Canad. Math. Bull. Vol. **16** (3), 1973

THE CARDINALITIES OF $A+A$ AND $A-A$

BY
SHERMAN K. STEIN

H. T. Croft's Research Problems, 1967, contains the following problem due to J. H. Conway. "Let $A=\{a_1, a_2, \ldots, a_N\}$ be a finite set of integers, and define

$$A+A = \{a_i+a_j; 1 \leq i, j \leq N\}$$

and

$$A-A = \{a_i-a_j; 1 \leq i, j \leq N\}.$$

Prove that $A-A$ always has more members than $A+A$, unless A is symmetric about 0." Marica in [1] showed that the conjecture is false for the set $A=\{1, 2, 3, 5, 8, 9, 13, 15, 16\}$. In this case $A+A$ has 30 elements and $A-A$ has 29 elements.

In Marica's example the ratio between the cardinality of $A-A$ and the cardinality of $A+A$ is 29/30 or 0.966 ... It is the purpose of this note to show that there are sets A for which this ratio is as close to 0 as we please (and also as large as we please).

A few definitions will be given first. The cardinality of a finite set X will be denoted $|X|$. If A is a finite set of integers, the ratio

$$\frac{|A-A|}{|A+A|}$$

will be denoted $r(A)$.

Also, if A is a set and n is an integer, $A+nA$ will stand for the set $\{a+na' \mid a \in A, a' \in A\}$. The result will follow easily from these three lemmas.

LEMMA 1. *Let X be a finite set of integers. Then there exists an integer n such that the equality $x_1+nx_1'=x_2+nx_2'$ for x_1, x_1', x_2, x_2' in X implies that $x_1=x_2$ and $x_1'=x_2'$. Thus $|X+nX|=|X|^2$.*

Proof. Let n be any integer distinct from all of the fractions.

$$\frac{x_1-x_2}{x_2'-x_1'}$$

that can be formed with $x_1, x_2, x_1', x_2' \in X$ and $x_2' \neq x_1'$. Such an n satisfies the demand of the lemma.

Received by the editors September 23, 1971.

https://doi.org/10.4153/CMB-1973-055-6 Published online by Cambridge University Press

LEMMA 2. *Let $X_1, X_2, \ldots, X_k$ be finite sets of integers. Then there is an integer n such that $|X_i+nX_i|=|X_i|^2$ for $i, i=1, 2, \ldots, k$.*

The proof follows easily from the proof of Lemma 1.

LEMMA 3. *Let A be a finite set of integers. Then there is an integer n such that $r(A+nA)=(r(A))^2$.*

Proof. Let n be an integer whose existence is assured by Lemma 2 for the three sets $X_1=A$, $X_2=A+A$, and $X_3=A-A$. Let $B=A+nA$. Then

$$\begin{aligned} B+B &= \{(a_1+na_1')+(a_2+na_2') \mid a_1, a_1', a_2, a_2' \in A\} \\ &= \{(a_1+a_2)+n(a_1'+a_2') \mid a_1, a_1', a_2, a_2' \in A\} \\ &= A+A+n(A+A). \end{aligned}$$

Thus

$$|B+B| = |A+A|^2.$$

Also,

$$\begin{aligned} B-B &= \{(a_1+na_1')-(a_2+na_2') \mid a_1, a_1', a_2, a_2' \in A\} \\ &= \{a_1-a_2+n(a_1'-a_2') \mid a_1, a_1', a_2, a_2' \in A\} \\ &= A-A+n(A-A). \end{aligned}$$

Thus

$$|B-B| = |A-A|^2.$$

Consequently

$$r(B) = \frac{|B-B|}{|B+B|} = \frac{|A-A|^2}{|A+A|^2} = (r(A))^2.$$

THEOREM. *There exist finite sets of integers A for which $r(A)$ is arbitrarily small or arbitrarily large.*

Proof. Marica's example shows that there is a set A for which $r(A)$ is less than 1. Repeated application of Lemma 3, starting with Marica's example, provides sets A of arbitrarily small $r(A)$. Repeated application of Lemma 3, starting with any set for which $r(A)$ is larger than 1, the simplest of which is $\{0, 1, 3\}$, provides sets A of arbitrarily large $r(A)$.

The proof of the theorem raises another question. For convenience assume that A contains only nonnegative integers and that 0 is an element of A. The sets A constructed in the proof of the theorem, when $r(A)$ is very small or very large, have many elements spread sparsely over a large interval. Is there some general inequality relating $r(A)$, $|A|$, and the largest element in A?

Postscript

H. Croft has called to my attention Sophie Piccard's *Sur des ensembles parfaits*, Mémoires de l'université de Neuchatel, **16** (1942), (Zentralblatt fur Mathematik, **27** (1943), 204–205), which examines the sets $A+A$ and $A-A$ where A is a set of real numbers. On p. 176 these two propositions are to be found:

PROPOSITION 1. *There is a set A of real numbers such that $A+A$ consists of all nonnegative real numbers and $A-A$ has measure zero.*

PROPOSITION 2. *There is a set A of real numbers such that $A+A$ has measure zero and $A-A$ consists of all real numbers.*

A negligible modification of her arguments easily establishes that there are finite sets of integers A for which $r(A)$ is as small or as large as we please. We sketch the argument, based on that for Proposition 1, that shows that $r(A)$ can be made arbitrarily small.

Let $K=\{0, 1, 3, 4, 5, 7, 10, 14\}$ and let n be a positive integer (later to be chosen large). Observe that $K+K \supseteq \{0, 1, 2, \ldots, 15\}$ while $K-K$ does not contain the elements 8 and 15.

Let $A=K+16K+16^2K+\cdots+16^{3n-1}K$, that is, the nonnegative integers less than 16^{3n} whose representation in base 16 uses only the eight digits in K.

Then $A+A \supseteq \{0, 1, \ldots, 16^{3n}-1\}$ while $A-A$ contains no integer that has the three successive digits 080 in base 16 (because neither 8 nor 15 is in $K-K$). Thus $A-A$ contains no integer whose representation in base 16^3 has the digit $8 \cdot 16=128$. Consequently $A-A$ has at most $2((16^3-1)/16^3)^n 16^{3n}$ integers. Thus $r(A) \le 2((16^3-1)/16^3)^n$, which approaches 0 as n increases.

A similar argument, starting with $K=\{0, 2, 3, 7\}$ and using base 10, produces sets of integers for which $r(A)$ is as large as we please.

Reference

1. J. Marica, *On a conjecture of Conway*, Canad. Math. Bull. **12** (1969), 233–234.

UNIVERSITY OF CALIFORNIA,
DAVIS, CALIFORNIA