Matroids on Groups?

Jeremy S. LeCrone and Nancy Ann Neudauer

Josh Gross

Department of Physical Sciences
York College of Pennsylvania
York, PA 17403

Table of Contents

1. Introduction
2. Definitions
3. The search for a groupic matroid
4. Examples
5. Theorem 1
6. Properties of $\mathcal{M}(G)$
7. Another matroid?
8. Theorem 2
9. Counting
10. An original matroid structure?
11. Graphics
12. Conclusion

Introduction

Question

Is it possible for a group to be a matroid?

Introduction

Question

Is it possible for a group to be a matroid?

What is a group?

What is a matroid?

Definitions

A brief set theory review

- $A \subseteq B$: The set A is a subset of (or equal to) the set B.
- $\emptyset$: The empty set.
- $a \in A$: The element a is in the set A.
- $|A| = x$: The order of (number of elements in) A is equal to x.
- $C = A \setminus B$: C is comprised of all the elements in A that are not in B.
- $C = A \cup B$: C is comprised of all the elements that are in A or B.

Definitions

What is a group?

A group is a set G with a binary operation $*$ typically denoted $(G, *)$ in which the following conditions hold:

Closure: $\forall a, b \in G, a * b \in G$

Associativity: $\forall a, b, c \in G, (a * b) * c = a * (b * c)$

Identity: $\exists e \in G \mid \forall a \in G, a * e = a$

Inverse: $\forall a \in G, \exists a^{-1} \in G \mid a * a^{-1} = e$

Definitions

What is a group?

A group is a set G with a binary operation $*$ typically denoted $(G, *)$ in which the following conditions hold:

Closure: $\forall a, b \in G, a * b \in G$

Associativity: $\forall a, b, c \in G, (a * b) * c = a * (b * c)$

Identity: $\exists e \in G \mid \forall a \in G, a * e = a$

Inverse: $\forall a \in G, \exists a^{-1} \in G \mid a * a^{-1} = e$

Examples of groups: $(\mathbb{Z}, +)$, $(\mathbb{Q}, *)$

Definitions

What is a group?

A group is a set G with a binary operation $*$ typically denoted $(G, *)$ in which the following conditions hold:
Closure: $\forall a, b \in G, a * b \in G$
Associativity: $\forall a, b, c \in G, (a * b) * c = a * (b * c)$
Identity: $\exists e \in G \mid \forall a \in G, a * e = a$
Inverse: $\forall a \in G, \exists a^{-1} \in G \mid a * a^{-1} = e$

Examples of groups: $(\mathbb{Z}, +)$, $(\mathbb{Q}, *)$
Examples of !groups: $(\mathbb{N}, +)$, $(\mathbb{Z}, *)$

Definitions

What is a group?

A group is a set G with a binary operation $*$ typically denoted $(G, *)$ in which the following conditions hold:
Closure: $\forall a, b \in G, a * b \in G$
Associativity: $\forall a, b, c \in G, (a * b) * c = a * (b * c)$
Identity: $\exists e \in G \mid \forall a \in G, a * e = a$
Inverse: $\forall a \in G, \exists a^{-1} \in G \mid a * a^{-1} = e$

Examples of groups: $(\mathbb{Z}, +)$, $(\mathbb{Q}, *)$
Examples of !groups: $(\mathbb{N}, +)$, $(\mathbb{Z}, *)$
$(\mathbb{N}, +)$ is not a group as no additive identity exists.

Definitions

What is a group?

A group is a set G with a binary operation $*$ typically denoted $(G, *)$ in which the following conditions hold:
Closure: $\forall a, b \in G, a * b \in G$
Associativity: $\forall a, b, c \in G, (a * b) * c = a * (b * c)$
Identity: $\exists e \in G \mid \forall a \in G, a * e = a$
Inverse: $\forall a \in G, \exists a^{-1} \in G \mid a * a^{-1} = e$

Examples of groups: $(\mathbb{Z}, +)$, $(\mathbb{Q}, *)$
Examples of !groups: $(\mathbb{N}, +)$, $(\mathbb{Z}, *)$
$(\mathbb{N}, +)$ is not a group as no additive identity exists.
$(\mathbb{Z}, *)$ is not a group as there are elements without inverses.

Definitions

What is a group?

A group is a set G with a binary operation $*$ typically denoted $(G, *)$ in which the following conditions hold:
Closure: $\forall a, b \in G, a * b \in G$
Associativity: $\forall a, b, c \in G, (a * b) * c = a * (b * c)$
Identity: $\exists e \in G \mid \forall a \in G, a * e = a$
Inverse: $\forall a \in G, \exists a^{-1} \in G \mid a * a^{-1} = e$

Examples of groups: $(\mathbb{Z}, +)$, $(\mathbb{Q}, *)$
Examples of !groups: $(\mathbb{N}, +)$, $(\mathbb{Z}, *)$
$(\mathbb{N}, +)$ is not a group as no additive identity exists.
$(\mathbb{Z}, *)$ is not a group as there are elements without inverses.
Note: The order of an element a in a group G is the smallest integer k such that $a^k = e$, where $a^k = \underbrace{a * a ... * a}_{\text{k times}}$ and e is the group's identity. If no such integer exists, a is said to have infinite order.

Definitions

What is a matroid?

A matroid M is comprised of a finite set of elements E, called the ground set, and a collection $\mathcal{I}$ of subsets $I \subseteq E$, the independent sets, which satisfy the following:
1) $\emptyset \in \mathcal{I}$,
2) If $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$,
3) If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}$

Definitions

What is a matroid?

A matroid M is comprised of a finite set of elements E, called the ground set, and a collection $\mathcal{I}$ of subsets $I \subseteq E$, the independent sets, which satisfy the following:
1) $\emptyset \in \mathcal{I}$,
2) If $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$,
3) If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}$

In English:
1) The empty set is independent.
2) A subset of an independent set is itself independent.
3) If the order of an independent set is less than the order of another independent set, there is an element in the larger-order set that can be added to the smaller-order set to produce another independent set.

The search for a groupic matroid

Question

Knowing the definitions of a group and a matroid, how can we define a matroid on a group?

The search for a groupic matroid

Question

Knowing the definitions of a group and a matroid, how can we define a matroid on a group?

Define the ground set

Define what independence means

The search for a groupic matroid

Question

Knowing the definitions of a group and a matroid, how can we define a matroid on a group?

Define the ground set

We will define the ground set of a groupic matroid to be the group's set.

Define what independence means

The search for a groupic matroid

Question

Knowing the definitions of a group and a matroid, how can we define a matroid on a group?

Define the ground set

We will define the ground set of a groupic matroid as the group's set.

Define what independence means

We will define two elements of a group's set as independent if their product (using the group's operation) is not the group's identity.

The search for a groupic matroid

Question

Knowing the definitions of a group and a matroid, how can we define a matroid on a group?

Define the ground set

We will define the ground set of a groupic matroid as the group's set.

Define what independence means

We will define two elements of a group's set as independent if their product (using the group's operation) is not the group's identity.

Note: these choices are somewhat arbitrary, but they are intuitive.

The search for a groupic matroid

A word on notation

For convenience, we will write the elements of a group G's set in the following way:

$$G = \{e; a_1, a_2, ..., a_m; g_1, g_1^{-1}, g_2, g_2^{-1}, ..., g_k, g_k^{-1}\}$$

Where e is the identity, $a_{1...m}$ are the involutions (elements who are their own inverse), and $g_{1...k}$ are the elements of higher order.

The search for a groupic matroid

Definition of a groupic matroid

Let $(G, \mathcal{I})$ be the ordered pair where the ground set is G and $\mathcal{I}$ is the collection of subsets $I \subseteq G$ such that $xy \neq e$ for all $x, y \in I$. This is the groupic matroid of G, denoted $\mathcal{M}(G) = (G, \mathcal{I})$

Examples

Example: $\mathcal{M}(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo $4 = \{0, 1, 2, 3\}$

Examples

Example: $\mathcal{M}(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo 4 $= \{0, 1, 2, 3\}$

- The ground set is $\{0; 2; 1, 3\}$ as $e = 0$, $2 + 2 \equiv 0 \pmod 4$, and 1 and 3 are inverses.

Examples

Example: $\mathcal{M}(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo 4 $= \{0, 1, 2, 3\}$

- The ground set is $\{0; 2; 1, 3\}$ as $e = 0$, $2 + 2 \equiv 0 \pmod 4$, and 1 and 3 are inverses.
- $\mathcal{I} = ?$

Examples

Example: $\mathcal{M}(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo $4 = \{0, 1, 2, 3\}$

- The ground set is $\{0; 2; 1, 3\}$ as $e = 0$, $2 + 2 \equiv 0 \pmod 4$, and 1 and 3 are inverses.
- $\mathcal{I} = ?$
  - Because 0 is the identity, it cannot be in an independent set as if it were, $0 + 0 \equiv 0 \pmod 4$ which would mean the set is not independent, a contradiction.

Examples

Example: $\mathcal{M}(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo $4 = \{0, 1, 2, 3\}$

- The ground set is $\{0; 2; 1, 3\}$ as $e = 0$, $2 + 2 \equiv 0 \pmod 4$, and 1 and 3 are inverses.
- $\mathcal{I} = ?$
    - Because 0 is the identity, it cannot be in an independent set as if it were, $0 + 0 \equiv 0 \pmod 4$ which would mean the set is not independent, a contradiction.
    - Similarly, because 2 is its own inverse, if it were in an independent set, $2 + 2 \equiv 0 \pmod 4$ which would mean the set is not independent, a contradiction.

Examples

Example: $\mathcal{M}(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo $4 = \{0, 1, 2, 3\}$

- The ground set is $\{0; 2; 1, 3\}$ as $e = 0$, $2 + 2 \equiv 0 \pmod 4$, and 1 and 3 are inverses.
- $\mathcal{I} = ?$
  - Because 0 is the identity, it cannot be in an independent set as if it were, $0 + 0 \equiv 0 \pmod 4$ which would mean the set is not independent, a contradiction.
  - Similarly, because 2 is its own inverse, if it were in an independent set, $2 + 2 \equiv 0 \pmod 4$ which would mean the set is not independent, a contradiction.
  - Also, 1 and 3 cannot both be in an independent set, as $3 + 1 \equiv 0 \pmod 4$, which would mean the set is not independent, a contradiction. Note: this applies to any pair of inverses - only one or the other can be in an independent set, not both.

Examples

Example: $\mathcal{M}(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo $4 = \{0, 1, 2, 3\}$

Thus, $\mathcal{I} = \{\emptyset, \{1\}, \{3\}\} \implies \mathcal{M}(\mathbb{Z}_4) = (\mathbb{Z}_4, \{\emptyset, \{1\}, \{3\}\})$.

Examples

Example: $\mathcal{M}(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo 4 $= \{0, 1, 2, 3\}$

Thus, $\mathcal{I} = \{\emptyset, \{1\}, \{3\}\} \implies \mathcal{M}(\mathbb{Z}_4) = (\mathbb{Z}_4, \{\emptyset, \{1\}, \{3\}\})$.
Returning to the matroid criteria:
1) $\emptyset \in \mathcal{I}$

- Clearly, $\emptyset \in \mathcal{I}$

Examples

Example: $\mathcal{M}(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo 4 $= \{0, 1, 2, 3\}$

Thus, $\mathcal{I} = \{\emptyset, \{1\}, \{3\}\} \implies \mathcal{M}(\mathbb{Z}_4) = (\mathbb{Z}_4, \{\emptyset, \{1\}, \{3\}\})$.
Returning to the matroid criteria:

1) $\emptyset \in \mathcal{I}$

- Clearly, $\emptyset \in \mathcal{I}$

2) If $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$

- This only occurs when $I_1 = \{1\}$ or $I_1 = \{3\}$ and $I_2 = \emptyset$, and in both cases, as confirmed in (1), $\emptyset \in \mathcal{I}$

Examples

Example: $\mathcal{M}(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo 4 $= \{0, 1, 2, 3\}$

Thus, $\mathcal{I} = \{\emptyset, \{1\}, \{3\}\} \implies \mathcal{M}(\mathbb{Z}_4) = (\mathbb{Z}_4, \{\emptyset, \{1\}, \{3\}\})$.
Returning to the matroid criteria:

1) $\emptyset \in \mathcal{I}$

- Clearly, $\emptyset \in \mathcal{I}$

2) If $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$

- This only occurs when $I_1 = \{1\}$ or $I_1 = \{3\}$ and $I_2 = \emptyset$, and in both cases, as confirmed in (1), $\emptyset \in \mathcal{I}$

3) If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}$

- This only occurs when $I_1 = \emptyset$ and $I_2 = \{1\}$ or $I_2 = \{3\}$. In both cases, $(I_2 \setminus I_1) \cup I_1 = I_2$, which is independent by definition.

Examples

Example: $\mathcal{M}(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo 4 $= \{0, 1, 2, 3\}$

Thus, $\mathcal{I} = \{\emptyset, \{1\}, \{3\}\} \implies \mathcal{M}(\mathbb{Z}_4) = (\mathbb{Z}_4, \{\emptyset, \{1\}, \{3\}\})$.
Returning to the matroid criteria:

1) $\emptyset \in \mathcal{I}$

- Clearly, $\emptyset \in \mathcal{I}$

2) If $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$

- This only occurs when $I_1 = \{1\}$ or $I_1 = \{3\}$ and $I_2 = \emptyset$, and in both cases, as confirmed in (1), $\emptyset \in \mathcal{I}$

3) If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}$

- This only occurs when $I_1 = \emptyset$ and $I_2 = \{1\}$ or $I_2 = \{3\}$. In both cases, $(I_2 \setminus I_1) \cup I_1 = I_2$, which is independent by definition.

Thus, $\mathcal{M}(\mathbb{Z}_4)$ is a matroid.

Examples

Example: $\mathcal{M}(\mathbb{Z}_5)$

$\mathbb{Z}_5$ is the group of integers under addition modulo 5 $= \{0, 1, 2, 3, 4\}$

Examples

Example: $\mathcal{M}(\mathbb{Z}_5)$

$\mathbb{Z}_5$ is the group of integers under addition modulo $5 = \{0, 1, 2, 3, 4\}$

- The ground set is $\{0; ; 1, 4, 2, 3\}$ as $e = 0$, and $(1, 4)$ and $(2, 3)$ are inverses.

Examples

Example: $\mathcal{M}(\mathbb{Z}_5)$

$\mathbb{Z}_5$ is the group of integers under addition modulo $5 = \{0, 1, 2, 3, 4\}$

- The ground set is $\{0; ; 1, 4, 2, 3\}$ as $e = 0$, and $(1, 4)$ and $(2, 3)$ are inverses.
- $\mathcal{I} = ?$

Examples

Example: $\mathcal{M}(\mathbb{Z}_5)$

$\mathbb{Z}_5$ is the group of integers under addition modulo $5 = \{0, 1, 2, 3, 4\}$

- The ground set is $\{0; ; 1, 4, 2, 3\}$ as $e = 0$, and $(1, 4)$ and $(2, 3)$ are inverses.
- $\mathcal{I} = ?$
  - Again, because 0 is the identity, it cannot be in an independent set as if it were, $0 + 0 \equiv 0 \pmod 5$ which would mean the set is not independent, a contradiction.

Examples

Example: $\mathcal{M}(\mathbb{Z}_5)$

$\mathbb{Z}_5$ is the group of integers under addition modulo 5 $= \{0, 1, 2, 3, 4\}$

- The ground set is $\{0; ; 1, 4, 2, 3\}$ as $e = 0$, and $(1, 4)$ and $(2, 3)$ are inverses.
- $\mathcal{I} = ?$
  - Again, because 0 is the identity, it cannot be in an independent set as if it were, $0 + 0 \equiv 0 \pmod 5$ which would mean the set is not independent, a contradiction.
  - Also, $(1, 4)$ and $(2, 3)$ cannot both be in an independent set, as $1 + 4 \equiv 0 \pmod 5$ (and similarly for $(2, 3)$), which would mean the set is not independent, a contradiction.

Examples

Example: $\mathcal{M}(\mathbb{Z}_5)$

$\mathbb{Z}_5$ is the group of integers under addition modulo 5 $= \{0, 1, 2, 3, 4\}$

Thus, $\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{2, 4\}, \{3, 4\}\} \implies \mathcal{M}(\mathbb{Z}_5) = (\mathbb{Z}_5, \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{2, 4\}, \{3, 4\}\})$.

Examples

Example: $\mathcal{M}(\mathbb{Z}_5)$

$\mathbb{Z}_5$ is the group of integers under addition modulo 5 $= \{0, 1, 2, 3, 4\}$

Thus, $\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{2, 4\}, \{3, 4\}\} \implies$ $\mathcal{M}(\mathbb{Z}_5) = (\mathbb{Z}_5, \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{2, 4\}, \{3, 4\}\})$.
Returning to the matroid criteria:
1) $\emptyset \in \mathcal{I}$

- Clearly, $\emptyset \in \mathcal{I}$

Examples

Example: $\mathcal{M}(\mathbb{Z}_5)$

$\mathbb{Z}_5$ is the group of integers under addition modulo 5 $= \{0, 1, 2, 3, 4\}$

Thus, $\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{2, 4\}, \{3, 4\}\} \implies \mathcal{M}(\mathbb{Z}_5) = (\mathbb{Z}_5, \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{2, 4\}, \{3, 4\}\})$.
Returning to the matroid criteria:

1) $\emptyset \in \mathcal{I}$

- Clearly, $\emptyset \in \mathcal{I}$

2) If $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$

- This is easily, though tediously, verified.

Examples

Example: $\mathcal{M}(\mathbb{Z}_5)$

$\mathbb{Z}_5$ is the group of integers under addition modulo 5 $= \{0, 1, 2, 3, 4\}$

Thus, $\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{2, 4\}, \{3, 4\}\} \implies \mathcal{M}(\mathbb{Z}_5) = (\mathbb{Z}_5, \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{2, 4\}, \{3, 4\}\})$.

Returning to the matroid criteria:

1) $\emptyset \in \mathcal{I}$

- Clearly, $\emptyset \in \mathcal{I}$

2) If $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$

- This is easily, though tediously, verified.

3) If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}$

- This is easily, though tediously, verified.

Examples

Example: $\mathcal{M}(\mathbb{Z}_5)$

$\mathbb{Z}_5$ is the group of integers under addition modulo 5 $= \{0, 1, 2, 3, 4\}$

Thus, $\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{2, 4\}, \{3, 4\}\} \implies$ $\mathcal{M}(\mathbb{Z}_5) = (\mathbb{Z}_5, \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{2, 4\}, \{3, 4\}\})$.
Returning to the matroid criteria:

1) $\emptyset \in \mathcal{I}$

- Clearly, $\emptyset \in \mathcal{I}$

2) If $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$

- This is easily, though tediously, verified.

3) If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}$

- This is easily, though tediously, verified.

Thus, $\mathcal{M}(\mathbb{Z}_5)$ is a matroid.

Examples

Example: $\mathcal{M}(K_4)$

To make the example clearer, we will take K_4 to be the set $\{1, 3, 5, 7\}$ with the operation multiplication mod 8.

Examples

Example: $\mathcal{M}(K_4)$

To make the example clearer, we will take K_4 to be the set $\{1, 3, 5, 7\}$ with the operation multiplication mod 8.

Thus, $\mathcal{I} = \{\emptyset\}$

Examples

Example: $\mathcal{M}(K_4)$

To make the example clearer, we will take K_4 to be the set $\{1, 3, 5, 7\}$ with the operation multiplication mod 8.

Thus, $\mathcal{I} = \{\emptyset\}$
$\mathcal{M}(K_4) = (K_4, \{\emptyset\})$

Example: $\mathcal{M}(K_4)$

To make the example clearer, we will take K_4 to be the set $\{1, 3, 5, 7\}$ with the operation multiplication mod 8.

Thus, $\mathcal{I} = \{\emptyset\}$
$\mathcal{M}(K_4) = (K_4, \{\emptyset\})$
It is clear that $\mathcal{M}(K_4)$ satisfies the matroid criteria.

Examples

Example: $\mathcal{M}(K_4)$

To make the example clearer, we will take K_4 to be the set $\{1, 3, 5, 7\}$ with the operation multiplication mod 8.

Thus, $\mathcal{I} = \{\emptyset\}$
$\mathcal{M}(K_4) = (K_4, \{\emptyset\})$
It is clear that $\mathcal{M}(K_4)$ satisfies the matroid criteria.
Notice that $\mathcal{M}(K_4)$ and $\mathcal{M}(\mathbb{Z}_4)$ give different groupic matroids - this means that given a groupic matroid with a ground set containing four elements, we can determine the group used to construct the matroid.

Theorem 1

Theorem 1: $\mathcal{M}(G)$ is a matroid

Theorem 1

Theorem 1: $\mathcal{M}(G)$ is a matroid

To prove this, we must show that for any group, the matroid criteria hold for the constructed groupic matroid's $\mathcal{I}$:

1) $\emptyset \in \mathcal{I}$
2) If $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$
3) If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}$

Theorem 1

Theorem 1: $\mathcal{M}(G)$ is a matroid

$\emptyset \in \mathcal{I}$

It is vacuously true to say that $\emptyset$ is independent, as no product of a pair of elements in $\emptyset$ yield an identity element.

If $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$

If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}$

Theorem 1

Theorem 1: $\mathcal{M}(G)$ is a matroid

$\emptyset \in \mathcal{I}$

If $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$

Proof by contradiction: assume $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, and that $I_2 \notin \mathcal{I}$. This means that $\exists x, y \in I_2 \mid x * y = e$, where e is the group's identity element. However, since $x, y \in I_2$ and $I_2 \subseteq I_1$, $x, y \in I_1$. But, since $x * y = e$, this means that I_1 is not independent, a contradiction. Therefore, I_2 must also be independent.

If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}$

Theorem 1

Theorem 1: $\mathcal{M}(G)$ is a matroid

$\emptyset \in \mathcal{I}$

If $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$

If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}$

Suppose $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$. Thus, $\forall g \in I_2$, either g or $g^{-1} \in I_1$, or neither are in I_1. Because $|I_2| > |I_1|$, there is an element $g^* \in I_2 \mid g^* \wedge {g^*}^{-1} \notin I_1$. Due to this, $I_1 \cup \{g^*\} \in \mathcal{I}$.

Theorem 1

Theorem 1: $\mathcal{M}(G)$ is a matroid

Having proven that $\mathcal{M}(G)$ satisfies the three matroid criteria, we know that $\mathcal{M}(G)$ is indeed a matroid.

Properties of $\mathcal{M}(G)$

Earlier we saw that $\mathcal{M}(K_4)$ and $\mathcal{M}(\mathbb{Z}_4)$ gave groupic matroids with differing $\mathcal{I}$: $\mathcal{I}_{K_4} = \{\emptyset\}$ and $\mathcal{I}_{\mathbb{Z}_4} = \{\emptyset, \{1\}, \{3\}\}$. The properties of each group's elements determine $\mathcal{I}$, as demonstrated by the makeup of $\mathbb{Z}_4$ and K_4:

Properties of $\mathcal{M}(G)$

Earlier we saw that $\mathcal{M}(K_4)$ and $\mathcal{M}(\mathbb{Z}_4)$ gave groupic matroids with differing $\mathcal{I}$: $\mathcal{I}_{K_4} = \{\emptyset\}$ and $\mathcal{I}_{\mathbb{Z}_4} = \{\emptyset, \{1\}, \{3\}\}$. The properties of each group's elements determine $\mathcal{I}$, as demonstrated by the makeup of $\mathbb{Z}_4$ and K_4:

$$\mathbb{Z}_4 = \{0; 2; 1, 3\} = \{e; a_1; g_1, {g_1}^{-1}\}$$

Properties of $\mathcal{M}(G)$

Earlier we saw that $\mathcal{M}(K_4)$ and $\mathcal{M}(\mathbb{Z}_4)$ gave groupic matroids with differing $\mathcal{I}$: $\mathcal{I}_{K_4} = \{\emptyset\}$ and $\mathcal{I}_{\mathbb{Z}_4} = \{\emptyset, \{1\}, \{3\}\}$. The properties of each group's elements determine $\mathcal{I}$, as demonstrated by the makeup of $\mathbb{Z}_4$ and K_4:

$$\mathbb{Z}_4 = \{0; 2; 1, 3\} = \{e; a_1; g_1, {g_1}^{-1}\}$$

$$K_4 = \{1; 3, 5, 7; \} = \{e; a_1, a_2, a_3; \}$$

Properties of $\mathcal{M}(G)$

Question

Are all $\mathcal{I}$ unique, or can two different groups give isomorphic groupic matroids?

Properties of $\mathcal{M}(G)$

Question

Are all $\mathcal{I}$ unique, or can two different groups give isomorphic groupic matroids?

In the case of $\mathbb{Z}_4$ and K_4, the order of the groups were equal (4), however they had a different amount of involutions and higher-order elements.

Properties of $\mathcal{M}(G)$

Question

Are all $\mathcal{I}$ unique, or can two different groups give isomorphic groupic matroids?

In the case of $\mathbb{Z}_4$ and K_4, the order of the groups were equal (4), however they had a different amount of involutions and higher-order elements. Perhaps two groups with the same number of involutions and higher-order elements provide an answer?

A brief aside

Our answer lies in a comparison of two groupic matroids, one of which involves quaternions. A crash course follows.

A brief aside

Quaternions

Quaternions ($\mathbb{H}$), simply put, are a number system that extend the complex numbers. We need only concern ourselves with the following information.

A brief aside

Quaternions

Quaternions ($\mathbb{H}$), simply put, are a number system that extend the complex numbers. We need only concern ourselves with the following information.

- A quaternion takes the form: $a + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$

A brief aside

Quaternions

Quaternions ($\mathbb{H}$), simply put, are a number system that extend the complex numbers. We need only concern ourselves with the following information.

- A quaternion takes the form: $a + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$
- i, j, and k can be interpreted as unit vectors that satisfy the following conditions:

A brief aside

Quaternions

Quaternions ($\mathbb{H}$), simply put, are a number system that extend the complex numbers. We need only concern ourselves with the following information.

- A quaternion takes the form: $a + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$
- i, j, and k can be interpreted as unit vectors that satisfy the following conditions:
  - $i^2 = j^2 = k^2 = -1$

A brief aside

Quaternions

Quaternions ($\mathbb{H}$), simply put, are a number system that extend the complex numbers. We need only concern ourselves with the following information.

- A quaternion takes the form: $a + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$
- i, j, and k can be interpreted as unit vectors that satisfy the following conditions:
  - $i^2 = j^2 = k^2 = -1$
  - $ij = k, ji = -k$

A brief aside

Quaternions

Quaternions ($\mathbb{H}$), simply put, are a number system that extend the complex numbers. We need only concern ourselves with the following information.

- A quaternion takes the form: $a + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$
- i, j, and k can be interpreted as unit vectors that satisfy the following conditions:
  - $i^2 = j^2 = k^2 = -1$
  - $ij = k, ji = -k$
  - $jk = i, kj = -i$

A brief aside

Quaternions

Quaternions ($\mathbb{H}$), simply put, are a number system that extend the complex numbers. We need only concern ourselves with the following information.

- A quaternion takes the form: $a + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$
- i, j, and k can be interpreted as unit vectors that satisfy the following conditions:
  - $i^2 = j^2 = k^2 = -1$
  - $ij = k, ji = -k$
  - $jk = i, kj = -i$
  - $ki = j, ik = -j$

A brief aside

Quaternions

Quaternions ($\mathbb{H}$), simply put, are a number system that extend the complex numbers. We need only concern ourselves with the following information.

- A quaternion takes the form: $a + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$
- i, j, and k can be interpreted as unit vectors that satisfy the following conditions:
  - $i^2 = j^2 = k^2 = -1$
  - $ij = k, ji = -k$
  - $jk = i, kj = -i$
  - $ki = j, ik = -j$
- A multiplicative group exists for the quaternions, known as the Hamilton product, which we'll use to construct a subgroup $\mathbb{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}$.

Properties of $\mathcal{M}(G)$

$\mathcal{M}(\mathbb{Z}_8)$ vs. $\mathcal{M}(\mathbb{H}_8)$

Examining $\mathcal{M}(\mathbb{Z}_8)$, the set of integers under addition mod 8, and $\mathcal{M}(\mathbb{H}_8)$, our constructed subgroup, we confirm that both group sets have the same structure, $\{e; a_1; g_1, {g_1}^{-1}, g_2, {g_2}^{-1}, g_3, {g_3}^{-1}\}$

Properties of $\mathcal{M}(G)$

$\mathcal{M}(\mathbb{Z}_8)$ vs. $\mathcal{M}(\mathbb{H}_8)$

Examining $\mathcal{M}(\mathbb{Z}_8)$, the set of integers under addition mod 8, and $\mathcal{M}(\mathbb{H}_8)$, our constructed subgroup, we confirm that both group sets have the same structure, $\{e; a_1; g_1, g_1^{-1}, g_2, g_2^{-1}, g_3, g_3^{-1}\}$

$$\mathbb{Z}_8 = \{0; 4; 1, 7, 2, 6, 3, 5\}$$

Properties of $\mathcal{M}(G)$

$\mathcal{M}(\mathbb{Z}_8)$ vs. $\mathcal{M}(\mathbb{H}_8)$

Examining $\mathcal{M}(\mathbb{Z}_8)$, the set of integers under addition mod 8, and $\mathcal{M}(\mathbb{H}_8)$, our constructed subgroup, we confirm that both group sets have the same structure, $\{e; a_1; g_1, g_1^{-1}, g_2, g_2^{-1}, g_3, g_3^{-1}\}$

$$\mathbb{Z}_8 = \{0; 4; 1, 7, 2, 6, 3, 5\}$$

$$\mathbb{H}_8 = \{1; -1; i, -i, j, -j, k, -k\}$$

Properties of $\mathcal{M}(G)$

$\mathcal{M}(\mathbb{Z}_8)$ vs. $\mathcal{M}(\mathbb{H}_8)$

Having confirmed that both group sets have the same structure, by our definition of a groupic matroid, $|\mathcal{I}_{\mathbb{Z}_8}| = |\mathcal{I}_{\mathbb{H}_8}|$, and indeed, the number of subsets in both $\mathcal{I}$ with order 0, 1, 2 are similar and comprised of the 'same' elements

Properties of $\mathcal{M}(G)$

$\mathcal{M}(\mathbb{Z}_8)$ vs. $\mathcal{M}(\mathbb{H}_8)$

$\mathcal{I}_{\mathbb{Z}_8} = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{5\}, \{6\}, \{7\}, \{1,2\}, \{1,3\}, \{1,5\}, \{1,6\}, \{2,3\}, \{2,5\}, \{2,7\}, \{3,6\}, \{3,7\}, \{5,6\}, \{5,7\}, \{6,7\}, \{1,2,3\}, \{1,2,5\}, \{1,3,6\}, \{1,5,6\}, \{2,3,7\}, \{2,5,7\}, \{3,6,7\}, \{5,6,7\} \}$

Properties of $\mathcal{M}(G)$

$\mathcal{M}(\mathbb{Z}_8)$ vs. $\mathcal{M}(\mathbb{H}_8)$

$\mathcal{I}_{\mathbb{Z}_8} = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{5\}, \{6\}, \{7\}, \{1,2\}, \{1,3\}, \{1,5\}, \{1,6\}, \{2,3\}, \{2,5\}, \{2,7\}, \{3,6\}, \{3,7\}, \{5,6\}, \{5,7\}, \{6,7\}, \{1,2,3\}, \{1,2,5\}, \{1,3,6\}, \{1,5,6\}, \{2,3,7\}, \{2,5,7\}, \{3,6,7\}, \{5,6,7\} \}$

$\mathcal{I}_{\mathbb{H}_8} = \{ \emptyset, \{i\}, \{j\}, \{k\}, \{-k\}, \{-j\}, \{-i\}, \{i,j\}, \{i,k\}, \{i,-k\}, \{i,-j\}, \{j,k\}, \{j,-k\}, \{j,-i\}, \{k,-j\}, \{k,-i\}, \{-k,-j\}, \{-k,-i\}, \{-j,-i\}, \{i,j,k\}, \{i,j,-k\}, \{i,k,-j\}, \{i,-k,-j\}, \{j,k,-i\}, \{j,-k,-i\}, \{k,-j,-i\}, \{-j,-k,-i\} \}$

Properties of $\mathcal{M}(G)$

$\mathcal{M}(\mathbb{Z}_8)$ vs. $\mathcal{M}(\mathbb{H}_8)$

$\mathcal{I}_{\mathbb{Z}_8} = \{\ \emptyset, \{1\}, \{2\}, \{3\}, \{5\}, \{6\}, \{7\}, \{1,2\}, \{1,3\}, \{1,5\}, \{1,6\}, \{2,3\}, \{2,5\}, \{2,7\}, \{3,6\}, \{3,7\}, \{5,6\}, \{5,7\}, \{6,7\}, \{1,2,3\}, \{1,2,5\}, \{1,3,6\}, \{1,5,6\}, \{2,3,7\}, \{2,5,7\}, \{3,6,7\}, \{5,6,7\}\ \}$

$\mathcal{I}_{\mathbb{H}_8} = \{\ \emptyset, \{i\}, \{j\}, \{k\}, \{-k\}, \{-j\}, \{-i\}, \{i,j\}, \{i,k\}, \{i,-k\}, \{i,-j\}, \{j,k\}, \{j,-k\}, \{j,-i\}, \{k,-j\}, \{k,-i\}, \{-k,-j\}, \{-k,-i\}, \{-j,-i\}, \{i,j,k\}, \{i,j,-k\}, \{i,k,-j\}, \{i,-k,-j\}, \{j,k,-i\}, \{j,-k,-i\}, \{k,-j,-i\}, \{-j,-k,-i\}\ \}$

With the mapping: $1 \to i, 2 \to j, 3 \to k, 5 \to -k, 6 \to -j, 7 \to -i$, we see that these two collections are isomorphic.

Properties of $\mathcal{M}(G)$

$\mathcal{M}(\mathbb{Z}_8)$ vs. $\mathcal{M}(\mathbb{H}_8)$

$\mathcal{I}_{\mathbb{Z}_8} = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{5\}, \{6\}, \{7\}, \{1,2\}, \{1,3\}, \{1,5\}, \{1,6\}, \{2,3\}, \{2,5\}, \{2,7\}, \{3,6\}, \{3,7\}, \{5,6\}, \{5,7\}, \{6,7\}, \{1,2,3\}, \{1,2,5\}, \{1,3,6\}, \{1,5,6\}, \{2,3,7\}, \{2,5,7\}, \{3,6,7\}, \{5,6,7\} \}$

$\mathcal{I}_{\mathbb{H}_8} = \{ \emptyset, \{i\}, \{j\}, \{k\}, \{-k\}, \{-j\}, \{-i\}, \{i,j\}, \{i,k\}, \{i,-k\}, \{i,-j\}, \{j,k\}, \{j,-k\}, \{j,-i\}, \{k,-j\}, \{k,-i\}, \{-k,-j\}, \{-k,-i\}, \{-j,-i\}, \{i,j,k\}, \{i,j,-k\}, \{i,k,-j\}, \{i,-k,-j\}, \{j,k,-i\}, \{j,-k,-i\}, \{k,-j,-i\}, \{-j,-k,-i\} \}$

With the mapping: $1 \to i, 2 \to j, 3 \to k, 5 \to -k, 6 \to -j, 7 \to -i$, we see that these two collections are isomorphic.
Thus, it is not always true that $\mathcal{I}$ (and the groupic matroid itself) are unique to the group it is constructed over.

Another matroid?

Earlier we noted that our choices for the groupic matroid's ground set and notion of independence were somewhat arbitrary. We can slightly alter those choices to obtain a different groupic matroid structure.

Another matroid?

Earlier we noted that our choices for the groupic matroid's ground set and notion of independence were somewhat arbitrary. We can slightly alter those choices to obtain a different groupic matroid structure.

Definition of a groupic matroid (1)

Let $(G, \mathcal{I})$ be the ordered pair where the ground set is G and $\mathcal{I}$ is the collection of subsets $I \subseteq G$ such that $xy \neq e$ for all $x, y \in I$. This is the groupic matroid of G, denoted $\mathcal{M}(G) = (G, \mathcal{I})$

Another matroid?

Earlier we noted that our choices for the groupic matroid's ground set and notion of independence were somewhat arbitrary. We can slightly alter those choices to obtain a different groupic matroid structure.

Definition of a groupic matroid (1)

Let $(G, \mathcal{I})$ be the ordered pair where the ground set is G and $\mathcal{I}$ is the collection of subsets $I \subseteq G$ such that $xy \neq e$ for all $x, y \in I$. This is the groupic matroid of G, denoted $\mathcal{M}(G) = (G, \mathcal{I})$

Question

What if our selected notion of independence requires that x and y are distinct?

Another matroid?

Definition of a groupic matroid (2)

Let $\mathcal{M}^*(G)$ be the ordered pair $(G, \mathcal{I}^*$, where $\mathcal{I}^*)$ is the collection of subsets $I \subseteq G$ such that, for all elements $x, y \in I$, if $x \neq y$, then $xy \neq e$

As in $\mathcal{M}(G)$, an element g_i of the group or its inverse $g_i{}^{-1}$ may appear in an independent set of $\mathcal{M}^*(G)$, but not both. However, identities and involutions can now appear, due to the independence criteria requiring that $x \neq y$.

Another matroid?

Example: $\mathcal{M}^*(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo $4 = \{0, 1, 2, 3\}$

Another matroid?

Example: $\mathcal{M}^*(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo $4 = \{0, 1, 2, 3\}$

- The ground set is still $\{0; 2; 1, 3\}$

Another matroid?

Example: $\mathcal{M}^*(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo $4 = \{0, 1, 2, 3\}$

- The ground set is still $\{0; 2; 1, 3\}$
- $\mathcal{I}^* = ?$

Another matroid?

Example: $\mathcal{M}^*(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo 4 $= \{0, 1, 2, 3\}$

- The ground set is still $\{0; 2; 1, 3\}$
- $\mathcal{I}^* = ?$
  - 1 and 3 cannot both be in an independent set, as $3 + 1 \equiv 0 \pmod 4$, which would mean the set is not independent, a contradiction.
  - The other restrictions no longer apply by the new definition of independence.

Another matroid?

Example: $\mathcal{M}^*(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo 4 $= \{0, 1, 2, 3\}$

Thus, $\mathcal{I}^* = \{\emptyset, \{0\}, \{1\}, \{2\}, \{3\}, \{0,1\}, \{0,2\}, \{0,3\}, \{1,2\}, \{2,3\}, \{0,1,2\}, \{0,2,3\}\}$
$\implies \mathcal{M}^*(\mathbb{Z}_4) = (\mathbb{Z}_4, \{\emptyset, \{0\}, \{1\}, \{2\}, \{3\}, \{0,1\}, \{0,2\}, \{0,3\}, \{1,2\}, \{2,3\}, \{0,1,2\}, \{0,2,3\}\})$.

Another matroid?

Example: $\mathcal{M}^*(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo 4 = $\{0, 1, 2, 3\}$

Thus, $\mathcal{I}^* = \{\emptyset, \{0\}, \{1\}, \{2\}, \{3\}, \{0,1\}, \{0,2\}, \{0,3\}, \{1,2\}, \{2,3\}, \{0,1,2\}, \{0,2,3\}\}$

$\implies \mathcal{M}^*(\mathbb{Z}_4) = (\mathbb{Z}_4, \{\emptyset, \{0\}, \{1\}, \{2\}, \{3\}, \{0,1\}, \{0,2\}, \{0,3\}, \{1,2\}, \{2,3\}, \{0,1,2\}, \{0,2,3\}\})$.

Returning to the matroid criteria:

1) $\emptyset \in \mathcal{I}^*$

- Clearly, $\emptyset \in \mathcal{I}^*$

Another matroid?

Example: $\mathcal{M}^*(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo $4 = \{0, 1, 2, 3\}$

Thus, $\mathcal{I}^* = \{\emptyset, \{0\}, \{1\}, \{2\}, \{3\}, \{0,1\}, \{0,2\}, \{0,3\}, \{1,2\}, \{2,3\}, \{0,1,2\}, \{0,2,3\}\}$

$\implies \mathcal{M}^*(\mathbb{Z}_4) = (\mathbb{Z}_4, \{\emptyset, \{0\}, \{1\}, \{2\}, \{3\}, \{0,1\}, \{0,2\}, \{0,3\}, \{1,2\}, \{2,3\}, \{0,1,2\}, \{0,2,3\}\})$.

Returning to the matroid criteria:

1) $\emptyset \in \mathcal{I}^*$

- Clearly, $\emptyset \in \mathcal{I}^*$

2) If $I_1 \in \mathcal{I}^*$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}^*$

- This is easily, though tediously, verified.

Another matroid?

Example: $\mathcal{M}^*(\mathbb{Z}_4)$

$\mathbb{Z}_4$ is the group of integers under addition modulo $4 = \{0,\ 1,\ 2,\ 3\}$

Thus, $\mathcal{I}^* = \{\emptyset,\ \{0\},\ \{1\},\ \{2\},\ \{3\},\ \{0,1\},\ \{0,2\},\ \{0,3\},\ \{1,2\},\ \{2,3\},$ $\{0,1,2\},\ \{0,2,3\}\}$
$\implies \mathcal{M}^*(\mathbb{Z}_4) = (\mathbb{Z}_4,\ \{\emptyset,\ \{0\},\ \{1\},\ \{2\},\ \{3\},\ \{0,1\},\ \{0,2\},\ \{0,3\},$ $\{1,2\},\ \{2,3\},\ \{0,1,2\},\ \{0,2,3\}\})$.
Returning to the matroid criteria:
1) $\emptyset \in \mathcal{I}^*$

- Clearly, $\emptyset \in \mathcal{I}^*$

2) If $I_1 \in \mathcal{I}^*$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}^*$

- This is easily, though tediously, verified.

3) If $I_1, I_2 \in \mathcal{I}^*$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}^*$

- This is easily, though tediously, verified.

Thus, $\mathcal{M}^*(\mathbb{Z}_4)$ is a matroid.

Theorem 2

Theorem 2: $\mathcal{M}^*(G)$ is a matroid

Theorem 2

Theorem 2: $\mathcal{M}^*(G)$ is a matroid

To prove this, we must show that for any group, the matroid criteria hold for the constructed groupic matroid's $\mathcal{I}^*$:

1) $\emptyset \in \mathcal{I}^*$

2) If $I_1 \in \mathcal{I}^*$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}^*$

3) If $I_1, I_2 \in \mathcal{I}^*$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}^*$

Theorem 2

Theorem 2: $\mathcal{M}^*(G)$ is a matroid

1) $\emptyset \in \mathcal{I}^*$

It is vacuously true to say that $\emptyset$ is independent, as no product of a pair of elements in $\emptyset$ yield an identity element.

Theorem 2

Theorem 2: $\mathcal{M}^*(G)$ is a matroid

2) If $I_1 \in \mathcal{I}^*$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}^*$

Proof by contradiction: assume $I_1 \in \mathcal{I}^*$ and $I_2 \subseteq I_1$, and that $I_2 \notin \mathcal{I}^*$. This means that $\exists x, y \in I_2 \mid x * y = e$, where e is the group's identity element. However, since $x, y \in I_2$ and $I_2 \subseteq I_1$, $x, y \in I_1$. But, since $x * y = e$, this means that I_1 is not independent, a contradiction. Therefore, I_2 must also be independent.

Theorem 2

Theorem 2: $\mathcal{M}^*(G)$ is a matroid

3) If $I_1, I_2 \in \mathcal{I}^*$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}^*$

$|I_1| < |I_2|$ implies there is at least one element $w \in I_2, w \notin I_1$. Unlike Theorem 1, we cannot assume w is a non-identity or non-involution element. Thus, we handle the three cases:

- Case 1, $w = e$: Since $\forall x \in I_1, x * e \neq e$, $I_1 \cup \{e\} \in \mathcal{I}^*$. If such an x existed, it would have to be e itself, which by definition is $\notin I_1$.

Theorem 2

Theorem 2: $\mathcal{M}^*(G)$ is a matroid

3) If $I_1, I_2 \in \mathcal{I}^*$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}^*$

$|I_1| < |I_2|$ implies there is at least one element $w \in I_2, w \notin I_1$. Unlike Theorem 1, we cannot assume w is a non-identity or non-involution element. Thus, we handle the three cases:

- Case 1, $w = e$: Since $\forall x \in I_1, x * e \neq e$, $I_1 \cup \{e\} \in \mathcal{I}^*$. If such an x existed, it would have to be e itself, which by definition is $\notin I_1$.
- Case 2, $w = a_k$ (w is an involution): Since $\forall x \in I_1, x * a_k \neq e$, $I_1 \cup \{a_k\} \in \mathcal{I}^*$. If such an x existed, it would have to be a_k itself, which by definition is $\notin I_1$.

Theorem 2

Theorem 2: $\mathcal{M}^*(G)$ is a matroid

3) If $I_1, I_2 \in \mathcal{I}^*$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}^*$

$|I_1| < |I_2|$ implies there is at least one element $w \in I_2, w \notin I_1$. Unlike Theorem 1, we cannot assume w is a non-identity or non-involution element. Thus, we handle the three cases:

- Case 1, $w = e$: Since $\forall x \in I_1, x * e \neq e$, $I_1 \cup \{e\} \in \mathcal{I}^*$. If such an x existed, it would have to be e itself, which by definition is $\notin I_1$.
- Case 2, $w = a_k$ (w is an involution): Since $\forall x \in I_1, x * a_k \neq e$, $I_1 \cup \{a_k\} \in \mathcal{I}^*$. If such an x existed, it would have to be a_k itself, which by definition is $\notin I_1$.
- Case 3, $w = g_k$ ($\exists w^{-1}, w^{-1} \neq w$): By $|I_1| < |I_2|$, $\exists g^* \in I_2$ such that neither g^* nor $g^{*-1} \in I_1$. If not, $|I_1| = |I_2|$. Thus, letting $g_k = g^*$, $I_1 \cup \{g_k\} \in \mathcal{I}^*$.

Theorem 2

Theorem 2: $\mathcal{M}^*(G)$ is a matroid

Having proven that $\mathcal{M}^*(G)$ satisfies the three matroid criteria, we know that $\mathcal{M}^*(G)$ is indeed a matroid.

Counting $|\mathcal{I}|$ and $|\mathcal{I}^*|$

Having constructed $\mathcal{M}(G)$ and $\mathcal{M}^*(G)$, and proven they are indeed matroids, we ask one final question.

Counting $|\mathcal{I}|$ and $|\mathcal{I}^*|$

Having constructed $\mathcal{M}(G)$ and $\mathcal{M}^*(G)$, and proven they are indeed matroids, we ask one final question.

Question

What are $|\mathcal{I}|$ and $|\mathcal{I}^*|$?

Counting $|\mathcal{I}|$ and $|\mathcal{I}^*|$

Remark

Recall our ordering of G's elements:

$$G = \{e; a_1, a_2, \ldots, a_m; g_1, g_1^{-1}, g_2, g_2^{-1}, \ldots, g_k, g_k^{-1}\}$$

$|\mathcal{I}|$: By the notion of independence used to construct $\mathcal{M}(G)$, only $g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}$ are eligible to be in an independent set. For each (g_i, g_i^{-1}), either g_i, g_i^{-1}, or neither are in an independent set. Thus, there are 3^k independent sets.

Counting $|\mathcal{I}|$ and $|\mathcal{I}^*|$

Example: $k = 2$

$\mathcal{I} = \{\emptyset, \{g_1\}, \{{g_1}^{-1}\}, \{g_2\}, \{{g_2}^{-1}\}, \{g_1, g_2\}, \{g_1, {g_2}^{-1}\}, \{{g_1}^{-1}, g_2\},$
$\{{g_1}^{-1}, {g_2}^{-1}\}\}$
$|\mathcal{I}| = 3^2 = 9$

Counting $|\mathcal{I}|$ and $|\mathcal{I}^*|$

Example: $k = 2$

$\mathcal{I} = \{\emptyset, \{g_1\}, \{g_1{}^{-1}\}, \{g_2\}, \{g_2{}^{-1}\}, \{g_1, g_2\}, \{g_1, g_2{}^{-1}\}, \{g_1{}^{-1}, g_2\},$
$\{g_1{}^{-1}, g_2{}^{-1}\}\}$
$|\mathcal{I}| = 3^2 = 9$

$|\mathcal{I}^*|$: By the notion of independence used to construct $\mathcal{M}^*(G)$, every element in G is eligible to be in an independent set.

- Similar to our logic to find $|\mathcal{I}|$, for each $(g_i, g_i{}^{-1})$, either g_i, $g_i{}^{-1}$, or neither are in an independent set. Thus, there are 3^k independent sets for the elements of higher order.
- An independent set can either contain or not contain the identity e. Thus, there are 2 states for the identity.
- An independent set can either contain or not contain an involution a_i. Thus, there are 2 states for each a_i.

Combining these, we find that there are $2^{m+1}3^k$ independent sets.

Counting $|\mathcal{I}|$ and $|\mathcal{I}^*|$

Example: $m = 1, k = 1$

$\mathcal{I}^* = \{\emptyset, \{g_1\}, \{{g_1}^{-1}\}, \{a_1\}, \{a_1, g_1\}, \{a_1, {g_1}^{-1}\}, \{e\}, \{g_1, e\}, \{{g_1}^{-1}, e\}, \{a_1, \mathrm{e}\}, \{a_1, g_1, \mathrm{e}\}, \{a_1, {g_1}^{-1}, e\}\}$

$|\mathcal{I}^*| = (3^1)2^{1+1} = 12$

An original matroid structure?

Earlier we saw the notion of independence used for $\mathcal{M}(G)$ was:
$\mathcal{I}_{\mathcal{M}(G)} = \{I \mid \forall x, y \in I, xy \neq e\}$

An original matroid structure?

Earlier we saw the notion of independence used for $\mathcal{M}(G)$ was:
$\mathcal{I}_{\mathcal{M}(G)} = \{I \mid \forall x, y \in I, xy \neq e\}$
Effectively, this made the identity and elements of order two 'dependent' elements, thus, they could never appear in any $I \in \mathcal{I}$.

An original matroid structure?

Earlier we saw the notion of independence used for $\mathcal{M}(G)$ was:
$\mathcal{I}_{\mathcal{M}(G)} = \{I \mid \forall x, y \in I, xy \neq e\}$
Effectively, this made the identity and elements of order two 'dependent' elements, thus, they could never appear in any $I \in \mathcal{I}$.

Question

What happens if we define a notion of independence in order to purposely exclude elements of higher order?

An original matroid structure?

$\mathcal{J}_k(G)$

We construct a new family of groupic matroid, $\mathcal{J}_k(G)$, with the following notion of independence:
$\mathcal{I}_{\mathcal{J}_k(G)} = \{I \mid \forall x \in I, x^k \neq e\}$

An original matroid structure?

$\mathcal{J}_k(G)$

We construct a new family of groupic matroid, $\mathcal{J}_k(G)$, with the following notion of independence:
$\mathcal{I}_{\mathcal{J}_k(G)} = \{I \mid \forall x \in I, x^k \neq e\}$

This does precisely what we desired: it makes every element of order k dependent, thus, not in any independent sets.

An original matroid structure?

$\mathcal{J}_k(G)$

We construct a new family of groupic matroid, $\mathcal{J}_k(G)$, with the following notion of independence:
$\mathcal{I}_{\mathcal{J}_k(G)} = \{I \mid \forall x \in I, x^k \neq e\}$

This does precisely what we desired: it makes every element of order k dependent, thus, not in any independent sets.
Thus, $\mathcal{J}_k(G) = (\mathrm{G}, \mathcal{I}_{\mathcal{J}_k(G)})$.

An original matroid structure?

Example: $\mathcal{J}_3(\mathbb{Z}_4)$

The ground set is once again $\{0; 2; 1, 3\}$.

An original matroid structure?

Example: $\mathcal{J}_3(\mathbb{Z}_4)$

The ground set is once again $\{0; 2; 1, 3\}$.
However, as the operator is addition, only elements $x \mid 3x \not\equiv 0 \pmod 4$ are independent, and can appear in an independent set.

An original matroid structure?

Example: $\mathcal{J}_3(\mathbb{Z}_4)$

The ground set is once again $\{0; 2; 1, 3\}$.
However, as the operator is addition, only elements $x \mid 3x \not\equiv 0 \pmod 4$ are independent, and can appear in an independent set.
These are: 1, 2, 3.

An original matroid structure?

Example: $\mathcal{J}_3(\mathbb{Z}_4)$

The ground set is once again $\{0; 2; 1, 3\}$.
However, as the operator is addition, only elements $x \mid 3x \not\equiv 0 \pmod 4$ are independent, and can appear in an independent set.
These are: 1, 2, 3.

Thus, $\mathcal{I}_{\mathcal{J}_3(\mathbb{Z}_4)} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

An original matroid structure?

Example: $\mathcal{J}_3(\mathbb{Z}_4)$

The ground set is once again $\{0;\ 2;\ 1,\ 3\}$.
However, as the operator is addition, only elements $x \mid 3x \not\equiv 0 \pmod 4$ are independent, and can appear in an independent set.
These are: 1, 2, 3.

Thus, $\mathcal{I}_{\mathcal{J}_3(\mathbb{Z}_4)} = \{\emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1,2\},\ \{1,3\},\ \{2,3\},\ \{1,2,3\}\}$
Thus, $\mathcal{J}_3(\mathbb{Z}_4) = (\mathbb{Z}_4,\ \{\emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1,2\},\ \{1,3\},\ \{2,3\},\ \{1,2,3\}\})$.

An original matroid structure?

Theorem 3: $\mathcal{J}_k(G)$ is a matroid

To prove this, we must show that for any group, the matroid criteria hold for the constructed groupic matroid's $\mathcal{I}_{\mathcal{J}_k(G)}$:

1) $\emptyset \in \mathcal{I}_{\mathcal{J}_k(G)}$
2) If $I_1 \in \mathcal{I}_{\mathcal{J}_k(G)}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}_{\mathcal{J}_k(G)}$
3) If $I_1, I_2 \in \mathcal{I}_{\mathcal{J}_k(G)}$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}_{\mathcal{J}_k(G)}$

An original matroid structure?

Theorem 3: $\mathcal{J}_k(G)$ is a matroid

1) $\emptyset \in \mathcal{I}_{\mathcal{J}_k(G)}$

It is vacuously true to say that $\emptyset \in \mathcal{I}_{\mathcal{J}_k(G)}$ as every element $\in \emptyset$ does not have order k.

Theorem 3: $\mathcal{J}_k(G)$ is a matroid

2) If $I_1 \in \mathcal{I}_{\mathcal{J}_k(G)}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}_{\mathcal{J}_k(G)}$

Proof by contradiction: assume $I_1 \in \mathcal{I}_{\mathcal{J}_k(G)}$ and $I_2 \subseteq I_1$, and that $I_2 \notin \mathcal{I}_{\mathcal{J}_k(G)}$. This means that $\exists x \in I_2 \mid x^k = e$, where e is the group's identity element. However, since $x \in I_2$ and $I_2 \subseteq I_1$, $x \in I_1$. But, since $x^k = e$, this means that I_1 is not independent, a contradiction. Therefore, I_2 must also be independent.

An original matroid structure?

Theorem 3: $\mathcal{J}_k(G)$ is a matroid

3) If $I_1, I_2 \in \mathcal{I}_{\mathcal{J}_k(G)}$ and $|I_1| < |I_2|$, then $\exists x \in (I_2 \setminus I_1) \mid I_1 \cup \{x\} \in \mathcal{I}_{\mathcal{J}_k(G)}$

Since $|I_1| < |I_2|$, $\exists g \in I_2 \mid g \notin I_1$. However, by the notion of independence for $\mathcal{I}_{\mathcal{J}_k(G)}$, $g^k \neq e$. Since the notion of independence only references a single element, and not a pair of elements (as the previous notions did), $I_1 \cup \{g\} \in \mathcal{I}_{\mathcal{J}_k(G)}$.

An original matroid structure?

Theorem 3: $\mathcal{J}_k(G)$ is a matroid

Having proven that $\mathcal{J}_k(G)$ satisfies the three matroid criteria, we know that $\mathcal{J}_k(G)$ is indeed a matroid.

An original matroid structure?

Two insights may arise from this structure, as evidenced by the previous example:

An original matroid structure?

Two insights may arise from this structure, as evidenced by the previous example:

1) $\mathcal{I}_{\mathcal{J}_k(\mathbb{Z}_n)} = \mathcal{P}(\mathbb{Z}_n - \{0, a_1, a_2, ...a_m\})$, where a_i are the elements $x \in \mathbb{Z}_n \mid x^k = e$ (in other words, the elements of order k), and $\mathcal{P}(X)$ is the power set of the set X.

An original matroid structure?

Two insights may arise from this structure, as evidenced by the previous example:
1) $\mathcal{I}_{\mathcal{J}_k(\mathbb{Z}_n)} = \mathcal{P}(\mathbb{Z}_n - \{0, a_1, a_2, ...a_m\})$, where a_i are the elements $x \in \mathbb{Z}_n \mid x^k = e$ (in other words, the elements of order k), and $\mathcal{P}(X)$ is the power set of the set X.
2) $|\mathcal{I}_{\mathcal{J}_k(\mathbb{Z}_n)}| = 2^{(n-|\{0,a_1,a_2,...a_m\}|)}$

An original matroid structure?

Two insights may arise from this structure, as evidenced by the previous example:
1) $\mathcal{I}_{\mathcal{J}_k(\mathbb{Z}_n)} = \mathcal{P}(\mathbb{Z}_n - \{0, a_1, a_2, ...a_m\})$, where a_i are the elements $x \in \mathbb{Z}_n \mid x^k = e$ (in other words, the elements of order k), and $\mathcal{P}(X)$ is the power set of the set X.
2) $|\mathcal{I}_{\mathcal{J}_k(\mathbb{Z}_n)}| = 2^{(n - |\{0, a_1, a_2, ...a_m\}|)}$

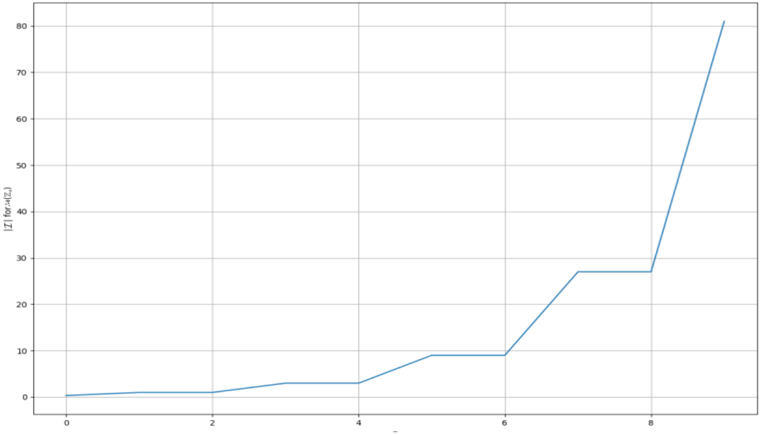
In our example:
1) $\mathcal{I}_{\mathcal{J}_3(\mathbb{Z}_4)} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\} = \mathcal{P}(\mathbb{Z}_4 - \{0\})$

An original matroid structure?

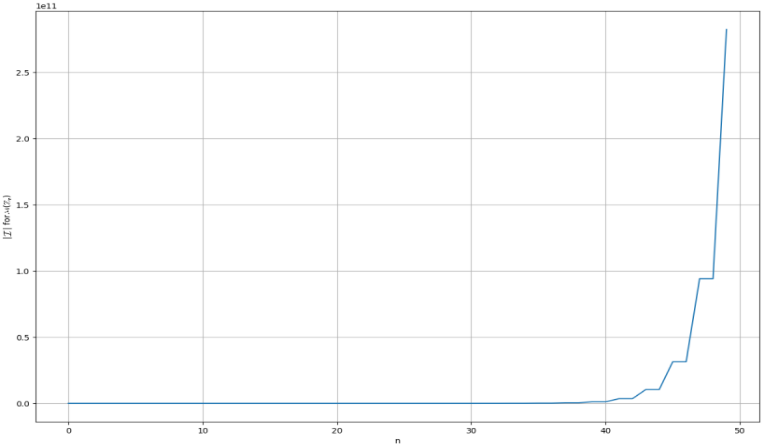
Two insights may arise from this structure, as evidenced by the previous example:
1) $\mathcal{I}_{\mathcal{J}_k(\mathbb{Z}_n)} = \mathcal{P}(\mathbb{Z}_n - \{0, a_1, a_2, ...a_m\})$, where a_i are the elements $x \in \mathbb{Z}_n \mid x^k = e$ (in other words, the elements of order k), and $\mathcal{P}(X)$ is the power set of the set X.
2) $|\mathcal{I}_{\mathcal{J}_k(\mathbb{Z}_n)}| = 2^{(n-|\{0,a_1,a_2,...a_m\}|)}$

In our example:
1) $\mathcal{I}_{\mathcal{J}_3(\mathbb{Z}_4)} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\} = \mathcal{P}(\mathbb{Z}_4 - \{0\})$
2) $|\mathcal{I}_{\mathcal{J}_3(\mathbb{Z}_4)}| = |\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}| = 8 = 2^{4-1} = 2^{4-|\{0\}|}$

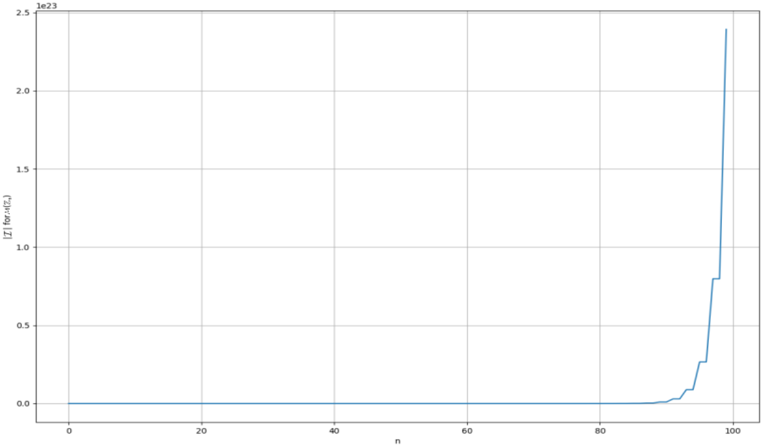
Graphics - $|\mathcal{I}_{\mathbb{Z}_n}|$, $n = 0...10$



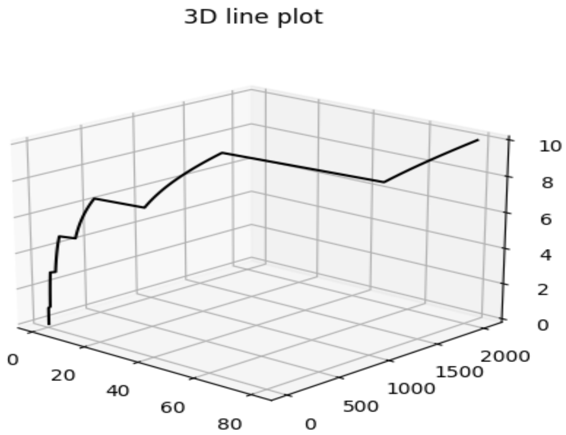
Graphics - $|\mathcal{I}_{\mathbb{Z}_n}|$, $n = 0...50$



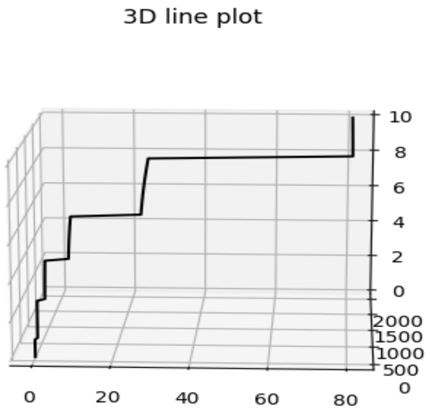
Graphics - $|\mathcal{I}_{\mathbb{Z}_n}|$, $n = 0 \ldots 100$



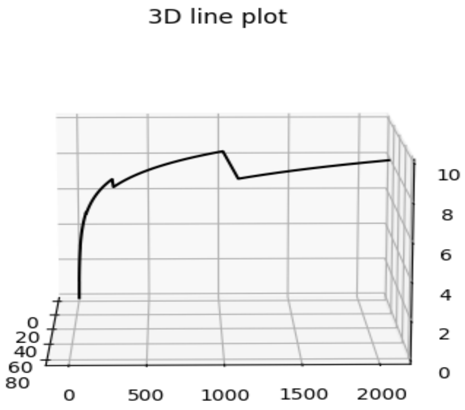
Graphics - $|\mathcal{I}^*|, m = 0...10, k = 0...10$



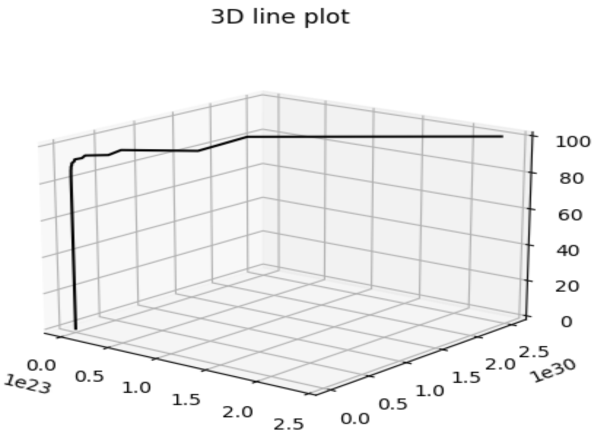
Graphics - $|\mathcal{I}^*|, m = 0...10, k = 0...10$



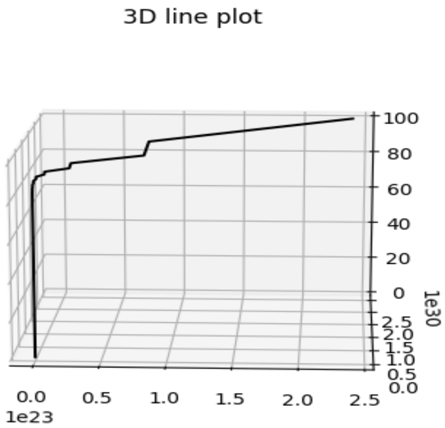
Graphics - $|\mathcal{I}^*|, m = 0...10, k = 0...10$



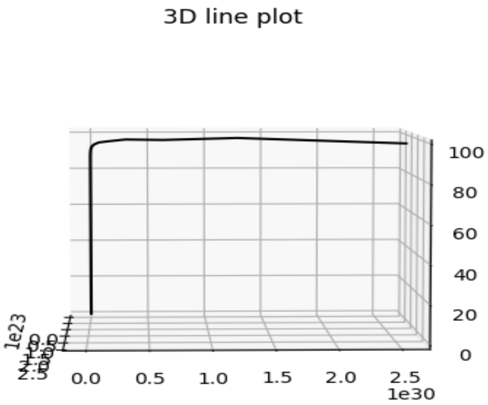
Graphics - $|\mathcal{I}^*|, m = 0...100, k = 0...100$



Graphics - $|\mathcal{I}^*|, m = 0...100, k = 0...100$



Graphics - $|\mathcal{I}^*|$, $m = 0...100$, $k = 0...100$



Conclusion

In this presentation, we defined:

Conclusion

In this presentation, we defined:

- Groups

Conclusion

In this presentation, we defined:

- Groups
- Matroids

Conclusion

In this presentation, we defined:

- Groups
- Matroids
- Three groupic matroids with differing independence notions

Conclusion

In this presentation, we defined:

- Groups
- Matroids
- Three groupic matroids with differing independence notions

We also:

Conclusion

In this presentation, we defined:

- Groups
- Matroids
- Three groupic matroids with differing independence notions

We also:

- Proved that all three groupic matroids are indeed matroids

Conclusion

In this presentation, we defined:

- Groups
- Matroids
- Three groupic matroids with differing independence notions

We also:

- Proved that all three groupic matroids are indeed matroids
- Determined the number of independent sets for two of the three groupic matroid structures

Conclusion

In this presentation, we defined:

- Groups
- Matroids
- Three groupic matroids with differing independence notions

We also:

- Proved that all three groupic matroids are indeed matroids
- Determined the number of independent sets for two of the three groupic matroid structures
- Showed how the number of independent sets changes as a function of the input group's order

Link to groupic matroid generator:
https://jgross11.github.io/GroupicMatroidGenerator.html