0.1 Notes on Checksum Communication Complexity

A paper has shown that the Number on Forehead communication complexity of CheckSum has been bounded as follows:

$$(\log N)^{\Omega(1)} \leq NOF(CheckSum) \leq O(\sqrt{\log N})$$

There are many different techniques to analyze something called Ramsey type Problems, where we try to maximize the size of a set while avoiding a certain pattern (like 3-Arithmetic Progressions).

- Graph Theory
- Ergodic Theory
- Fourier Analysis (Most Success)
- Polynomial Method

1 3AP Over Finite Field

The 3AP problem is the same as the original problem over $[N]$, however, we focus on the case where arithmetic is done over $\mathbb{R}_3^n$. This argument generalizes to any group where there exists a plus operation and we make a set such that:

$$\nexists a, b, c | a \neq b \neq c, a + c = 2b$$

We want to determine, given the universe $U = \{0,1,2\}^n$ where addition is mod 3:

$$r_3(\mathbb{F}_3^n) = \max |S| \text{ where } S \subseteq \{0,1,2\}^n \text{ and no 3AP exists.}$$

This is also called the "CAP-SET PROBLEM".

1.1 Size of CAP-SET

Recall that Beherend's construction led to a subset $S \subseteq [N]$, where:

$$|S| \subseteq \frac{N}{2^{c \cdot \sqrt{\log N}}}$$

In CAPSET case, the size of N is 3^n. We argue that it is easier to form a $3AP$ in $\mathbb{F}_3^n$ than in $[3^n]$.

Intuition: Finding solutions to $x + y = 2z$ modular arithmetic is easier over $\mathbb{F}_3^n$ than $\mathbb{Z}$. (I do not get his argument)

Theorem 1.1. $r_3(\mathbb{F}_3^n) \leq (2.76)^n = N^c$ *for some* $c < 1$.

Recall that $N/(2^{c \cdot \sqrt{\log N}}) \leq r_3(\mathbb{Z}_n)$

1.2 Examples and Properties

Firstly, we know that we can select a set that has size 2^n that satisfies that there are no $3AP$'s. We argue that $A = \{0, 1\}^n$ has no $3AP$'s.

Proof. Assume that there was some a, b, c such that they form a nontrivial $3AP$. The argument is relatively straightforward, but we know that if $a_i + b_i$ is 1, c_i cannot be a three AP, if $a_i + b_i = 0$ then $a_i = b_i = c_i = 0$ so they must be the same bit and if $a_i + b_i = 2$ then $c_i = b_i = a_i = 1$. So either the three numbers are the same or they do not form a $3AP$. $\square$

This provides a lower bound for $r_3(\mathbb{F}_3^n)$:

$$r_3(\mathbb{F}_3^n) \geq 2^n = N^{\log_3 2} \approx N^{0.63}$$

What do $3AP$s over mod 3 arithmetic look like? We know that:

$$(a, b, c) \in \{0, 1, 2\}^n \text{ and } a + b = 2c$$

We can think of it as:

$$\begin{aligned} a + b &\equiv 2c \mod 3 \\ \forall i, a_i + b_i &\equiv 2c_i \mod 3 \\ a_i + b_i &\equiv -c_i \mod 3 \\ a_i + b_i + c_i &\equiv 0 \mod 3 \end{aligned}$$

This equation is satisifed when all $a_i = b_i = c_i$ or each value is unique.