When is a set determined by its pairwise sums? (Exposition)

William Gasarch *

Univ. of MD at College Park

1 Introduction

Everything in this exposition was told to me by Noga Alon; however, he does not claim to be the originator of it nor does he know who is. Selfridge and Straus [1] proved the main result originally with a different proof.

Def 1.1 If A is a set then

$$\begin{aligned} A + A = & \quad \{x + y : x, y \in A\} \\ A +^* A = & \quad \{x + y : x, y \in A, x \neq y\}. \end{aligned}$$

Let $A = \{x, y\} \in \binom{\mathsf{N}}{2}$. Does $A +^* A$ determine A? NO- if $x + y = 5$ then $\{x, y\}$ could be either $\{1, 4\}$ or $\{2, 3\}$.

Let $A = \{x, y, z\} \in \binom{\mathsf{N}}{3}$. Does $A +^* A$ determine A? YES:

First determine $S = ((x + y) + (x + z) + (y + z))/2 = x + y + z$.

Then determine

$x = S - (y + z)$

*University of Maryland, College Park, MD 20742, gasarch@cs.umd.edu

$y = S - (x + z)$

$z = S - (x + y)$.

Let $A = \{x, y, z, w\} \in \binom{\mathsf{N}}{4}$. Does $A +^* A$ determine A? We will see soon.

Def 1.2 A number n is *nice* if, for all $A \in \binom{\mathsf{N}}{n}$, A is completely determined by $A +^* A$.

Which n are nice? Selfridge and Straus showed that n is nice iff n is not a power of two. The proof uses Generating Functions. I do not know of another way to do it.

2 The Main Theorem

Theorem 2.1 *n is nice iff n is not a power of two.*

Proof:

PART I:

We show that if n IS a power of 2 then there exists $A, B \in \binom{\mathsf{N}}{n}$ such that $A +^* A = B +^* B$. The proof is by induction on n (actually on $\lg n$).

If $n = 2^1$ then take $A = \{1, 4\}$ and $B = \{2, 3\}$.

Assume that we have sets $A', B' \in \binom{[2^m]}{2}$ such that $A' +^* A' = B' +^* B'$. Let

$$\begin{aligned} x = &\ \max\{A', B'\} + 1 \\ A = &\ A' \cup (B + x) \\ B = &\ B' \cup (A + x) \end{aligned}$$

We leave it to the reader to show that $A +^* A = B +^* B$.

PART II:

We show that if there exists $A, B \in \binom{\mathsf{N}}{n}$ with $A +^* A = B +^* B$ then n is a power of 2. Let

$$\begin{aligned} A(x) = &\ \textstyle\sum_{i \in A} x^i \\ B(x) = &\ \textstyle\sum_{i \in B} x^i \end{aligned}$$

Clearly

$$\begin{aligned}\textstyle\sum_{i\in A^*+A} x^i = &\; A(x)^2 - A(x^2)\\ \textstyle\sum_{i\in B^*+B} x^i = &\; B(x)^2 - B(x^2)\end{aligned}$$

Hence

$$\begin{aligned}A(x)^2 - A(x^2) = &\; B(x)^2 - B(x^2)\\ (A(x) - B(x)(A(x) + B(x) = &\; A(x^2) - B(x^2) \text{ MAIN EQUATION}\end{aligned}$$

Note that $A(1) - B(1) = n - n = 0$. Hence there exists $m \geq 1$ and polynomial f such that $f(1) \neq 0$ and

$$A(x) - B(x) = (x-1)^m f(x).$$

Hence also note that

$$A(x^2) - B(x^2) = (x^2-1)^m f(x^2).$$

Using both of these in the MAIN EQUATION above yields

$$\begin{aligned}(x-1)^m f(x)(A(x) + B(x)) = &\; (x^2-1)^m f(x^2)\\ f(x)(A(x) + B(x)) = &\; (x+1)^m f(x^2)\end{aligned}$$

Plug in $x = 1$ to obtain

$$\begin{aligned}f(1)(A(1) + B(1)) = &\; (1+1)^m f(1^2)\\ f(1) \times 2n = &\; 2^m f(1)\\ 2n = &\; 2^m \text{ (Can divide by } f(1) \text{ since } f(1) \neq 0.)\\ n = &\; 2^{m-1}\end{aligned}$$

So we have that n is a power of 2. ∎

What did we use about the natural numbers in this proof? Not much— just that if p is a polynomial (so natural number exponents) and $p(1) = 0$ then $p(x) = (x-1)^m h(x)$ where $h(1) \neq 0$.

If instead of natural numbers we had real (complex) numbers we would need this to be true of the functions that are sums of terms of the form x^r where r is real (complex). There is a slight issue with the fact that (say) $x^{1/3}$ is not uniquely defined; however, we are confident this could be worked out and that the proof presented can be extended to the complex case.

References

[1] J. Selfridge and E. Straus. On the determination of numbers by their sums of a fixed order. *Pacific Journal of Mathematics*, 8(4):847–856, 1958. `http://www.cs.umd.edu/~gasarch/BLOGPAPERS/selfridgeorig.html`.