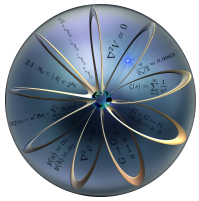

planetmath.org

Math for the people, by the people.

sum-product theorem

Canonical name	SumproductTheorem
Date of creation	2013-03-22 16:54:48
Last modified on	2013-03-22 16:54:48
Owner	Algeboy (12884)
Last modified by	Algeboy (12884)
Numerical id	8
Author	Algeboy (12884)
Entry type	Theorem
Classification	msc 11T99
Classification	msc 05B25
Synonym	Sum-product estimate

Suppose $\mathbb{F}$ is a finite field. Then given a subset A of $\mathbb{F}$ we define the *sum* of A to be the set

$$A + A = \{a + b : a, b \in A\}$$

and the product to be the set

$$A \cdot A = \{a \cdot b : a, b \in A\}.$$

We concern ourselves with estimating the size of $A + A$ and $A \cdot A$ relative to the size of A, and ultimately also to the size of $\mathbb{F}$.

If A is empty then $A+A$ is empty as is $A \cdot A$ and so $|A| = |A+A| = |A \cdot A|$. Now suppose A is non-empty then let $a \in A$. Then

$$a + A = \{a + b : b \in A\} \subset A + A$$

so $|A| \leq |A + A|$. If $A = \{0\}$ then $A \cdot A = A$ so finally assume $a \in A$, $a \neq 0$. Then we have

$$a \cdot A = \{a \cdot b : b \in A\} \subset A \cdot A$$

so in any case it always follows that

$$|A| \leq |A + A|, |A \cdot A|. \tag{1}$$

Now if $\mathbb{F}$ has a proper subfield $\mathbb{F}_0$ – for instance $\mathbb{F} = GF(p^2)$ and $\mathbb{F}_0 = GF(P)$ – then setting $A = \mathbb{F}_0$ makes $A = A + A = A \cdot A$ and so in this situation the bound in (**??**) is tight, that is, $|A| = |A + A| = |A \cdot A|$. So we insist now that $\mathbb{F}$ is a prime field, so it has no proper subfields.

We would like to understand what size A must have to ensure that either $A + A$ or $A \cdot A$ is larger than A. (Note this is not the same as asking if $A \neq A + A$ or $A \cdot A$ as we are concerned only with growth in size not the change in the elements of the set.) Clearly $A = \{0\}$ fails, as does $A = \mathbb{F}$ and with some intuition as guidance it is safe to presume that A must be large enough to have enough elements to produce many elements as a sum or product but also small enough that these these new elements outgrow the size of A. This is the content of the following important result.

Theorem 1 (Sum-Product estimate:Bourgain-Katz-Tao (2003))**.** *Let $\mathbb{F} = \mathbb{Z}_p$ be the field of prime order p. Let A be any subset of $\mathbb{F}$ such that*

$$|\mathbb{F}|^{\delta} < |A| < |\mathbb{F}|^{1-\delta}$$

for some $\delta > 0$. Then

$$\max\{|A + A|, |A \cdot A|\} \geq C|A|^{1+\varepsilon}$$

for some $\varepsilon > 0$ which depends on δ and some constant C which also depends on δ.

The proof is non-trivial. Jean Bourgain was awarded the Fields' medal in 1994, Terence Tao in 2006 with the prize in part due to his various contributions in additive number theory.

`http://www.arxiv.org/abs/math/0301343` Bourgain, Katz, and Tao, *A Sum-Product estimate in finite fields, and applications*, (preprint) arXiv:math/CO/0301343 v2, 2003.