A Dream of Set Systems; or A Song of Splitting and Splittability vol. VII

B. Frederickson, S. Mathers, H. T. Yan

27 July 2018

Boise State University

Introduction

What is splitting?

Definition

A set A is said to split a set B if half of the elements of B are in A and half are not. We allow rounding if B has an odd number of elements.

What is splitting?

Definition

A set A is said to split a set B if half of the elements of B are in A and half are not. We allow rounding if B has an odd number of elements.

Example

$$\{1, 3\} \text{ splits } \{1, 2, 3, 4\}\ .$$

What is splitting?

Definition

A set A is said to split a set B if half of the elements of B are in A and half are not. We allow rounding if B has an odd number of elements.

Example

$$\{1,3\} \text{ splits } \{1,2,3,4\}\ .$$

$$\{1,2,5,6\} \text{ splits } \{1,2,3,4\}\ .$$

What is splitting?

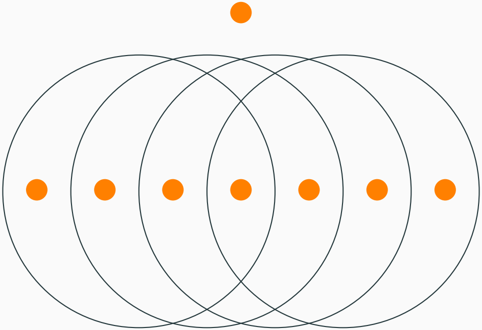
Definition

Suppose $\mathcal{F} = \{A_1, A_2, \ldots, A_n\} \subseteq \mathcal{P}([k])$ is a family of sets. We say that $\mathcal{F}$ is a splitting family if for each set $B \in \mathcal{P}([k])$, there exists a set $A_i \in \mathcal{F}$ such that A_i splits B.

What is splitting?

Definition

Suppose $\mathcal{F} = \{A_1, A_2, \ldots, A_n\} \subseteq \mathcal{P}([k])$ is a family of sets. We say that $\mathcal{F}$ is a splitting family if for each set $B \in \mathcal{P}([k])$, there exists a set $A_i \in \mathcal{F}$ such that A_i splits B.



A splitting family

What is splitting?

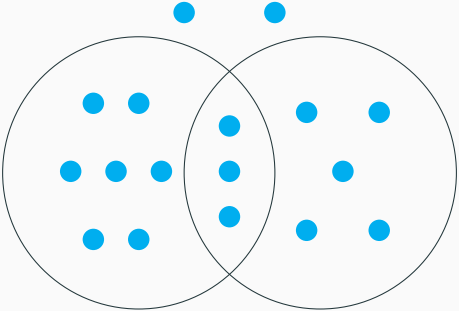
Definition

Suppose $\mathcal{B} = \{B_1, B_2, \ldots, B_n\} \subseteq \mathcal{P}([k])$ is a family of sets. We say that $\mathcal{B}$ is a splittable family if there exists a set $A \in \mathcal{P}([k])$ that simultaneously splits each element of $\mathcal{B}$.

What is splitting?

Definition

Suppose $\mathcal{B} = \{B_1, B_2, \ldots, B_n\} \subseteq \mathcal{P}([k])$ is a family of sets. We say that $\mathcal{B}$ is a splittable family if there exists a set $A \in \mathcal{P}([k])$ that simultaneously splits each element of $\mathcal{B}$.

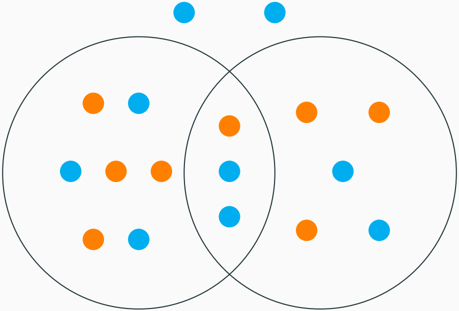


A splittable family

What is splitting?

Definition

Suppose $\mathcal{B} = \{B_1, B_2, \ldots, B_n\} \subseteq \mathcal{P}([k])$ is a family of sets. We say that $\mathcal{B}$ is a splittable family if there exists a set $A \in \mathcal{P}([k])$ that simultaneously splits each element of $\mathcal{B}$.



A splittable family

Splitting families

The smallest family: $\sigma(k)$ and $\tau(n)$

Definition

$\sigma(k) :=$ the minimum number of sets needed to split any subset of $[k]$.

The smallest family: $\sigma(k)$ and $\tau(n)$

Definition

$\sigma(k) :=$ the minimum number of sets needed to split any subset of $[k]$.
$\tau(n) :=$ the maximum number of points split by n sets.

The smallest family: $\sigma(k)$ and $\tau(n)$

Definition

$\sigma(k) :=$ the minimum number of sets needed to split any subset of $[k]$.
$\tau(n) :=$ the maximum number of points split by n sets.

- By definition, σ and τ are inverse to each other.

The smallest family: $\sigma(k)$ and $\tau(n)$

Definition

$\sigma(k) :=$ the minimum number of sets needed to split any subset of $[k]$.
$\tau(n) :=$ the maximum number of points split by n sets.

- By definition, σ and τ are inverse to each other.
- Coppersmith showed that a set of size k has a splitting family of size $\lceil \frac{k}{2} \rceil$.

The smallest family: $\sigma(k)$ and $\tau(n)$

Definition

$\sigma(k) :=$ the minimum number of sets needed to split any subset of $[k]$.
$\tau(n) :=$ the maximum number of points split by n sets.

- By definition, σ and τ are inverse to each other.
- Coppersmith showed that a set of size k has a splitting family of size $\lceil \frac{k}{2} \rceil$.
- Thus $\sigma(k) \leq \lceil \frac{k}{2} \rceil$ and $\tau(n) \geq 2n$.

The smallest family: $\sigma(k)$ and $\tau(n)$

Definition

$\sigma(k) :=$ the minimum number of sets needed to split any subset of $[k]$.
$\tau(n) :=$ the maximum number of points split by n sets.

- By definition, σ and τ are inverse to each other.
- Coppersmith showed that a set of size k has a splitting family of size $\lceil \frac{k}{2} \rceil$.
- Thus $\sigma(k) \leq \lceil \frac{k}{2} \rceil$ and $\tau(n) \geq 2n$.
- Can we find a splitting family of fewer elements?

The Coppersmith construction

Given k, Coppersmith showed that a collection $\mathcal{A}$ of size $\lceil \frac{k}{2} \rceil$ given as follows is a splitting family:

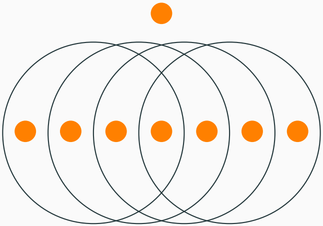
$$\mathcal{A} = \bigcup_{i=1}^{\lceil \frac{k}{2} \rceil} \{i, \ldots, i + \lceil \tfrac{k}{2} \rceil\} \, .$$

The Coppersmith construction

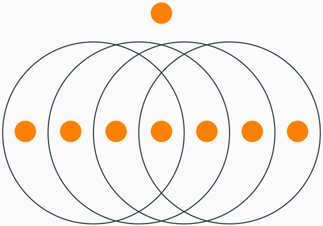
Given k, Coppersmith showed that a collection $\mathcal{A}$ of size $\lceil \frac{k}{2} \rceil$ given as follows is a splitting family:

$$\mathcal{A} = \bigcup_{i=1}^{\lceil \frac{k}{2} \rceil} \{i, \ldots, i + \lceil \tfrac{k}{2} \rceil\} \, .$$

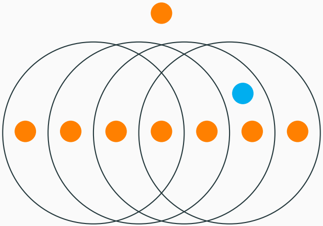
Example The Coppersmith construction for $k = 8$.



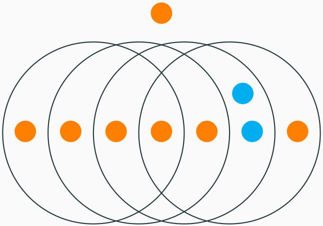
Can we add points to the Coppersmith construction?



Can we add points to the Coppersmith construction?



Can we add points to the Coppersmith construction?



Coppersmith Inextendability Theorem

Coppersmith Inextendability Theorem

Theorem

Given a Coppersmith arrangement, adding an additional point to it always yields a nonsplitting family.

The volume method

- We want to find a lower bound on $\sigma(k)$, that is, the size of a splitting family of $[k]$.

The volume method

- We want to find a lower bound on $\sigma(k)$, that is, the size of a splitting family of $[k]$.
- The volume method considers the number of sets N that need to be split, as well as the maximum number v of sets that one splitter can split.

The volume method

- We want to find a lower bound on $\sigma(k)$, that is, the size of a splitting family of $[k]$.
- The volume method considers the number of sets N that need to be split, as well as the maximum number v of sets that one splitter can split.
- Thus a lower bound can be given by N/v.

The volume method

- We want to find a lower bound on $\sigma(k)$, that is, the size of a splitting family of $[k]$.
- The volume method considers the number of sets N that need to be split, as well as the maximum number v of sets that one splitter can split.
- Thus a lower bound can be given by N/v.
- We have $N = |\mathcal{P}([k])| = 2^k$.

The volume method

- We want to find a lower bound on $\sigma(k)$, that is, the size of a splitting family of $[k]$.
- The volume method considers the number of sets N that need to be split, as well as the maximum number v of sets that one splitter can split.
- Thus a lower bound can be given by N/v.
- We have $N = |\mathcal{P}([k])| = 2^k$.
- A splitter with $k/2$ elements splits the most sets of $\mathcal{P}([k])$.

The volume method

- We want to find a lower bound on $\sigma(k)$, that is, the size of a splitting family of $[k]$.
- The volume method considers the number of sets N that need to be split, as well as the maximum number v of sets that one splitter can split.
- Thus a lower bound can be given by N/v.
- We have $N = |\mathcal{P}([k])| = 2^k$.
- A splitter with $k/2$ elements splits the most sets of $\mathcal{P}([k])$.
- We compute and use Stirling's approximation to obtain $v = \binom{k}{k/2} \approx 2^k/\sqrt{k}$.

The volume method

- We want to find a lower bound on $\sigma(k)$, that is, the size of a splitting family of $[k]$.
- The volume method considers the number of sets N that need to be split, as well as the maximum number v of sets that one splitter can split.
- Thus a lower bound can be given by N/v.
- We have $N = |\mathcal{P}([k])| = 2^k$.
- A splitter with $k/2$ elements splits the most sets of $\mathcal{P}([k])$.
- We compute and use Stirling's approximation to obtain $v = \binom{k}{k/2} \approx 2^k/\sqrt{k}$.
- Thus our lower bound is $N/v = \sqrt{k}$.

The volume method

- We want to find a lower bound on $\sigma(k)$, that is, the size of a splitting family of $[k]$.
- The volume method considers the number of sets N that need to be split, as well as the maximum number v of sets that one splitter can split.
- Thus a lower bound can be given by N/v.
- We have $N = |\mathcal{P}([k])| = 2^k$.
- A splitter with $k/2$ elements splits the most sets of $\mathcal{P}([k])$.
- We compute and use Stirling's approximation to obtain $v = \binom{k}{k/2} \approx 2^k/\sqrt{k}$.
- Thus our lower bound is $N/v = \sqrt{k}$.
- Using tighter approximations, we found a better bound $\sqrt{\frac{\pi k}{8}}$.

Other splitting families

Our bound isn't all that tight, so is there a different type of splitting family of size n that splits more than $2n$ points?

Other splitting families

Our bound isn't all that tight, so is there a different type of splitting family of size n that splits more than $2n$ points?

n	$\tau(n)$
1	2
2	4
3	**6**
4	**8**
5	**10**
6	**12**
7	$14 \leq \tau(7) \leq$ **24** $<$ **124**
8	$16 \leq \tau(8) \leq$ **46** $<$ **162**
$\vdots$	$\vdots$
n	$2n \leq \tau(n) \leq \boldsymbol{\frac{8}{\pi} n^2}$

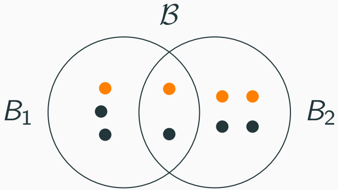
Conjecture

We conjecture that the minimum size of a splitting family on k elements is $\lceil \frac{k}{2} \rceil$. In other words, $\sigma(k) = \lceil \frac{k}{2} \rceil$ and $\tau(n) = 2n$.

Splittable families

Definition

Suppose $\mathcal{B} = \{B_1, B_2, \ldots, B_n\} \subseteq \mathcal{P}([k])$ is a family of sets. We say that $\mathcal{B}$ is a splittable family if there exists a set $A \in \mathcal{P}([k])$ that simultaneously splits each element of $\mathcal{B}$.



Central question

Given a fixed number of sets, which arrangement yields the least splitters? The most?

Results from REU 14 found the lower bound for the least number of splitters on two sets to be asymptotic to $2^k/k$. We improve upon this by giving the exact arrangements, and thus, proving $2^k/k$ is tight.

A family $\mathcal{B} = \{B_1, \ldots, B_n\}$ of subsets of $[k]$ has the maximal number of splitters, 2^k, iff $|B_i| \in \{0, 1\}$ for each $i \in [n]$.

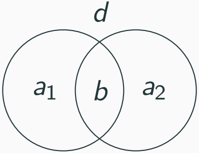
Minimum number of splitters

This question is much harder than the maximal version and has more variation depending on the number of sets.

Minimum number of splitters

This question is much harder than the maximal version and has more variation depending on the number of sets. We will give the full result for families with two sets and conjectures on families with three sets.

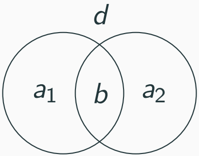
Let $\mathcal{B} = \{B_1, B_2\}$ be a family of subsets of $[k]$. Label the cardinalities of the Venn regions as follows:



We denote the above arrangement by the 4-tuple (a_1, b, a_2, d).

Counting splitters on two sets

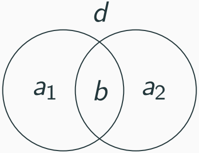
Let $\mathcal{B} = \{B_1, B_2\}$ be a family of subsets of $[k]$. Label the cardinalities of the Venn regions as follows:



We denote the above arrangement by the 4-tuple (a_1, b, a_2, d). We denote the number of splitters by $\text{split}(a_1, b, a_2, d)$.

Counting splitters on two sets

Let $\mathcal{B} = \{B_1, B_2\}$ be a family of subsets of $[k]$. Label the cardinalities of the Venn regions as follows:

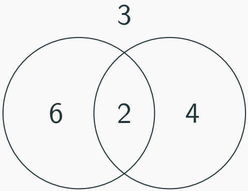


We denote the above arrangement by the 4-tuple (a_1, b, a_2, d). We denote the number of splitters by $\mathrm{split}(a_1, b, a_2, d)$. Then the number of splitters of $\mathcal{B}$ is

$$\mathrm{split}(a_1, b, a_2, d) = 2^d \sum_{\epsilon_1=-1}^{1} \sum_{\epsilon_2=-1}^{1} \sum_{i=0}^{b} \binom{a_1}{\frac{a_1+b+\epsilon_1}{2} - i} \binom{b}{i} \binom{a_2}{\frac{a_2+b+\epsilon_2}{2} - i}.$$

Example calculation

Suppose you have the following arrangement,



We then have

$$2^3 \sum_{i=0}^{2} \binom{6}{\frac{6+2}{2} - i} \binom{2}{i} \binom{4}{\frac{4+2}{2} - i} = 2880$$

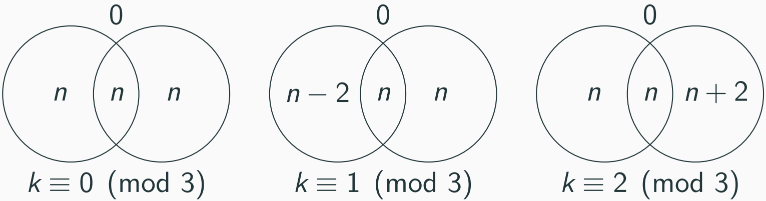
splitters of this arrangement.

Minimum number of splitters on two sets

Theorem

The number of splitters is minimized for

$$\begin{aligned} &(\quad n,\ n,\ n,\ 0), \quad \textit{when}\ k \equiv 0 \pmod 3,\\ &(n-2,\ n,\ n,\ 0), \quad \textit{when}\ k \equiv 1 \pmod 3,\\ &(n+2,\ n,\ n,\ 0), \quad \textit{when}\ k \equiv 2 \pmod 3. \end{aligned}$$



Minimum number of splitters on two sets

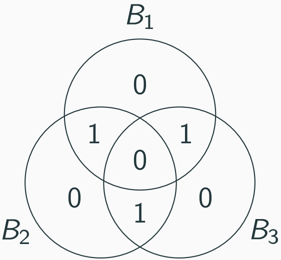
Proof outline.

- Slightly altering one of the minimal arrangements by moving elements between regions increases the number of splitters.
- There exists a partial injection between the minimal arrangement and the new arrangement.
- Ignoring the splitters in the injection, we can show that the resulting number of splitters is smaller for the minimal arrangement.
- Any arrangement can be reached by a sequence of such alterations.

□

Three sets

Unsplittable arrangements exist on three sets. For example,



Thus, the question is more interesting if we ask for the arrangement with the minimum number of splitters given that it has at least one splitter. It turns out that the minimal arrangements resemble the unsplittable arrangements on three sets rather than the minimal arrangements on two sets.

Experimental results

Let $A(k)$ denote the least positive number of splitters an arrangement of k points on 3 sets could have. Data suggests that $A(k)$ follows the recurrence

$$\frac{A(k+1)}{A(k)} = \begin{cases} 2 - \frac{1}{\lfloor k/6 \rfloor + 1}, & k \text{ even} \\ 2, & k \text{ odd} \end{cases}$$

- If true, this is asymptotic to $2^k / k^{3/2}$
- For two sets, it is asmyptotic to $2^k / k$
- For one set, it is asmyptotic to $2^k / k^{1/2}$

The Splitting Game

Motivation

In the previous section, we explored "how splittable" a family of sets $\mathcal{B}$ is by counting the number of distinct sets that split $\mathcal{B}$.

Motivation

In the previous section, we explored "how splittable" a family of sets $\mathcal{B}$ is by counting the number of distinct sets that split $\mathcal{B}$.

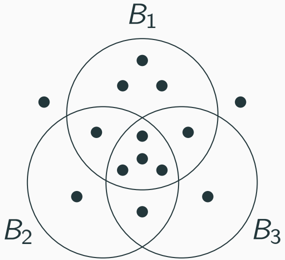
The Splitting Game aims to answer the same question in a different sense, that is:
Can $\mathcal{B}$ always be split under certain adversarial conditions?

The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \ldots, B_n\}$ of finite sets of "points".

Players take turns claiming one point until all points have been claimed.

Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.



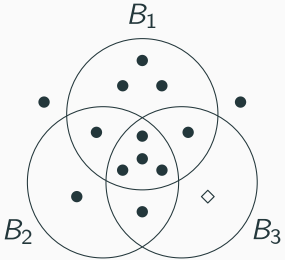
Splitter: $\diamond$
Skewer: $\star$

The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \ldots, B_n\}$ of finite sets of "points".

Players take turns claiming one point until all points have been claimed.

Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.



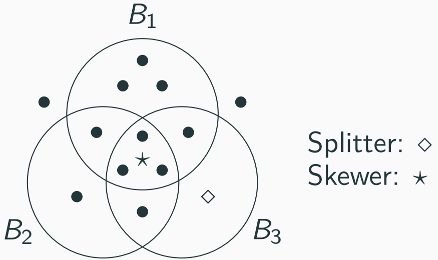
Splitter: $\diamond$
Skewer: $\star$

The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \dots, B_n\}$ of finite sets of "points".

Players take turns claiming one point until all points have been claimed.

Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.

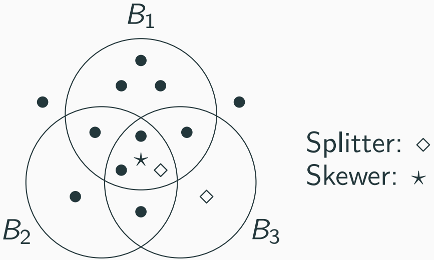


The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \ldots, B_n\}$ of finite sets of "points".

Players take turns claiming one point until all points have been claimed.

Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.

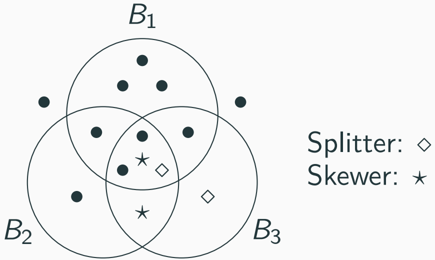


The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \ldots, B_n\}$ of finite sets of "points".

Players take turns claiming one point until all points have been claimed.

Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.

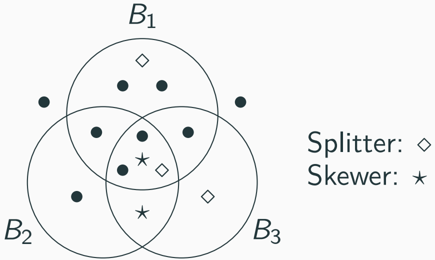


The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \ldots, B_n\}$ of finite sets of “points”.

Players take turns claiming one point until all points have been claimed.

Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.

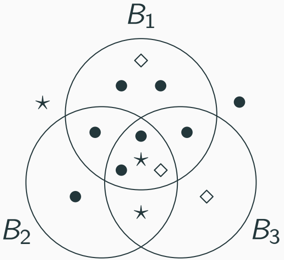


The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \ldots, B_n\}$ of finite sets of "points".

Players take turns claiming one point until all points have been claimed.

Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.



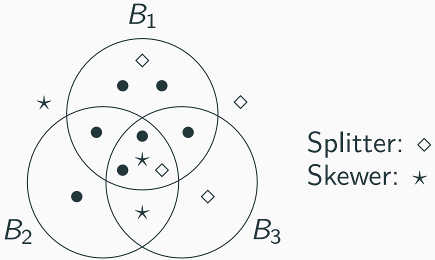
Splitter: $\diamond$
Skewer: $\star$

The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \dots, B_n\}$ of finite sets of "points".

Players take turns claiming one point until all points have been claimed.

Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.

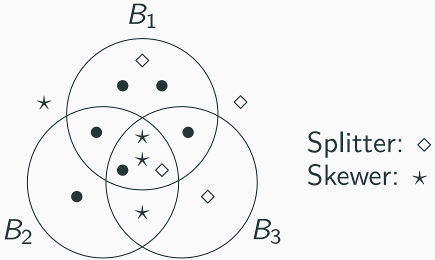


The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \ldots, B_n\}$ of finite sets of "points".

Players take turns claiming one point until all points have been claimed.

Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.

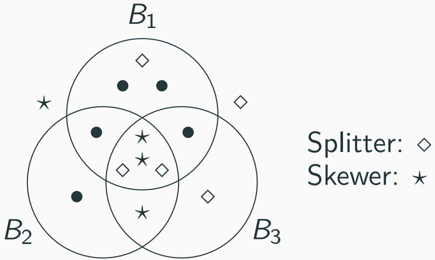


The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \ldots, B_n\}$ of finite sets of "points".

Players take turns claiming one point until all points have been claimed.

Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.

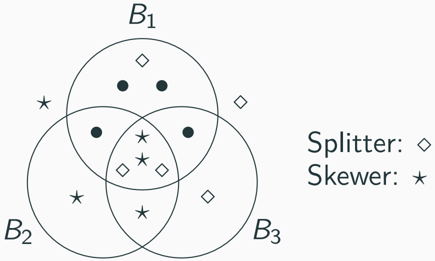


The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \ldots, B_n\}$ of finite sets of "points".

Players take turns claiming one point until all points have been claimed.

Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.

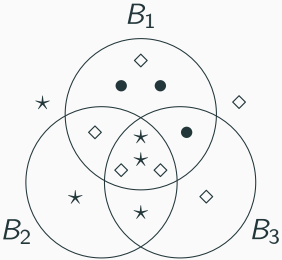


The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \ldots, B_n\}$ of finite sets of "points".

Players take turns claiming one point until all points have been claimed.

Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.



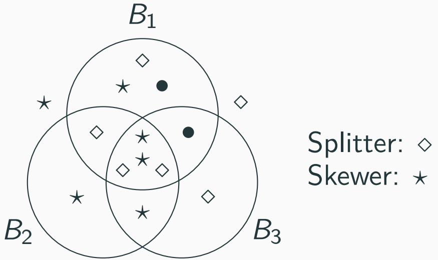
Splitter: $\diamond$
Skewer: $\star$

The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \ldots, B_n\}$ of finite sets of "points".

Players take turns claiming one point until all points have been claimed.

Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.

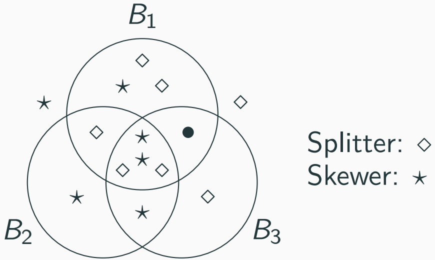


The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \ldots, B_n\}$ of finite sets of "points".

Players take turns claiming one point until all points have been claimed.

Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.

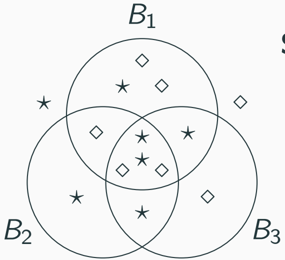


The rules of the game

The Splitting Game is played by two players, Split and Skew, on a family $\{B_1, \ldots, B_n\}$ of finite sets of "points".

Players take turns claiming one point until all points have been claimed.

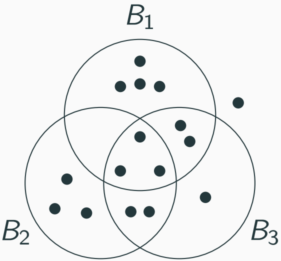
Split wins if the set of points he claimed is a splitter for $\mathcal{B}$, while Skew wins if any B_i is not split by that set.



Splitter wins!

Splitter: $\diamond$
Skewer: $\star$

Your turn



Zermelo's Theorem

In games like this, one of the players is guaranteed to have a winning strategy. This means that there exists a strategy for one of the players such that, if they play accordingly, then the other player has no way to win the game.

Zermelo's Theorem

In games like this, one of the players is guaranteed to have a winning strategy. This means that there exists a strategy for one of the players such that, if they play accordingly, then the other player has no way to win the game.

If Split has a winning strategy, we say the game is strategically splittable. If Skew has a winning strategy, we say the game is strategically skewable.

Zermelo's Theorem

In games like this, one of the players is guaranteed to have a winning strategy. This means that there exists a strategy for one of the players such that, if they play accordingly, then the other player has no way to win the game.

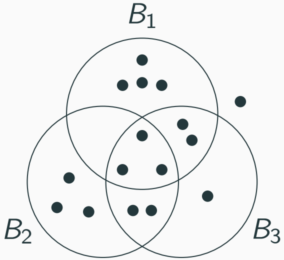
If Split has a winning strategy, we say the game is strategically splittable. If Skew has a winning strategy, we say the game is strategically skewable.

Remark.
A family being strategically splittable is a stronger condition than just being splittable. Strategically splittable families are favorable when one wishes to "divide things up evenly" without having full control of a situation.

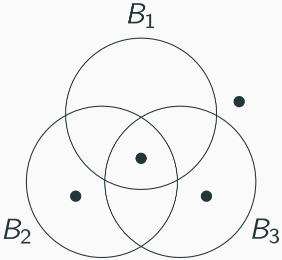
Results

Lemma (Reduction Lemma)
Games with the same parity of points in each Venn region are equivalent.

Example:

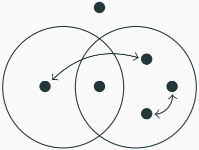


reduces to



Definition

We say that Split (or Skew) has a pairing strategy in $\mathcal{B}$ if there exists a set $\mathcal{P}$ of disjoint pairs of points such that all splitters of $\mathcal{P}$ are also splitters (or non-splitters) of $\mathcal{B}$.



Lemma (Pairing lemma)

If there exists a pairing strategy for a family, then strategic splittability is independent of:

1. *which player goes first;*
2. *how many points are in the outside region.*

Results

The reduction lemma allows us to provide a complete analysis of the game for two and three sets and determine the proportion of Split-winnable games.

Results

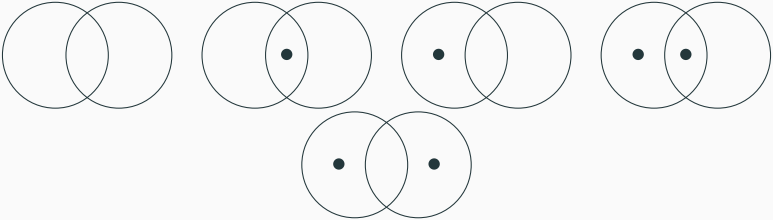
The reduction lemma allows us to provide a complete analysis of the game for two and three sets and determine the proportion of Split-winnable games.

Conveniently, there is a pairing strategy for all families with 3 sets or fewer.

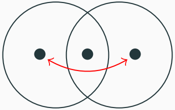
Two sets

The proportion of strategically splittable games on two sets is .875 (28/32).

Strategically splittable configurations:

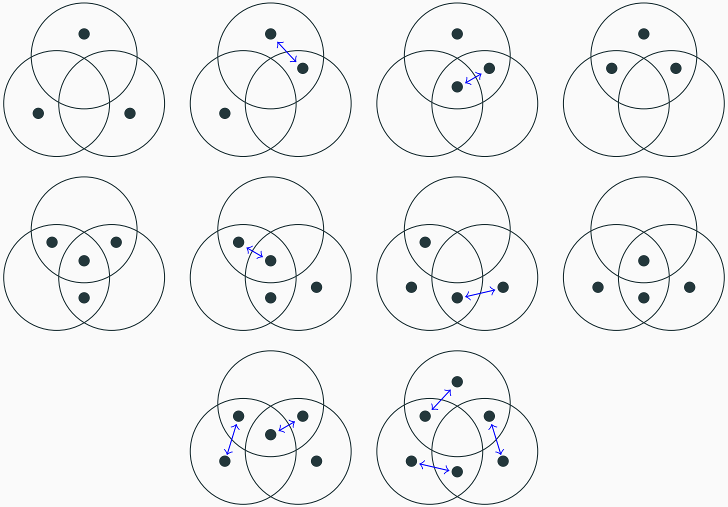


Strategically skewable configurations:

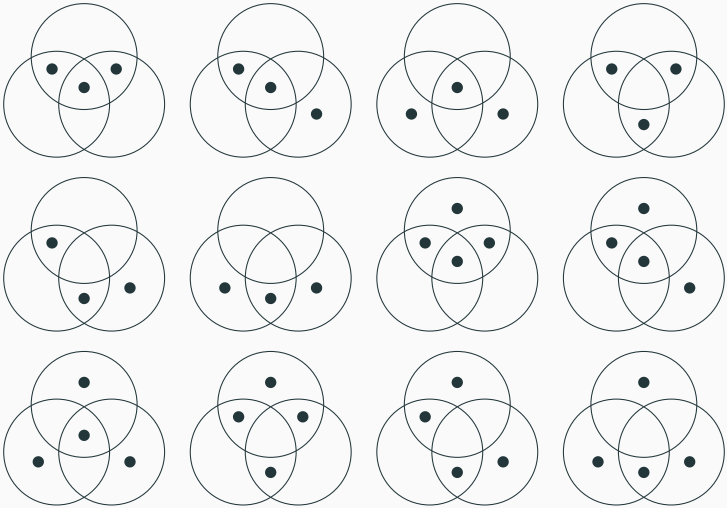


Three sets: Strategically splittable configurations

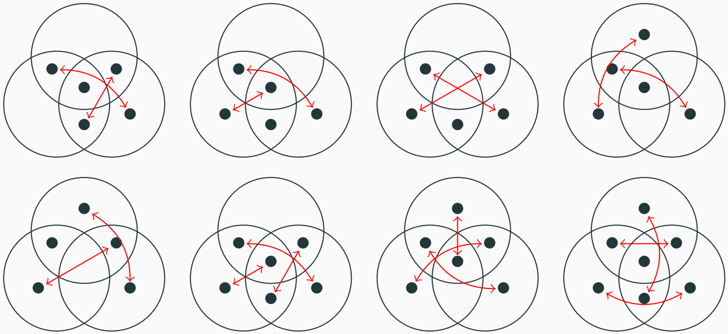
The proportion of strategically splittable games on three sets is .508 (260/512).



Three sets: Strategically skewable configurations



Three sets: Strategically skewable configurations



More sets

Theorem.
The proportion of strategically splittable games on n sets decreases monotonically as n increases.

More sets

Theorem.

The proportion of strategically splittable games on n sets decreases monotonically as n increases.

Conjecture.

That proportion tends to 0 as $n \to \infty$.

More sets

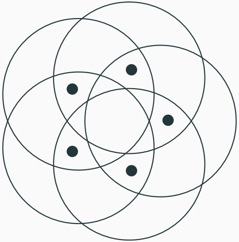
Theorem.

The proportion of strategically splittable games on n sets decreases monotonically as n increases.

Conjecture.

That proportion tends to 0 as $n \to \infty$.

A pairing strategy isn't always possible. For example, we have the following configuration on five sets that is only strategically splittable if Skewer goes first.



References and acknowledgements

- D. Condon et al., *On Generalizations of Separating and Splitting Families*, Electronic Journal of Combinatorics 23:3 (2016).
- D.R. Stinson, *Some Baby-Step Giant-Step Algorithms for the Low Hamming Weight Discrete Logarithm Problem*, Mathematics of Computation (2001), 379–391.

This work was supported by NSF grant No. DMS 1659872 and Boise State University.