Capset constructions

Felipe Voloch

$\mathbb{F}_{q^{16}}$

July 2025

Abstract

Capsets are subsets of the n-dimensional affine space over the field of three elements with no three points on a line and there has been a lot of interest in them, which we will briefly explain. We will also survey some of the main results and then present some new algebraic constructions of capsets and discuss their properties.

Outline

Introduction

Small complete capsets

Greedy capsets

Quadrics

Introduction

Capsets

$\mathbb{F}_3^n$ is the n-dimensional vector space over $\mathbb{F}_3$.

Definition

A *capset* is a subset of $\mathbb{F}_3^n$ containing no three distinct points on a line. A capset is *complete* if it's not a subset of a larger capset. Let $\mathcal{C}$ be the set of real numbers α, for which there exists an increasing sequence $n_k \in \mathbb{N}$ and complete capsets $C_k \subset \mathbb{F}_3^{n_k}$, with $\lim(|C_k|)^{1/n_k} = \alpha$.

Questions: How large can a capset be? What are the sizes of complete capsets? What is the value of $c := \sup \mathcal{C}$?

We have that $\mathcal{C} = [\sqrt{3}, c]$. Ellenberg-Gijswijt: $c \leq 2.756$. Tyrell: $c \geq 2.217$.

Caps

More generally, we can consider *caps* in n-dimensional affine or projective space over $\mathbb{F}_q$, which are sets with no three distinct points on a line. We will use this notion when q is a power of 3.

We note that the situation for fixed n and large q is very different from the case fixed q and large n.

Applications

- Matrix multiplication algorithms
- Coding theory: error-correcting codes
- Randomness extractors
- Model for Erdős's problem on subsets of $[1, N] \cap \mathbb{N}$ with no three in an arithmetic progression

Small complete capsets

Lower bound

Consider a capset in $\mathbb{F}_3^n$ with N points, the $\mathbb{F}_3$ lines through the $N(N-1)/2$ pairs of points of the capset have their third point in the complement of the capset, so if $N(N-1)/2 < 3^n - N$, the capset is not complete. Hence:

Theorem

A complete capset $C \subset \mathbb{F}_3^n$ satisfies

$$|C|(|C|+1) \geq 2 \cdot 3^n$$

Roughly, C has at least $\sqrt{2} \cdot 3^{n/2}$ points, so $\inf \mathcal{C} \geq \sqrt{3}$.

A conic is a capset but it is too small to be complete.

Construction of a small capset

Theorem

Let $q = 3^m, m$ *odd and* $C \subset \mathbb{F}_q^2$ *be given by*

$$C = \{(x, x^2) \mid x \in \mathbb{F}_q, x \neq 0\} \cup \{(x, -x^2) \mid x \in \mathbb{F}_q, x \neq 0\}.$$

Then C *is a complete capset.*

This example has roughly $2 \cdot 3^{n/2}$ points, which proves $\min \mathcal{C} = \sqrt{3}$. But there is still a gap between this result and the lower bound. What is the size of the smallest complete capset?

Greedy capsets

Greedy capsets, definition

Definition
Start with $S_0 = \mathbb{F}_3^n$ and for $i = 1, 2, \ldots$ define $S_i = S_{i-1} \setminus \{P_i\}$, where the point P_i is among those points $P \in S_{i-1}$ such that the number of lines through P contained in S_{i-1} is positive and maximal among all points of S_{i-1}. The procedure stops when S_i is a capset. A capset generated by a greedy construction is called a *greedy capset*.

The output capset is not uniquely determined as there is a choice for P_i whenever there is more than one point with the maximal count of lines. This certainly happens at the first step and can happen at subsequent ones as well.

Greedy capsets, characterization

The following result characterizes greedy capsets.

Theorem

(Dawson, Shuvaev, V.) A subset $C \subset \mathbb{F}_3^n$ *is a greedy capset if and only if it has the following structure. There is a hyperplane* $H_0 \subset \mathbb{F}_3^n$ *such that* $C \cap H_0 = \emptyset$ *and, if* H_1, H_2 *denote the two hyperplanes of* $\mathbb{F}_3^n$ *parallel to* H_0*, then* $C \cap H_i, i = 1, 2$ *are greedy capsets, so miss a hyperplane of* H_i *and so on, recursively. In particular,* $\#C = 2^n$*.*

Can we characterize complete greedy capsets? How big can the completion of a greedy capset be?

Quadrics

Quadrics as capsets

Theorem

Let λ be a non-square in $\mathbb{F}_q$ and $Q \subset \mathbb{F}_q^3$ be given by

$$Q = \{(x, y, x^2 - \lambda y^2) \mid x, y \in \mathbb{F}_q\}.$$

Then Q is a complete capset.

Proof

Since Q is an elliptic quadric, it is a cap, so it is a capset. To show it is complete, let $(a, b, c) \notin Q$ and consider the set $Q' = \{(x, y, z) \mid -(a, b, c) - (x, y, z) \in Q\}$. This is clearly also an elliptic quadric. As algebraic varieties, Q and Q' meet at infinity on a pair of (conjugate) lines so the affine part of their intersection is a conic (by Bézout), hence has a rational point.

Thank You

Questions?