Simple Games and Ideal Secret Sharing Schemes

Arkadii Slinko

(joint research with Ali Hameed and Rupert Freeman)

Department of Mathematics
The University of Auckland

Workshop on Simple Games
Dauphine University, 27 September 2013

Plan for the Talk

- Introduction to Secret Sharing
- Introduction to Simple Games
- Composition of Games
- Main Result: Classification Weighted Ideal Secret Sharing Schemes

Plan for the Talk

- Introduction to Secret Sharing
- Introduction to Simple Games
- Composition of Games
- Main Result: Classification Weighted Ideal Secret Sharing Schemes

"Good friends, good books, and a sleepy conscience: this is the ideal life." — Mark Twain

Back in the USSR

The three top state officials, the President, the Prime Minister, and the Minister of Defence, all had "nuclear briefcases". Any two of them could authorise a launch of a nuclear warhead. No one could do it alone.

Back in the USSR

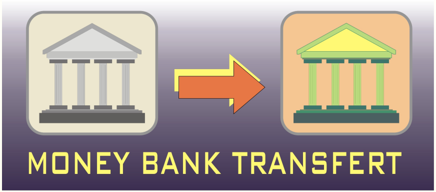
The three top state officials, the President, the Prime Minister, and the Minister of Defence, all had “nuclear briefcases”. Any two of them could authorise a launch of a nuclear warhead. No one could do it alone.

The secret (the launch code) was shared between three officials so that each pair of them could access the secret but no single agent could.

Opening vault

The secret combination opening the vault key must be distributed among bank employees. The bank policy requires the presence of three employees in opening the vault, but at least one of them must be a departmental manager.

Money Bank Transfert



If a significant sum of money is being transferred, an approval may require:

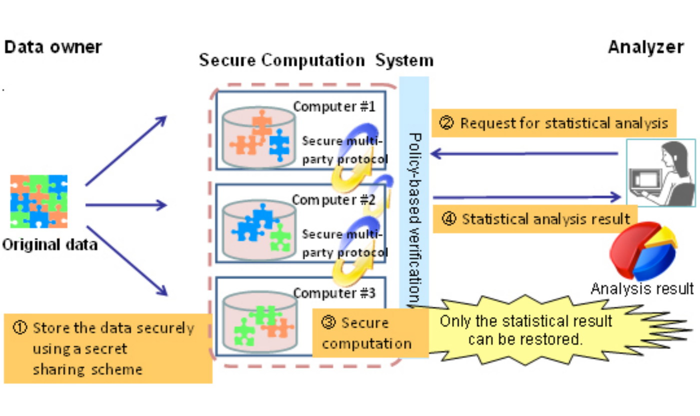
- approval of two vice-presidents, or
- three senior tellers; or
- a vice-president and two senior tellers.

Cloud computing

Cloud storage and cloud computing provides us with new security challenges.

Shamir's idea of storing sensitive data

For security data can be strored on several servers so that if some servers are compromised the data cannot be stolen and can be recovered from the remaining servers.



Idea of secret sharing

A secret sharing scheme ‘divides’ the secret S into ‘shares’ —one for every user—in such a way that:

- S can be easily reconstructed by any authorised coalition of users, but
- an unauthorised coalition of users cannot determine S.

Idea of secret sharing

A secret sharing scheme ‘divides’ the secret S into ‘shares’ —one for every user—in such a way that:

- S can be easily reconstructed by any authorised coalition of users, but
- an unauthorised coalition of users cannot determine S.

An economist can think about a solution concept of a cooperative game replacing money with information.

Idea of secret sharing

A secret sharing scheme ‘divides’ the secret S into ‘shares’ —one for every user—in such a way that:

- S can be easily reconstructed by any authorised coalition of users, but
- an unauthorised coalition of users cannot determine S.

An economist can think about a solution concept of a cooperative game replacing money with information.

The concept of authorised coalition must be formalised.

Access structure

The set $P = \{1, 2, \ldots, n\}$ denotes the set of users.

Access structure

The set $P = \{1, 2, \ldots, n\}$ denotes the set of users.

Definition

An access structure is a pair $G = (P, W)$, where W is a subset of the power set 2^P, different from $\emptyset$, which satisfies the monotonicity condition:

if $X \in W$ and $X \subset Y \subseteq P$, then $Y \in W$.

Coalitions from W are called authorised. We also denote

$$L = 2^P \setminus W$$

and call coalitions from L unauthorised.

Access structure

The set $P = \{1, 2, \ldots, n\}$ denotes the set of users.

Definition

An access structure is a pair $G = (P, W)$, where W is a subset of the power set 2^P, different from $\emptyset$, which satisfies the monotonicity condition:

if $X \in W$ and $X \subset Y \subseteq P$, then $Y \in W$.

Coalitions from W are called authorised. We also denote

$$L = 2^P \setminus W$$

and call coalitions from L unauthorised.

The access structure is a simple game.

Access Structure. Example 1

In the nuke briefcases game, if the set of agents is $P = \{1, 2, 3\}$, then the access structure is

$$W = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

In a threshold access structure or k-out-of-n access structure a coalition is authorised if it contains at least k agents.

Access Structure. Example 2

If in the bank transfert game there are two vice-presidents v_1, v_2 and three senior tellers t_1, t_2, t_3, then the set of minimal authorised coalitions is

$$\{\{v_1, v_2\}, \{t_1, t_2, t_3\}, \{v_1, t_1, t_2\}, \ldots, \{v_2, t_2, t_3\}\}.$$

Access Structure. Example 2

If in the bank transfert game there are two vice-presidents v_1, v_2 and three senior tellers t_1, t_2, t_3, then the set of minimal authorised coalitions is

$$\{\{v_1, v_2\}, \{t_1, t_2, t_3\}, \{v_1, t_1, t_2\}, \ldots, \{v_2, t_2, t_3\}\}.$$

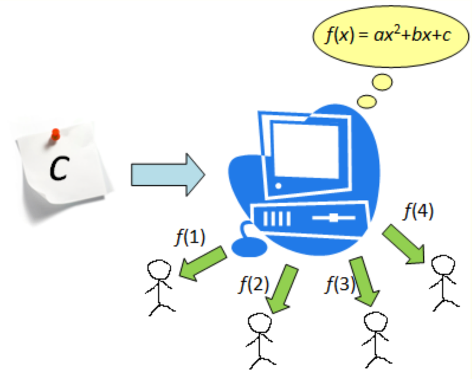
The access structure is fully defined by the set of minimal authorised coalitions.

Non-authorised coalition. Example

This is an old style of unauthorised coalition. These days the bad guys are armed with laptops.

Shamir's Scheme

Here is a pictorial interpretation of 3-out-of 4 scheme.



Any three would know the whole polynomial including *c*.

Ideal Secret Sharing Schemes

In situations like cloud storage the length of shares may represent a significant problem.

A secret sharing scheme is called ideal if it is

- perfect (revealing no information about the secret to non-authorised coalitions) and
- the size of the domain of secrets is the same as the domain of shares (it cannot be smaller in perfect schemes).

Ideal Secret Sharing Schemes

In situations like cloud storage the length of shares may represent a significant problem.

A secret sharing scheme is called ideal if it is

- perfect (revealing no information about the secret to non-authorised coalitions) and
- the size of the domain of secrets is the same as the domain of shares (it cannot be smaller in perfect schemes).

Shamir's secret sharing scheme is ideal.

Ideal Secret Sharing Schemes

In situations like cloud storage the length of shares may represent a significant problem.

A secret sharing scheme is called ideal if it is

- perfect (revealing no information about the secret to non-authorised coalitions) and
- the size of the domain of secrets is the same as the domain of shares (it cannot be smaller in perfect schemes).

Shamir's secret sharing scheme is ideal.

Here is a non-ideal access structure $\{\{1,2\},\{2,3\},\{3,4\}\}$.

Ideal Secret Sharing Schemes

In situations like cloud storage the length of shares may represent a significant problem.

A secret sharing scheme is called ideal if it is

- perfect (revealing no information about the secret to non-authorised coalitions) and
- the size of the domain of secrets is the same as the domain of shares (it cannot be smaller in perfect schemes).

Shamir's secret sharing scheme is ideal.

Here is a non-ideal access structure $\{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$.

Problem

Characterise access structures that can carry an ideal secret sharing scheme.

Example of Simple Game: UN Security Council

The 15 member UN Security Council consists of five permanent and 10 non-permanent countries. A passage requires:

- approval of at least nine countries,
- subject to a veto by any one of the permanent members.

Weighted Majority Games

This is the most known type of games.

Weighted Majority Games

This is the most known type of games.

Definition

A simple game G is called a weighted majority game if there exists a weight function $w\colon P \to \mathcal{R}^+$, where $\mathcal{R}^+$ is the set of all non-negative reals, and a real number q, called the quota, such that

$$X \in W \Longleftrightarrow \sum_{i \in X} w_i \geq q.$$

Weighted Majority Games

This is the most known type of games.

Definition

A simple game G is called a weighted majority game if there exists a weight function $w \colon P \to \mathcal{R}^+$, where $\mathcal{R}^+$ is the set of all non-negative reals, and a real number q, called the quota, such that

$$X \in W \Longleftrightarrow \sum_{i \in X} w_i \geq q.$$

Such game is denoted

$$[q; w_1, \ldots, w_n].$$

Weightedness of Games in Examples

Weightedness of Games in Examples

UN Security Council game is weighted:

$$[39; 7, 7, 7, 7, 7, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1].$$

Weightedness of Games in Examples

UN Security Council game is weighted:

$$[39; 7, 7, 7, 7, 7, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1].$$

Opening the vault game is not weighted:

$$(\{m_1, t_1, t_2\}, \{m_2, t_3, t_4\}; \{m_1, m_2\}, \{t_1, t_2, t_3, t_4\})$$

is a trading transform, which is a certificate of nonweightedness.

Comparing seniority of players

Given a game G we may also define a relation $\succeq_G$ on P by setting $i \succeq_G j$ if for every set $X \subseteq P$ not containing i and j

$$X \cup \{j\} \in W \Longrightarrow X \cup \{i\} \in W.$$

It is known as Isbell's desirability relation.

Comparing seniority of players

Given a game G we may also define a relation $\succeq_G$ on P by setting $i \succeq_G j$ if for every set $X \subseteq P$ not containing i and j

$$X \cup \{j\} \in W \Longrightarrow X \cup \{i\} \in W.$$

It is known as Isbell's desirability relation.

The game is called complete (also called directed and linear) if $\succeq_G$ is a total order.

Comparing seniority of players

Given a game G we may also define a relation $\succeq_G$ on P by setting $i \succeq_G j$ if for every set $X \subseteq P$ not containing i and j

$$X \cup \{j\} \in W \Longrightarrow X \cup \{i\} \in W.$$

It is known as Isbell's desirability relation.

The game is called complete (also called directed and linear) if $\succeq_G$ is a total order.

Any weighted game is complete.

Comparing seniority of players

Given a game G we may also define a relation $\succeq_G$ on P by setting $i \succeq_G j$ if for every set $X \subseteq P$ not containing i and j

$$X \cup \{j\} \in W \implies X \cup \{i\} \in W.$$

It is known as Isbell's desirability relation.

The game is called complete (also called directed and linear) if $\succeq_G$ is a total order.

Any weighted game is complete.

We also define $i \succ_G j$ as $i \succeq_G j$ but not $j \succeq_G i$.

Compressing information about the game

Many players in a game have equal status. Identifying equivalent players we get a multiset of players:

$$P = \{1^{n_1}, 2^{n_2}, \ldots, m^{n_m}\}.$$

A game with m equivalence classes is called m-partite.

Compressing information about the game

Many players in a game have equal status. Identifying equivalent players we get a multiset of players:

$$P = \{1^{n_1}, 2^{n_2}, \ldots, m^{n_m}\}.$$

A game with m equivalence classes is called m-partite.

UN Security Council is a bipartite game:

$$\{1^5, 2^{10}\}, \quad 1 \succ 2.$$

Compressing information about the game

Many players in a game have equal status. Identifying equivalent players we get a multiset of players:

$$P = \{1^{n_1}, 2^{n_2}, \ldots, m^{n_m}\}.$$

A game with m equivalence classes is called m-partite.

UN Security Council is a bipartite game:

$$\{1^5, 2^{10}\}, \quad 1 \succ 2.$$

Opening the vault game is also bipartite:

$$\{1^{n_1}, 2^{n_2}\}, \quad 1 \succ 2.$$

Compressing information about the game

Many players in a game have equal status. Identifying equivalent players we get a multiset of players:

$$P = \{1^{n_1}, 2^{n_2}, \ldots, m^{n_m}\}.$$

A game with m equivalence classes is called m-partite.

UN Security Council is a bipartite game:

$$\{1^5, 2^{10}\}, \quad 1 \succ 2.$$

Opening the vault game is also bipartite:

$$\{1^{n_1}, 2^{n_2}\}, \quad 1 \succ 2.$$

We have suppressed at this point the information about winning coalitions of those games.

Minimal and shift-minimal winning coalitions

Due to monotonic property the set of winning coalitions W is completely defined by the set

$$W^{\text{min}} = \{X \in W \mid \text{every proper subset of } X \text{ is losing}\}.$$

Minimal and shift-minimal winning coalitions

Due to monotonic property the set of winning coalitions W is completely defined by the set

$$W^{\min} = \{X \in W \mid \text{every proper subset of } X \text{ is losing}\}.$$

By a shift in a complete game we mean a replacement of a player in a coalition with less desirable player.

Minimal and shift-minimal winning coalitions

Due to monotonic property the set of winning coalitions W is completely defined by the set

$$W^{\text{min}} = \{X \in W \mid \text{every proper subset of } X \text{ is losing}\}.$$

By a shift in a complete game we mean a replacement of a player in a coalition with less desirable player.

The set of shift-minimal coalitions

$$W^{\text{smin}} = \{X \in W^{\text{min}} \mid \text{every shift of } X \text{ is losing}\}.$$

fully determines a complete game.

Compact presentation of shift-minimal winning coalitions

Compact presentation of shift-minimal winning coalitions

- UN Security Council game (has $\binom{10}{4}$ winning coalitions):

  $\{1^5, 2^{10}\}$, the type of shift-minimal winning coalitions is $\{1^5, 2^4\}$.

Compact presentation of shift-minimal winning coalitions

- UN Security Council game (has $\binom{10}{4}$ winning coalitions):

  $\{1^5, 2^{10}\}$, the type of shift-minimal winning coalitions is $\{1^5, 2^4\}$.

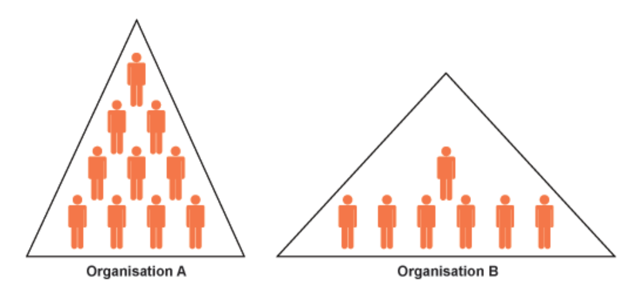
- Opening vault game:

  $\{1^{n_1}, 2^{n_2}\}$, the type of shift-minimal winning coalition is $\{1, 2^2\}$.

Composition of games (example)

The most general type of compositions of simple games was introduced by Shapley (1962).

We can take, for example, a unanimity game as a higher level game, i.e., both organisations must approve the decision.



Within each organisation we may use simple majority. This is how the European Union works.

Composition of games (formal definition)

We need a very partial case here rediscovered by Martin (1993) when only one member can be an organisation.

Composition of games (formal definition)

We need a very partial case here rediscovered by Martin (1993) when only one member can be an organisation.

Definition

Let $G = (P_G, W_G)$ and $H = (P_H, W_H)$ be two games defined on disjoint sets of players and $g \in P_G$. We define the composition game $C = G \circ_g H$ over g by defining $P_C = (P_G \setminus \{g\}) \cup P_H$ and

$$W_C = \{X \subseteq P_C \mid X_G \in W_G \text{ or } X_G \cup \{g\} \in W_G \text{ and } X_H \in W_H\},$$

where $X_G = X \cap P_G$ and $X_H = X \cap P_H$.

Composition of games (formal definition)

We need a very partial case here rediscovered by Martin (1993) when only one member can be an organisation.

Definition

Let $G = (P_G, W_G)$ and $H = (P_H, W_H)$ be two games defined on disjoint sets of players and $g \in P_G$. We define the composition game $C = G \circ_g H$ over g by defining $P_C = (P_G \setminus \{g\}) \cup P_H$ and

$$W_C = \{X \subseteq P_C \mid X_G \in W_G \text{ or } X_G \cup \{g\} \in W_G \text{ and } X_H \in W_H\},$$

where $X_G = X \cap P_G$ and $X_H = X \cap P_H$.

It expresses the idea that a collective member may be a player in the game.

Associativity of composition

Proposition

Let G, H, K be three games defined on the disjoint set of players and $g \in P_G$, $h \in P_H$. Then

$$(G \circ_g H) \circ_h K \cong G \circ_g (H \circ_h K),$$

that is the two products are isomorphic.

Associativity of composition

Proposition

Let G, H, K be three games defined on the disjoint set of players and $g \in P_G$, $h \in P_H$. Then

$$(G \circ_g H) \circ_h K \cong G \circ_g (H \circ_h K),$$

that is the two products are isomorphic.

Definition

A game G is said to be indecomposable if there does not exist two games H and K and $h \in P_H$ such that $\min(|H|, |K|) > 1$ and $G \cong H \circ_h K$.

Associativity of composition

Proposition

Let G, H, K be three games defined on the disjoint set of players and $g \in P_G$, $h \in P_H$. Then

$$(G \circ_g H) \circ_h K \cong G \circ_g (H \circ_h K),$$

that is the two products are isomorphic.

Definition

A game G is said to be indecomposable if there does not exist two games H and K and $h \in P_H$ such that $\min(|H|, |K|) > 1$ and $G \cong H \circ_h K$.

Example

Both UN Security Council game and Opening Vault game are indecomposable.

1-partite games

Since all n players are equivalent, there exist k such that it takes k or more players to win. Such a game is called k-out-of-n game, denoted $H_{n,k}$.

1-partite games

Since all n players are equivalent, there exist k such that it takes k or more players to win. Such a game is called k-out-of-n game, denoted $H_{n,k}$.

It is weighted and its voting representation is

$$[k; 1, \ldots, 1].$$

1-partite games

Since all n players are equivalent, there exist k such that it takes k or more players to win. Such a game is called k-out-of-n game, denoted $H_{n,k}$.

It is weighted and its voting representation is

$$[k; 1, \ldots, 1].$$

$H_{n,k}$ is indecomposable for $1 < k < n$.

1-partite games

Since all n players are equivalent, there exist k such that it takes k or more players to win. Such a game is called k-out-of-n game, denoted $H_{n,k}$.

It is weighted and its voting representation is

$$[k; 1, \ldots, 1].$$

$H_{n,k}$ is indecomposable for $1 < k < n$.

The game $H_{n,n}$ is special and is called the unanimity game on n players. We will denote it as U_n. Only U_2 is indecomposable.

1-partite games

Since all n players are equivalent, there exist k such that it takes k or more players to win. Such a game is called k-out-of-n game, denoted $H_{n,k}$.

It is weighted and its voting representation is

$$[k; 1, \ldots, 1].$$

$H_{n,k}$ is indecomposable for $1 < k < n$.

The game $H_{n,n}$ is special and is called the unanimity game on n players. We will denote it as U_n. Only U_2 is indecomposable.

The game $H_{n,1}$ does not have a name in the literature. We will call it anti-unanimity game and denote A_n. Only A_2 is indecomposable.

Compositions and completeness

Lemma

Let G, H be two games on disjoint sets of players and H is neither an anonymity nor an anti-unanimity game.

- *If for two elements $g, g' \in P_G$ we have $g \succ g'$ (and g' is not a dummy), then $G \circ_g H$ is not complete;*
- *If G and H are complete and $g \in P_G$ is a member of the weakest desirability class of G, then $G \circ_g H$ is complete.*

So, in the future we will compose complete games only through a player from the least desirable class.

The semigroup of complete games

Theorem (Freeman-Slinko, 2012)

Let $\mathcal{G}$ be the set of all complete games. Then $\mathcal{G}$, equipped with the operation of composition, is a semigroup with identity. Every $G \in \mathcal{G}$ can be expressed uniquely as a product of indecomposable games in this semigroup.

The semigroup of complete games

Theorem (Freeman-Slinko, 2012)

Let $\mathcal{G}$ be the set of all complete games. Then $\mathcal{G}$, equipped with the operation of composition, is a semigroup with identity. Every $G \in \mathcal{G}$ can be expressed uniquely as a product of indecomposable games in this semigroup.

Corollary

Every weighted simple game can be expressed uniquely as a product of indecomposable weighted simple games.

Counterexample

Do weighted games form a subsemigroup? No.

Counterexample

Do weighted games form a subsemigroup? No.

Example

Let G be defined on $P_G = \{1^2, 2^4\}$ and H on $P_H = \{3^3\}$ with weighted voting representations

$$[7; 3, 3, 2, 2, 2, 2] \quad \text{and} \quad H = [2; 1, 1, 1],$$

respectively. Let $g \in G$ be one of the players of weight 2. Then the composition $G \circ_g H$ is not weighted:

$$(\{1, 2, 3^2\}, \{1, 2, 3^2\}; \{1^2, 3\}, \{2^2, 3^3\}).$$

as this is a certificate of nonweightedness.

Two Major Theorems

Theorem (Beimel-Tassa-Weinreb, 2008)

Every ideal weighted game is a composition of indecomposable ideal weighted games.

Two Major Theorems

Theorem (Beimel-Tassa-Weinreb, 2008)

Every ideal weighted game is a composition of indecomposable ideal weighted games.

Theorem (Farràs-Padró, 2010)

Any indecomposable ideal weighted game belongs to one of the seven following types:

Onepartite: *k-out-of-n games - type* $\mathbf{H}$;

Bipartite: *types* $\mathbf{B_1}, \mathbf{B_2}, \mathbf{B_3}$;

Tripartite: *types* $\mathbf{T_1}, \mathbf{T_2}, \mathbf{T_3}$;

Two Major Theorems

Theorem (Beimel-Tassa-Weinreb, 2008)

Every ideal weighted game is a composition of indecomposable ideal weighted games.

Theorem (Farràs-Padró, 2010)

Any indecomposable ideal weighted game belongs to one of the seven following types:

- Onepartite: *k-out-of-n games - type* $\mathbf{H}$;
- Bipartite: *types* $\mathbf{B_1}, \mathbf{B_2}, \mathbf{B_3}$;
- Tripartite: *types* $\mathbf{T_1}, \mathbf{T_2}, \mathbf{T_3}$;

We have shown however that games of type $\mathbf{T_2}$ are decomposable.

Classification of Ideal Weighted Simple Games

Theorem (Hameed, Slinko, 2013)

G is an ideal weighted simple game if and only if

$$G = H_1 \circ \ldots \circ H_s \circ I \circ A_n \quad (s \geq 0);$$

where H_i is an indecomposable 1-partite game.

Also, I is an indecomposable game of types $\boldsymbol{B}_1$, $\boldsymbol{B}_2$, $\boldsymbol{B}_3$, $\boldsymbol{T}_1$, $\boldsymbol{T}_3$, and A_n is the anti-unanimity game on n players.

Moreover, A_n can be present only if I is either absent or it is of type $\boldsymbol{B}_2$.

This decomposition is unique.

The full paper is on ArXiv:

http://arxiv.org/abs/1308.3763

Any comments will be greatly appreciated.

The full paper is on ArXiv:

http://arxiv.org/abs/1308.3763

Any comments will be greatly appreciated.

Thank you for your attention!