Multipartite Secret Sharing

Laszlo Csirmaz

UTIA, Prague
Rényi Institute, Budapest

CECC 2020
June 24–26, Zagreb
Contents

1 Secret sharing

2 Capped structures

3 Bipartite and tripartite ideal structures

4 Some proofs

5 Acknowledgments
Secret sharing by groups

- Participants are in disjoint groups

\[ P = P_1 \cup P_2 \cup \cdots \cup P_m. \]

Sometimes we call them *departments*.

- Members of each group play the same role

any participant can be replaced by any other member from
the same group.

- Interesting only if there are few groups and several members
in each group.

- Many unsolved problems

even for the bipartite (two groups) case.
Definitions

- **Access structure**
  is the collection of qualified sets.

- **Complexity**
  is the maximal relative share size; it is at least 1

- **Ideal structures**
  are the ones with minimal complexity 1.

- **κ-ideal structures**
  are where the entropy method gives the lower bound 1 on the complexity (not necessarily ideal).

Theorem (Brickell & Davenport – informal)

κ-ideal access structures and matroids are in a one-to-one correspondence.
The “cap” theorem

**Theorem (Csirmaz & Matúš & Padró – informal)**

Multipartite $\kappa$-ideal structures are the same as “capped” structures.

1. For $m = 1$ “capped” structures are just the threshold ones.
2. Recipe to list / generate / recognize all such structures.
3. For $m = 1$, $m = 2$, and $m = 3$ “capped” structures are linearly representable.

**Corollary**

We have a complete description of all ideal tripartite access structures.

4. For $m = 4$ there is a $\kappa$-ideal structure which is not ideal.
Contents

1. Secret sharing
2. Capped structures
3. Bipartite and tripartite ideal structures
4. Some proofs
5. Acknowledgments
Capped structures
Capped structures

Each subset \( A \) of the groups (departments) has a **cap** \( f(A) \).

Mnemonic: the power of the coalition \( A \) of some departments is limited to \( f(A) \) counts.

**Example:**
Departments: \( \{1, 2\} \); \( f(1) = a, f(2) = b, f(12) = c \):

\[
\begin{align*}
&b \quad \text{cap a for department 1} \\
&c
\end{align*}
\]
Capped structures

Each subset $A$ of the groups (departments) has a cap $f(A)$. 

Mnemonic: the power of the coalition $A$ of some departments is limited to $f(A)$ counts.

Example:
Departments: $\{1, 2\}$; $f(1) = a$, $f(2) = b$, $f(12) = c$:

The diagram illustrates the cap $b$ for department 2.
Capped structures

Each subset $A$ of the groups (departments) has a **cap** $f(A)$.

Mnemonic: the power of the coalition $A$ of some departments is limited to $f(A)$ counts.

**Example:**
Departments: $\{1, 2\}$; $f(1) = a$, $f(2) = b$, $f(12) = c$:

![Diagram showing capped structures with cap $c$ for both departments]
Hitting the cap \( c \)

As \( f(1) = a \), there must be at least \( c - a \) members from group \( 2 \).
Hitting the cap $c$

As $f(1) = a$, there must be at least $c-a$ members from group 2.
As $f(2) = b$, there must be at least $c-b$ members from group 1.
Hitting the cap $c$

As $f(1) = a$, there must be at least $c - a$ members from group 2. As $f(2) = b$, there must be at least $c - b$ members from group 1. And at least $c$ members from the two groups together.
The cap function $f$

Participants are in $m$ disjoint groups (departments)

$$P = P_1 \cup P_2 \cup \cdots \cup P_m.$$ 

For each subset $A$ of the groups $f(A)$ is the “cap” of $A$ so that

1. $f(\emptyset) = 0$, otherwise $f(A)$ is a positive integer,
2. $f$ is monotonic: $f(A) \leq f(A \cup B)$,
3. $f$ is submodular:

$$f(A) + f(B) \geq f(A \cap B) + f(A \cup B).$$

Otherwise there is no way to hit the the cap $f(A \cup B)$. 
In secret sharing a capped access structure is defined by

- the set of participants \( P \) who are in \( m \) disjoint groups:
  \[
  P = P_1 \cup P_2 \cup \cdots \cup P_m, 
  \]

- the cap function \( f(A) \) defined for each subset of the groups,

- an upward closed collection of group subsets:
  \[
  A = \{A_1, A_2, \ldots, A_t\} 
  \]

(if \( B \supset A_i \), then \( B \) is also in \( A \)).

**Definition (Capped access structure)**

A subset of participants is qualified if and only if they hit the cap \( f(A_i) \) for some \( A_i \in A \).
Case of two departments 1 and 2

\[ A = \{\textbf{12}\} \]

\[ A = \{\textbf{1, 12}\} \]

\[ A = \{\textbf{2, 12}\} \]

\[ A = \{\textbf{1, 2, 12}\} \]
Case of three departments 1, 2, 3

Seven cap values:

\[ f(123) \]
\[ f(12) \quad f(13) \quad f(23) \]
\[ f(1) \quad f(2) \quad f(3) \]

numerous possibilities for \( \mathcal{A} \), e.g.,

\[ \mathcal{A} = \{1, 12, 13, 123\}, \]
each yielding an ideal structure.
Contents

1. Secret sharing
2. Capped structures
3. Bipartite and tripartite ideal structures
4. Some proofs
5. Acknowledgments
The C-M-P theorem, main points

- $\Sigma$ is a $\kappa$-ideal multipartite structure with partition $\pi$.
- The matroid $M$ corresponds to $\Sigma$ (Brickell-Davenport thm).
- Factor $M$ by the partition to get $N = M/\pi$, an integer polymatroid on the partition groups.
  Note: the ranks of $N$ define the values!
- $M$ can be recovered from $N$ uniquely (due to the multipartite symmetry).
- The secret defines a one-point extension of $M$ (and of $N$) and it has rank 1. Qualified subsets are those whose rank is not increased by this extension.
- Such a one-point extension is characterized by a modular cut in the factor polymatroid $N$: this is the collection of all flats whose ranks do not increase – the collection $A$ in the examples.
**Tripartite \( \kappa \)-ideal structures are linear**

- In the tripartite case the factor polymatroid \( N \) is integer and it is on three points. Such polymatroids are known to be linear.

- **If** the one-point extension of \( N \) (by the secret) is linear, then \( M \) is linear. There are arbitrary large vector space representations and one can choose many “generic” elements.

- An integer polymatroid on \( a, b, c, d \) is linearly representable if and only if it satisfies all instances of the Ingleton inequality
  \[
  0 \leq \text{ING}(a, b, c, d) = f(ab) + f(ac) + f(ad) + f(bc) + f(bd) - f(a) - f(b) - f(abc) - f(abd) - f(cd).
  \]

- In any polymatroid, \( 2 \cdot \text{ING}(a, b, c, d) + f(s) \geq 0 \) where \( s \) is any of \( a, b, c, d \).

- The one-point extension \( N \cup \{s\} \) is integer with \( f(s) = 1 \). Thus \( \text{ING}(a, b, c, d) \) is integer and at least \(-1/2\), thus non-negative.
Contents

1. Secret sharing
2. Capped structures
3. Bipartite and tripartite ideal structures
4. Some proofs
5. Acknowledgments
This work has be done jointly with Fero Matúš † (Prague) and Carles Padró (Barcelona)

The research has been supported by grant GACR 19-045798

I would like to thank the organizers of the CECC’20 conference, and especially Andrej Dujella for their fantastic work.
Thank your for your attention