}^{n-1}|p_j| \tag{2}$$

(where Δ_k, for $k\geq 1$, denotes the maximum determinant of $k\times k$ $0-1$ matrices), then P is independent.

The well-known Hadamard bound is $\Delta_k\leq k^{k/2}$ (see for instance [3]). Using this bound and the above lemma allows us to extend Theorem 2.3 in the following manner.

Theorem 2.5 *The following statements hold.*

1. *$A_{(5,m)}$ is independent for all $m\geq 19$.*
2. *$A_{(6,m)}$ is independent for all $m\geq 30$.*
3. *$A_{(7,m)}$ is independent for all $m\geq 45$.*

Thus, in view of Question 2.1, Theorem 2.5 resolves all cases for $A_{(5,m)}$ except $4\leq m\leq 18$, while the remaining cases of $A_{(6,m)}$ and $A_{(7,m)}$ are $5\leq m\leq 29$ and $6\leq m\leq 44$, respectively.

Resolution of the above problem would likely involve, in light of Theorem 2.5, finding better lower bounds for m, coupled with the use of a sieve.

3. Total Dependence of Polynomially Growing Sequences

While it is certainly possible to construct independent sets of nth powers for any positive integer $n\geq 2$, as we observed in the previous section, the question remains as to what, given such an n, the limiting rank of the set $P_n=\{1,2^n,3^n,\ldots.\}$ is, provided the limit exists.

We shall answer a more general version of this question. First, we give the following definition.

Definition 3.1 *A sequence of real numbers* $\{a_1, a_2, a_3, \ldots\}$ *grows polynomially in* k *if there exists a polynomial* P *(of degree* n*, say) with real coefficients, and a positive integer* K*, such that* $a_k \leq P(k)$ *for all* $k \geq K$*.*

Let $\mathbf{a} = \{a_1, a_2, \ldots\}$ be a nondecreasing positive integer sequence that grows polynomially in k, with $\lim_{k\to\infty} a_k = \infty$. Thus, $a_k \leq P(k)$ for $k \geq K$, say, where the degree of P is n, say. In particular, there exists a positive constant C such that $a_k \leq Ck^n$ for all $k \geq K$.

We claim that $\rho(\mathbf{a})$ exists, and equals 0. It is known (thanks to R. Sprague, see [6]) that, for every integer $n \geq 2$, there exists a largest positive integer r_n that is not expressible as a sum of distinct nth powers of positive integers. Let q be the largest positive integer such that $q^{n+1} \leq r_{n+1}$, and let $w = \max\{v, K-1\}$, where v is the largest integer k such that $a_k \leq r_{n+1}$. Set $T^{(0)} = \{a_1, a_2, \ldots, a_w\}$, and $S^{(0)} = T^{(0)} \cup \{1, 2^{n+1}, \ldots, q^{n+1}\}$, with $\lambda = |S^{(0)}|$. Clearly, $S^{(0)}$ represents $T^{(0)}$. We view the above setup as the zeroth stage of an algorithm whose purpose is to, ultimately, efficiently represent $\mathbf{a}$.

At the jth stage, $j \geq 1$, we represent $T^{(j)} = \{a_1, a_2, \ldots, a_w, \ldots, a_{w+j}\}$. To do this, we append, as necessary, $(q+1)^{n+1}$, $(q+2)^{n+1}$, $\ldots$, $(q+m_j)^{n+1}$ to $S^{(j-1)}$ to create $S^{(j)}$. Here $m_j < a_{w+j}^{1/(n+1)} - q \leq (C(w+j)^n)^{\frac{1}{n+1}} - q$ and is maximally chosen, thus ensuring (using Sprague's result) that $S^{(j)}$ represents $T^{(j)}$. Observe that, as j grows without bound, $m_j > 0$ for infinitely many j.

Now observe that

$$0 < \frac{rk(T^{(j)})}{|T^{(j)}|} \leq \frac{|S^{(j)}|}{|T^{(j)}|} = \frac{m_j + \lambda}{w+j} < \frac{(C(w+j)^n)^{\frac{1}{n+1}} - q + \lambda}{w+j} \longrightarrow 0$$

as $j \to \infty$, which completes the proof of the following statement.

Theorem 3.2 *Let* $\mathbf{a} = \{a_1, a_2, \ldots\}$ *be a nondecreasing positive integer sequence that grows polynomially in* k*, with* $\lim_{k\to\infty} a_k = \infty$*. Then* $\rho(\mathbf{a}) = 0$*.*

Corollary 3.3 *Let* n *be a positive integer. For the set* $P_n = \{1, 2^n, 3^n, \ldots.\}$*, we have* $\rho(P_n) = 0$*.*

The converse, namely what can be said of a given set S for which $\rho(S) = 0$, seems to be more difficult, and is left as an open problem.

4. Summary

For sets consisting of n^{th} powers, we have contrasted the notion of building independent sets using these powers with the limiting rank of such a set. In so doing, we have illustrated the

crucial role that rate of growth plays in determining, both for finite and infinite sets, whether a set is independent, and if not, the level of dependence under which the set operates. In particular, we now know that the limiting rank of any polynomially growing positive integer sequence **a** with infinite limit, and in particular the set $P_n = \{1, 2^n, 3^n, \ldots.\}$ for n a positive integer, exists and equals zero. On the other hand, sets of powers of a positive integer $r \geq 2$ have limiting rank at most $(2r-2)/(2r-1)$ (see [1] and [5]), while the factorial sequence has limiting rank at least 1/2 [1].

The above observations provoke the following question, an answer to which would be most welcome.

Problem 4.1 *For a given set S of positive integers whose elements are listed in increasing fashion, determine $\rho(S)$ if it exists, or at least offer reasonable upper and lower bounds for such. If $\rho(S)$ does not exist, explain why the limit fails to exist, and in so doing, describe the behavior of the sequence of ratios $\{rk(S_1), rk(S_2)/2, rk(S_3)/3, \ldots\}$, where S_m is the subset of S consisting of the first m elements of S.*

5. Acknowledgements

The author wishes to thank Joseph L. Yucas of Southern Illinois University and Patrick Mitchell of Midwestern State University for helpful discussions carried out in the course of writing this paper. The author also thanks the referee for his or her efforts in helping to improve the paper's quality.

References

[1] Develin, Mike. *On optimal subset representations of integer sets.* J. Number Theory **89** (2001), no. 2, 212-221.

[2] Ilie, Lucian and Salomaa, Arto. *On the expressiveness of subset-sum representations.* Acta Inform. **36** (2000), no. 8, 665-672.

[3] Johnson, Charles R. and Newman, Morris. *How bad is the Hadamard determinantal bound?* J. Res. Nat. Bur. Standards Sect. B **78B** (1974), 167-169.

[4] Lev, Vsevolod F. *Blocks and progressions in subset sums sets.* Acta Arith. **106** (2003), no. 2, 123-142.

[5] Moulton, David Petrie. *Representing powers of numbers as subset sums of small sets.* J. Number Theory **89** (2001), no. 2, 193-211.

[6] Sprague, Roland. *Über Zerlegungen in n-te Potenzen mit lauter verschiedenen Grundzahlen.* Math. Z. **51** (1948), 466-468.