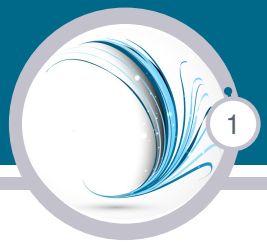
Mahidol University International College

The Cap Set Problem

Elaine Wong

November 16, 2016

Outline of Talk

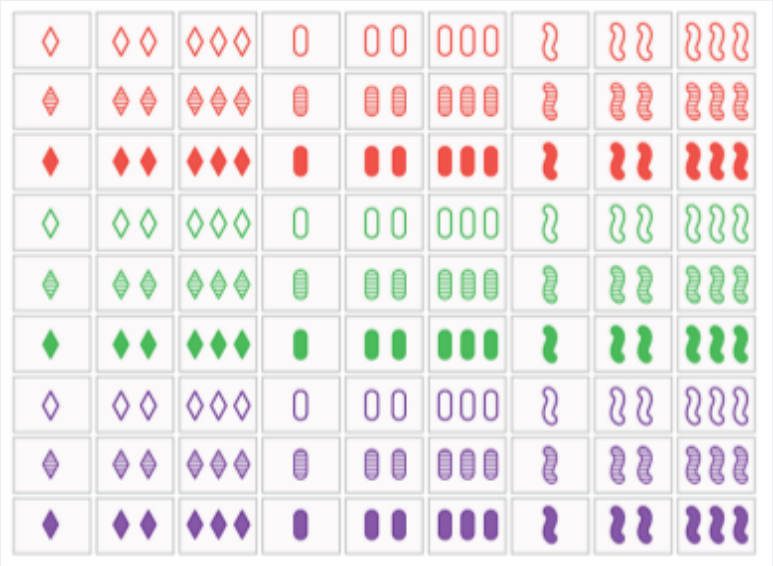


Set

Deck of Cards

Each card contains four attributes (color, shape, shading, number). Each attribute has three variations. How many cards are there?

The Full Deck



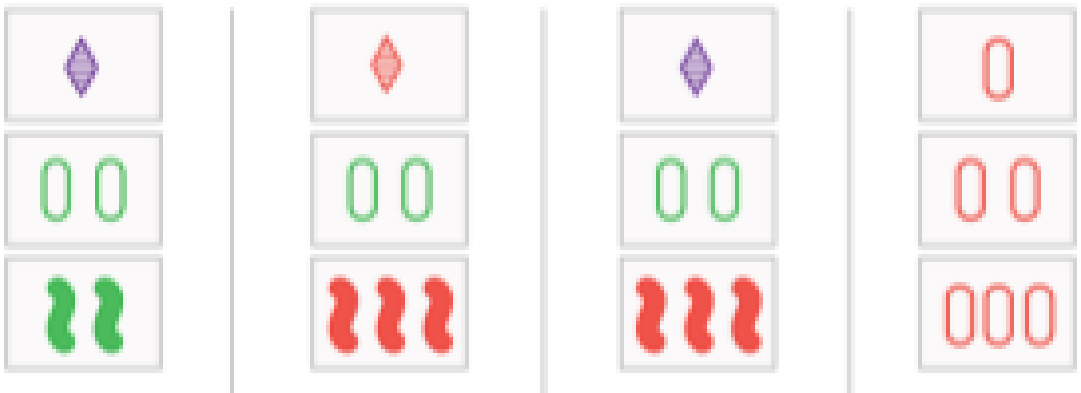
Set Game

Definition (Set)

A **set** consists of three cards such that each attribute is all the SAME on each card or all DIFFERENT on each card.

Therefore, all four of the following statements must hold for the collection of three cards to be considered a 'set':

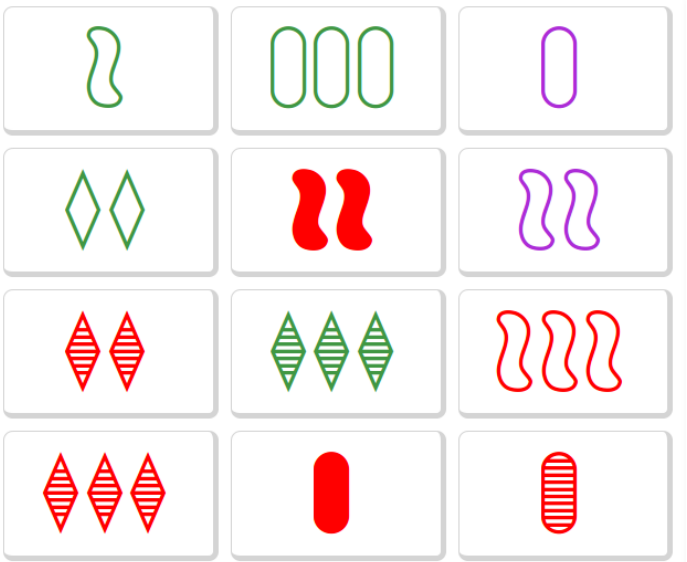
- They all have the same shape, or three different shapes.
- They all have the same color, or three different colors.
- They all have the same shading, or three different shadings.
- They all have the same number, or three different numbers.



Set Game

Directions (Falco, 1974)

Given that a single card contains all four attributes and that each attribute has three different variations, find as many sets as you can in a subset of the full deck (a collection of 12 cards is usually used).



Set Game

Observation

Sets do not always occur.

- Example: Three cards that contain a repeating attribute.
- Is there a way that you can choose a collection of cards so that you can always safely avoid a set?

Cap Sets in Set

A collection of cards with no set is called a cap* set.

*Early known usuages of the word 'cap' in Segre (1967) and Hill (1978).

Set Game

Question 1

How big is the largest cap set in the game Set?

Answer: 20 (Brute Force Computer Search)

Question 2

How big is the largest cap set if there are n attributes instead of 4?

Answer: (Pellegrino, 1971) 1, 2, 4, 9, 20, 45, 112 (OEIS A090245)

Encoding

Fun Game → Math Symbols → Solve Problems

1. Cards

Red = 0, Solid = 2, Squiggle = 1, Number = 1

Green = 1, Striped = 1, Diamond = 2, Number = 2

Purple = 2, Blank = 0, Oval = 0, Number = 0

2. Rewrite as Points in $\mathbb{Z}_3^4$

$$(0,2,1,1) \quad (1,1,2,2) \quad (2,0,0,0)$$

3. Set or not?
   Observe that three points correspond to a set precisely when they lie on the same line in $\mathbb{Z}_3^4$ as is the case with these three cards.

Cap Set

Cap Sets in $\mathbb{Z}_3^4$

A cap set is a collection of points in $\mathbb{Z}_3^4$ that contain no lines.

Definition (Cap Set)

A cap set in the vector space F_3^n over the finite field F_3 of three elements is a subset A of F_3^n that does NOT contain any lines $\{a, a+d, a+2d\}$, where $a, d \in F_3^n$ and $d \neq 0$.

Observe that for any $a, b, c \in A$, $a+b+c=0$ (equivalently, $a+b=2c$) has NO solutions except when $a=b=c$.

Cap Set

Notation

$F_3 := \{0, 1, 2\}$ is the field of integers modulo 3
$|S| :=$ number of elements of a finite set S

Theorem (Ellenberg and Gijswijt, 2016)

Suppose A is a cap set of F_3^n. Then

$$|A| \leq C \cdot 2.756^n \text{ for some constant } C.$$

People

The Efforts of Many

Author(s)	Bound*	Year
Brown-Buhler [BB]	3^n	1982
Meshulam [M]	$\frac{3^n}{n}$	1995
Bateman-Katz [BK]	$\frac{3^n}{n^{1+\epsilon}}$	2011
Croot-Lev-Pach [CLP]	–	2016
Ellenberg-Gijswijt [EG]	2.756^n	2016

*All bounds up to a factor of a constant C.

The Main Result

Suppose $\binom{n}{k}_2$ denotes the coefficient of x^k in $(1+x+x^2)^n$.

Theorem (Ellenberg and Gijswijt, 2016)

Suppose A is a cap set of F_3^n. Then

$$|A| \leq 3 \sum_{k=0}^{\lfloor \frac{2n}{3} \rfloor} \binom{n}{k}_2.$$

Computing the asymtotic behavior (for large n) will give the desired upper bound of $\mathcal{O}(2.756^n)$.

Polynomials on F_3^n

Vector Space of Polynomials

A vector space of polynomials on F_3^n has the basis

$$\{x_1^{\alpha_1} \dots x_n^{\alpha_n} \mid 0 \leq \alpha_i \leq 2\}.$$

The dimension of this space is 3^n.

Subspace S_d of Polynomials

A subspace S_d consisting of the set of polynomials of total degree at most d has the basis

$$\{x_1^{\alpha_1} \dots x_n^{\alpha_n} \mid 0 \leq \alpha_i \leq 2, \alpha_1 + \dots + \alpha_n \leq d\}.$$

The dimension of this space is $\sum_{k=0}^{d} \binom{n}{k}_2$.

The *Right* Vector Space of Polynomials

How are the cap set and set of polynomials related to each other? What is the right balance of polynomials that would correctly associate with a cap set?

Subspace V of polynomials vanishing on A

$$V := \{P(x_1, \ldots, x_n) \mid \deg(P) \leq d, P(x) = 0 \text{ for all } x \in A\}$$

$$\dim V \geq \dim S_d - |A|$$

This gives the lower bound of $|A|$ which is not what we are looking for.

Subspace V_c of polynomials vanishing on A^c

$$V_c := \{P(x_1, \ldots, x_n) \mid \deg(P) \leq d, P(x) = 0 \text{ for all } x \in F_3^n - A\}$$

$$\dim V_c \geq \dim S_d - |F_3^n - A|$$

This is a little bit better.

Proof

Steps of Proof

1. The Bound for $|A|$
2. The Crucial Observation of [CLP]
3. Optimization
4. Asymptotic Behavior

The Bound for $|A|$

Observe: $\dim V_c \geq \dim S_d - |F_3^n - A|$
$= \dim S_d - (3^n - |A|)$
$= |A| - (3^n - \dim S_d)$

The Bound for |A|

Rearrange the previous inequality to get

$$|A| \leq |\Sigma_d| + (3^n - \dim S_d)$$

where Σ_d is the maximal support of $P \in V_c$ giving the bound $|\Sigma_d| \geq \dim V_c$ (contradicts 'maximal' otherwise).

The Bound for |A|

We now use the fact that A is a capset.

Property of Cap Sets

For all $a, b, c \in A$ with $b \neq c$, $a + b + c \neq 0$.

Observe $\{-b - c \mid b, c \in A, b \neq c\} \subset F_3^n - A$ so the polynomial $P \in V_c$ must vanish over that set.

Vanishing Property

$P(-b - c) = 0$ whenever $b, c \in A$ and $b \neq c$

The polynomial $P(-b - c)$ contains $2n$ variables $b_1, \ldots, b_n; c_1, \ldots, c_n$ and is a sum of monomials of the form

$$(b_1^{\beta_1} \ldots b_n^{\beta_n}) \cdot (c_1^{\gamma_1} \ldots c_n^{\gamma_n}),$$

where $\beta_1 + \ldots + \beta_n + \gamma_1 + \ldots + \gamma_n \leq d$.

The Crucial Observation of [CLP]

Suppose two non-overlapping sets of n elements each are pairwise linked (so we have n pairs). Given that we can color at most d elements red, either set 1 will have at most $d/2$ colored red or else set 2 will. In either case, we can separate the red group neatly.

Rewriting Monomials

Every monomial $(b_1^{\beta_1} \dots b_n^{\beta_n}) \cdot (c_1^{\gamma_1} \dots c_n^{\gamma_n})$ where $\beta_1 + \dots + \beta_n + \gamma_1 + \dots + \gamma_n \leq d$ can be written as one of the following:

1. $m(b)m'(c)$ with deg $m(b) \leq d/2$
2. $m(c)m'(b)$ with deg $m(c) \leq d/2$

The Crucial Observation of [CLP]

Since every monomial in $P(-b-c)$ can be broken down this way, a little rearranging is all that is necessary to be able to measure the size of the support of $P \in V_c$. Hence, we have our brilliant observation:

Observation [CLP]

$$P(-b-c) = \sum_{m \in S_{d/2}} m(b) P_m(c) + \sum_{m \in S_{d/2}} m(c) P_m(b)$$

P_m is the polynomial with the corresponding monomial factored out.

The Crucial Observation [CLP]

Consider an $|A| \times |A|$ matrix, D, whose rows and columns are indexed by the members of A such that the (b, c) entry is $P(-b - c)$.

Then D is a diagonal matrix. The observation [CLP] also shows that D can be decomposed into a sum of $|S_{d/2}| + |S_{d/2}|$ matrices, each of rank 1 (since all rows (columns) are proportional to each other).

Hence $\text{rank}(D) \leq 2|S_{d/2}|$, that is, it can have at most $2|S_{d/2}|$ non-zero diagonal entries. In other words, $P(-b - b) = P(b) \neq 0$ for at most $2|S_{d/2}|$ members of $b \in A$.

Support of $P \in V_c$

The size of the support of every $P \in V_c$ is at most $2|S_{d/2}|$, i.e.

$$|\Sigma_d| \leq 2|S_{d/2}|$$

Optimization

We can now simplify the bound for $|A|$ for optimization:

$$|A| \leq |\Sigma_d| + (3^n - \dim S_d) \leq 2|S_{d/2}| + 3^n - |S_d|$$

This is valid for **every** d. Minimizing the right hand side gives the optimal value $d = \frac{4n}{3}$ (Zeilberger). Assuming that n is a multiple of 3, we now have a bound for $|A|$ which will give the result of the theorem [EG].

The Bound of |A| Optimized

$$|A| \leq 2|S_{2n/3}| + 3^n - |S_{4n/3}|$$

Optimization

Theorem (Ellenberg and Gijswijt, 2016)

Suppose A is a cap set of F_3^n. Then $|A| \leq 3 \sum_{k=0}^{\lfloor \frac{2n}{3} \rfloor} \binom{n}{k}_2$.

Proof.

For convience, we assume n is a multiple of 3. Our work above shows that $|A| \leq 2|S_{2n/3}| + 3^n - |S_{4n/3}|$. We now simplify the last two terms using symmetric properties of the trinomial:

$$3^n - |S_{4n/3}| = \sum_{k=0}^{2n} \binom{n}{k}_2 - \sum_{k=0}^{\frac{4n}{3}} \binom{n}{k}_2 = \sum_{k=0}^{\frac{2n}{3}} \binom{n}{k}_2 - \binom{n}{\frac{2n}{3}}_2$$

Thus, $|A| \leq 3 \sum_{k=0}^{\frac{2n}{3}} \binom{n}{k}_2 - \binom{n}{\frac{2n}{3}}_2 \leq 3 \sum_{k=0}^{\frac{2n}{3}} \binom{n}{k}_2$, as desired.

□

Asymptotic Behavior

Trinomial Coefficient Reformulation for Large n (Andrews, 1990)

$$\binom{n}{k}_2 \sim \frac{n!}{p_0!p_1!p_2!}$$

where p_0, p_1, p_2 are the numbers of powers $0, 1, 2$ respectively of the x^k term of $(1 + x + x^2)^n$.

Using densities $\pi_0, \pi_1, \pi_2 \geq 0$ where $\pi_0 + \pi_1 + \pi_2 = 1$, we can rewrite p_0, p_1, p_2 in terms of n:

$$p_0 = \pi_0 n + o(1),\ p_1 = \pi_1 n + o(1),\ p_2 = \pi_2 n + o(1)$$

The asymptotic behavior of the sum of trinomials will be achieved by following the asymptotics of the biggest term.

Asymptotic Behavior

Stirling's Approximation

$$n! \approx \left(\frac{n}{e}\right)^n$$

Stirling's Approximation gives us:

$$\frac{n!}{p_0!p_1!p_2!} \sim \frac{n!}{(\pi_0 n)!(\pi_1 n)!(\pi_2 n)!} \approx \frac{1}{(\pi_0^{\pi_0}\pi_1^{\pi_1}\pi_2^{\pi_2})^n}$$

Writing this in exponential form makes it easier to maximize:

$$\begin{aligned}\frac{1}{(\pi_0^{\pi_0}\pi_1^{\pi_1}\pi_2^{\pi_2})^n} &= \left(\left(\frac{1}{\pi_0}\right)^{\pi_0}\left(\frac{1}{\pi_1}\right)^{\pi_1}\left(\frac{1}{\pi_2}\right)^{\pi_2}\right)^n \\ &= \exp\left(\log\left(\left(\frac{1}{\pi_0}\right)^{\pi_0}\left(\frac{1}{\pi_1}\right)^{\pi_1}\left(\frac{1}{\pi_2}\right)^{\pi_2}\right)^n\right) \\ &= \exp\left(n\cdot(\pi_0\log(1/\pi_0)+\pi_1\log(1/\pi_1)+\pi_2\log(1/\pi_2))\right)\end{aligned}$$

Asymptotic Behavior

Define the function

$$E(\pi_0, \pi_1, \pi_2) := \pi_0 \log(1/\pi_0) + \pi_1 \log(1/\pi_1) + \pi_2 \log(1/\pi_2).$$

Subject to the constraints $\pi_0, \pi_1, \pi_2 \geq 0$, $\pi_0 + \pi_1 + \pi_2 = 1$ and $\pi_2 + 2\pi_3 \leq \frac{2}{3}$, we have that E achieves the maximum value of approximately 1.013455 (Tao), which gives

$$|A| \leq e^{(1.1013n + o(1))} = \mathcal{O}(2.756^n)$$

as desired.

References

- [CLP] Ernie Croot, Vsevolod Lev, and Péter Pál Pach, *Progression-Free Sets in $\mathbb{Z}_4^n$ are Exponentially Small*, Submitted May 2016, http://arxiv.org/abs/1605.01506
- [EG] Jordan S. Ellenberg and Dion Gijswijt, *On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression*, Submitted May 2016, http://arxiv.org/abs/1605.09223
- Terence Tao, *A symmetric formulation of the Croot-Lev-Pack-Ellenberg-Gijswijt capset bound*, May 18, 2016, https://terrytao.wordpress.com/2016/05/18/a-symmetric-formulation-of-the-croot-lev-pach-ellenberg-gijswijt-capset-bound/
- Doron Zeilberger, *A Motivated Rendition of the Ellenberg-Gijswijt Gorgeous Proof that the Largest Subset of F_3^n with No Three-Term Arithmetic Progression is $O(c^n)$, with $c \approx 2.755$*, July 6, 2016, http://www.math.rutgers.edu/$\sim$zeilberg/mamarim/mamarimhtml/f3n.html

Thank you!