Additive Combinatorics and applications, Winter 2014
Homework 3, due March 14, 2014

This homework will focus on the sum product theorem.

**Question 1.** Let $\mathbb{F}_p$ be a prime finite field. We showed that if $A \subset \mathbb{F}_p$ is a set of size $|A| \leq p^{0.9}$ (say), then

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

for some $\varepsilon = \varepsilon(0.9)$. Prove the following "off-diagonal" version: if $A, B, C \subset \mathbb{F}_p$ with $|A| = |B| = |C| = N$ with $N \leq p^{0.9}$, then

$$|A + B \cdot C| \geq N^{1+\varepsilon'}$$

for some $\varepsilon' = \varepsilon'(0.9)$.

We showed that multiple addition and multiplication on a set can increase its size to almost all the field. Consider the following strong conjecture: if $A \subset \mathbb{F}_p$ has size $|A| = p^\delta$, then for any $\varepsilon > 0$ there exist $t = t(\delta, \varepsilon)$ such that

$$\max(|tA|, |A^t|) \geq p^{1-\varepsilon}.$$

**Question 2.** Prove that this conjecture is false (eg, give a counter-example). What do you think is the best (weaker) version of this conjecture which may still be true?

The next question is about the distributional version of the sum-product theorem, which shows that it can be used to construct multi-source extractors.

**Question 3.** Let $\varepsilon, \delta > 0$. Prove that there exist $t = t(\varepsilon, \delta)$ and a polynomial $q(x_1, \ldots, x_t)$ such that the following holds. If $A \subset \mathbb{F}_p$ has size $|A| \geq p^\delta$, and $X_1, \ldots, X_t \in A$ are uniformly and independently chosen, then

$$q(X_1, \ldots, X_t)$$

is $\varepsilon$-close to a distribution with min-entropy $(1 - \varepsilon) \log p.$