SET AND AFFINE CAPS

ELLEN MCCULLAGH

Abstract. This paper begins by discussing the game SET, and uses it as an introduction to affine caps. I then go on to find a general upper bound for affine caps.

Contents

1. Introduction

Marsha Falco created the game SET while doing genetics research on epilepsy in German Shepherds. The game was published by SET enterprises in 1991. SET presents an accessible entry into the field of affine caps in finite fields. This paper starts by discussing the game, the rules, and the gameplay. The second section discusses the game in mathematical terms, and what a cap means in the game. In that section I prove that the maximal cap for $\mathbb{F}_3^2$ is 4, using SET. The third section introduces the abstract notion of a cap, and I prove that the maximal cap in $\mathbb{F}_2^k = |\mathbb{F}_2^k| = 2^k$. In the fifth section I derive a general inequality that puts an upper bound on the size of the maximal cap in $\mathbb{F}_q^k$.

2. The Game SET

SET is a game of patterns played with cards. Each card has a either one two or three shapes on it. The shapes are either diamonds, squiggles, or ovals. Each shape is either red, green, or purple. Each shape is also either solid, shaded or empty. In other words there are four categories of attributes, number, shape, color, and shading, and within each category there are three types. Since each card is unique it is easy to calculate that there are 81 or 3^4 cards. To begin the game the dealer sets out 12 cards in a 3 by 4 grid. The players then must find SETs.

Definition 2.1. A SET is a collection of three cards such that, within each category, the cards are either all the same or all different.

An example of a SET is a red solid diamond three, a purple shaded diamond two, and a green empty diamond one. As you can see in color, shading, and number these cards are all different, but in shape they are all the same. These cards could have been all different if one was an oval and the other a squiggle, and still made a SET. The key idea is that two cards do not share an attribute that the other does not have. When a player identifies a SET in the grid they say "SET" and collect the three cards. The dealer puts three more down and play continues until there are no more cards. The player with the most SETs wins.

Date: DEADLINE AUGUST 22, 2008.

3. Number Theory

To think of SET mathematically the cards and there attributes need to be represented by numbers. There are a few different ways to make this happen. The first way is to use the cards restricted to red solids and arrange them in a grid, as in fig 1. What is interesting here is that any "tic-tac-toe" line leads to a SET, but

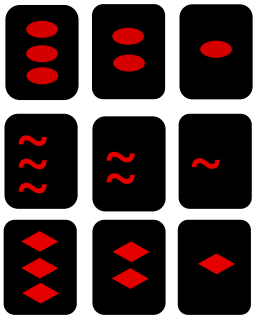

Figure 1. Here are all of the red solid cards arranged by number and shape.

slightly more interestingly any "tic-tac-toe on the torus" line leads to a SET, such as the two oval, the one diamond, and the three squiggle in fig. 1. As you can see this sort of understanding depends a great deal on arrangement. If any two cards were switched this wouldn't work, as in Fig. 2. So how must they be arranged?

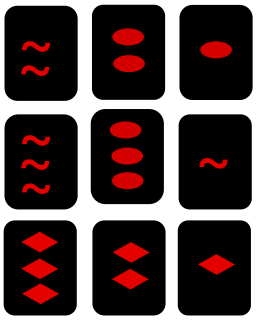

Figure 2. Here is figure one with the three ovals switched with the two squiggles. Here straight lines do not necessarily determine SETs.

Well this brings up the second way of thinking about this. If each category is put into a component of a vector eg (number, shape, color, shading), and within each category the types are assigned numbers (number 1-0, 2-1, 3-2; shape squiggle-0, diamond-1, oval-2; color red-0, green-1, purple-2; shading solid-0, shaded-1, empty-3), then a SET is one in which the sum of all three cards, in this form, is zero mod 3. More mathematically, there is a one to one correspondence between the SET cards and $\mathbb{F}_3^4$, the field of three elements in four dimensions. Given any three vectors, a_1, a_2, a_3, these vectors make a SET if $a_1 + a_2 + a_3 = 0$.

4. Affine Caps

It sometimes happens that when the 12 cards are put down that there are no SETs. In the rules of SET, if this happens three more cards are put down, and so on until there is a SET. This prompts the question how many cards must be put down to guarantee a SET? or equivalently: What is the maximum number of cards possible in a collection with no SETs?

Definition 4.1. A collection of cards such that there are no SETs is called a cap.

In the case of all red solid cards, or $\mathbb{F}_3^2$, the size of the maximal cap is 4. An example of a maximal cap is shown in Fig. 3.

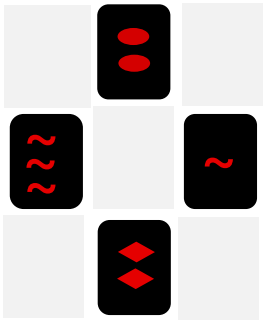

Figure 3. The cards shown are an example of a cap of size 4 in this field. Check to make sure there are no SETs!

Theorem 4.2. *The maximal cap size of* $\mathbb{F}_3^2$ *is 4.*

Proof. Suppose there exists a cap of size 5. This must mean that there are two elements in two of the rows and only one in the other row (eg Fig 4).

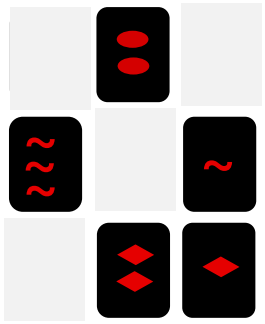

Figure 4. An example of a "5-cap"

Let the A be the element that is the only one in its row. There are four SETs using A, or four lines going through A (as below)

One of the four lines will be the row that contains A. That leaves three lines that contain the entire 'cap'. So by the pigeon hole principle one of the lines must contain two other points, making a SET. In the example the purple line contains a SET. □

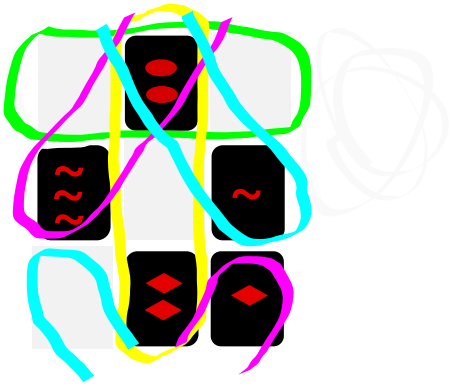

FIGURE 5. All possible SETs with A

5. Generalizing Caps

Now that we have seen caps in an elementary way, we can generalize to fields of arbitrary size and dimension. In this section we will find an upper bound on cap size for general finite fields.

Definition 5.1. $C \subset \mathbb{F}_q^k$ is a cap if for any $a_1, a_2, a_3 \in C$ there exist $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_q$ and $\lambda_i \neq 0$ for all i with $\lambda_1 + \lambda_2 + \lambda_3 = 0$ such that $\lambda_1 a_1 + \lambda_2 a_2 + \lambda_3 a_3 \neq 0$.

In our original problem we were dealing with $\mathbb{F}_3^4$. In this case we get a slightly simpler definition.

Theorem 5.2. *$C \subset \mathbb{F}_3^k$ is a cap if for any $a_1, a_2, a_3 \in C$, $a_1 + a_2 + a_3 \neq 0$.*

Proof. $C \subset \mathbb{F}_3^4$ is a cap so for any $a_1, a_2, a_3 \in C$ there exist $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_3$ with all λ non-zero and $\lambda_1 + \lambda_2 + \lambda_3 = 0$ such that $\lambda_1 a_1 + \lambda_2 a_2 + \lambda_3 a_3 \neq 0$. now if $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_3$ and $\lambda_1 + \lambda_2 + \lambda_3 = 0$ then $\lambda_1 = \lambda_3 = \lambda_3$ since in order for their sum to be zero in $\mathbb{F}_3$, it must be a multiple of three. so it is enough to assume that $\lambda_1 = \lambda_3 = \lambda_3 = 1$, since they cannot be zero, and if they equaled two the sum would not change, since we mod by 3. □

Definition 5.3. $C(q, k)$ is the maximum cap size for the field $\mathbb{F}_q^k$.

Theorem 5.4. $C(2, k) = |\mathbb{F}_2^k| = 2^k$.

Proof. Take $\lambda_1, ..., \lambda_3 \in \mathbb{F}_2$ and $\lambda_i \neq 0$ for $i = 1, 2, 3$ with $\sum_{i=0}^{3} \lambda_i = 0$. Since for any $x \in \mathbb{F}_2, x = 0$ or $x = 1$ and $\lambda_i \neq 0$ for $i = 1, 2, 3$ then $\lambda_1 = \lambda_2 = \lambda_3 = 1$, but $\lambda_1 + \lambda_2 + \lambda_3 = 1 + 1 + 1 = 1 \neq 0$. Thus no λs exist to satisfy the definition, meaning the entire space is a cap. □

The rest of this paper is devoted to finding a generalized equation for an upper bound of caps.

Theorem 5.5. *Let $q > 2$ with $q = p$ for p prime, $k > 3$, $V = \mathbb{F}_q^k$, $A \subset V$ a cap, $Q = |V| = q^k$, and ζ a complex primitive p^{th} root of unity. Given $a_1, a_2, a_3 \in A$ we can find $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_q$ with $\sum_i \lambda_i = 0$. Let*

$$S = \sum_{y \in V \setminus \{0\}} \sum_{a_1, a_2, a_3 \in A} \zeta^{(\sum_i \lambda_i a_i) \cdot y}. \tag{5.6}$$

Then $S = |A|(Q - |A|^2)$.

Proof. Notice that $\sum_{a_1,a_2,a_3 \in A} \zeta^{(\sum_i \lambda_i a_i)\cdot 0} = \sum_{a_1,a_2,a_3 \in A} 1 = |A|^3$ So we have

$$S = \sum_{y \in V} \sum_{a_1,a_2,a_3 \in A} \zeta^{(\sum_i \lambda_i a_i)\cdot y} - |A|^3 \tag{5.7}$$

Now we have to prove that

$$\sum_{y \in V} \sum_{a_1,a_2,a_3 \in A} \zeta^{(\sum_i \lambda_i a_i)\cdot y} = Q|A| \tag{5.8}$$

To prove this it is enough to show that whenever $\sum_{i=1}^{3} \lambda_i a_i \neq 0$

$$\sum_{y \in V} \sum_{a_1,a_2,a_3 \in A} \zeta^{(\sum_i \lambda_i a_i)\cdot y} = 0 \tag{5.9}$$

If (5.9) is true then, since A is a cap, the only non-vanishing sums are when $a_1 = a_2 = a_3$. So if $\sum_{i=1}^{3} \lambda_i a_i = 0$ then

$$\sum_{y \in V} \sum_{a_1,a_2,a_3 \in A} \zeta^{(\sum_i \lambda_i a_i)\cdot y} = \sum_{y \in V} \sum_{a_1 \in A} \zeta^{0 \cdot y}$$

$$= \sum_{y \in V} \sum_{a_1 \in A} 1 = \sum_{y \in V} |A| = |V||A|$$

So now on to proving (5.9). Let $x = \sum_{i=1}^{3} \lambda_i a_i$ and take A to be a bijective transformation such that $A^T x = e_1$. so

$$\sum_{y \in V} \zeta^{x \cdot y} = \sum_{y \in V} \zeta^{x \cdot A(A^{-1}y)}$$

$$= \sum_{y \in V} \zeta^{A^T x \cdot A^{-1} y} = \sum_{y \in V} \zeta^{A^{-1} y * e_1}$$

$$= C \sum_{y \in V} \zeta^{y_1} = C \sum_{y_1 \in \mathbb{F}_q} \zeta^{b}$$

for some constant C and where y_1 is the first component of y.

$$\sum_{y \in V} \zeta^{x \cdot y} = C \frac{\zeta^q - 1}{\zeta - 1}$$

$$= 0$$

since $\zeta = e^{\frac{2i\pi}{q}}$

□

Definition 5.10. Let $0 \neq \lambda \in \mathbb{F}_q$ and $0 \neq y \in V$. Define $U(\lambda)_y = \sum_{a \in A} \zeta^{(\lambda a)\cdot y}$, and $u(\lambda)_y = |U(\lambda)_y|$. Let $u(\lambda)$ be a real vector of length $Q - 1$ whose coordinates are parametrized by $0 \neq y \in V$ the corresponding entry being $u(\lambda)_y$.

Here we start to see the beginnings of our inequality.

Theorem 5.11. *Let* $0 \neq \lambda \in \mathbb{F}_q$ *and* $0 \neq y \in V$. *Then*

$$u(\lambda)_y \leq qC(q, k-1) - |A| = \frac{C(q, k-1)}{q^k} Q - |A|$$

where A *is a cap.*

Proof. Since caps remain caps through affine transformations λA is a cap. Thus we can assume that $\lambda = 1$. For every $c \in \mathbb{F}_q$ define v_c as the number of elements $a \in A$ such that $a \cdot y = c$. The SET of elements $v \in V$ satisfying $v \cdot y = c$ forms a subspace of $\mathbb{F}_q^{k-1}$. Now since the SET of elements $a \in A$ with $a \cdot y = c$ is a subset of both A and $AG(k-1,q)$ so $v_c \leq C(k-1,q)$, since $C(k-1,q)$ is the maximum cap size. It follows from the definition of $u(\lambda)_y$ that

$$u(\lambda)_y = |\sum_{c \in \mathbb{F}_q} v_c \zeta^c|$$

$$= \sum_{c \in \mathbb{F}_q} (C(k-1,q) - v_c)\zeta^c|$$

since $\sum_{c \in \mathbb{F}_q} \zeta^c = 0$ then $C(k-1,q) \sum_{c \in \mathbb{F}_q} \zeta^c = 0$. so by the triangle inequality

$$u(\lambda)_y \leq \sum_{c \in \mathbb{F}_q} (C(k-1,q) - v_c) = qC(k-1,q) - |A|$$

Since $\sum_{c \in \mathbb{F}_q} v_c = |A|$. □

Theorem 5.12. *Let $0 \neq \lambda \in \mathbb{F}_q$ Then*

$$||u(\lambda)||^2 = |A|(Q - |A|)$$

Proof.

$$||u(\lambda)||^2 = \sum_{y \in V \setminus \{0\}} u(\lambda)_y^2$$

$$= \sum_{y \in V} |\sum_{a \in A} \zeta^{(\lambda a) \cdot y}|^2 - |\sum_{a \in A} \zeta^{(\lambda a) \cdot 0}|^2$$

$$= \sum_{y \in V} |\sum_{a \in A} \zeta^{(\lambda a) \cdot y}|^2 - |A|^2$$

Now by a similar argument as in the proof of theorem 5.5

$$\sum_{y \in V} |\sum_{a \in A} \zeta^{(\lambda a) \cdot y}|^2 = Q|A|$$

so

$$||u(\lambda)||^2 = |A|(Q - |A|)$$

□

Definition 5.13. $c(k,q) = \frac{C(k,q)}{q^k}$

This simple substitution makes the following Theorem much easier. This is where we get our upper bound on cap size.

Theorem 5.14. *Choose A such that $|A| = C(k,q)$, in other words, choose A to be a maximal cap.* $(c(k-1,q) - c(k,q))^2 \geq c(k,q)(1 - c(k,q))/(q^k - 1)$

Proof. First $u(\lambda)_y \leq c(k-1,q)Q - |A| = c(k-1,q)q^k - q^k c(k,q)$ so we have

$$u(\lambda)_y \leq q^k(c(k-1,q) - c(k,q)$$

so

$$\sum_{y \in V \setminus \{0\}} (u(\lambda)_y)^2 \leq \sum_{y \in V \setminus \{0\}} q^k(c(k-1,q) - c(k,q)$$

$$||u(\lambda)||^2 \leq q^{2k}(c(k-1,q) - c(k,q))$$

now since $||u(\lambda)||^2 = |A|(Q - |A|) = q^k c(k,q)(q^k - q^k c(k,q))$,

$$q^{2k} c(k,q)(1 - c(k,q)) \leq q^{2k}(c(k-1,q) - c(k,q))$$

□

References

[1] J. Bierbrauer, Y. Edel. Bounds on affine caps. 2000.