

Research Article

Ali Hameed and Arkadii Slinko

A characterisation of ideal weighted secret sharing schemes

Abstract: Beimel, Tassa and Weinreb [2] and Farràs and Padró [9] partially characterised access structures of ideal weighted secret sharing schemes in terms of the operation of composition. They proved that any weighted ideal access structure is a composition of indecomposable ones. Farràs and Padró gave a list of seven classes of access structures – one unipartite, three bipartite and three tripartite – to which all weighted ideal indecomposable access structures may belong. In this paper we determine exactly which access structures from those classes are indecomposable. We also determine which compositions of indecomposable weighted access structures are again weighted and obtain an if-and-only-if characterisation of ideal weighted secret sharing schemes. We use game-theoretic techniques to achieve this.

Keywords: Secret sharing scheme, access structure, simple game, composition of games

MSC 2010: 94A62, 91A80, 91A12

Ali Hameed, Arkadii Slinko: Department of Mathematics, The University of Auckland, Private Bag 92019, Auckland 1142, New Zealand, e-mail: aham002@aucklanduni.ac.nz, a.slinko@auckland.ac.nz

Communicated by: Tor Helleseth

1 Introduction

A secret sharing scheme divides a secret into shares – which are then distributed among participating agents – so that some coalitions of agents have enough information to recover the secret (authorised coalitions) and some (non-authorised coalitions) do not. Secret-sharing schemes are used in cryptography in many different ways. Originally, they were introduced for secure storage of valuable information such as cryptographic keys, missile launch codes and numbered bank accounts but gradually have found numerous other applications in cryptography and distributed computing, e.g., Byzantine agreement, secure multi-party computations, threshold cryptography, access control, attribute-based encryption, and generalised oblivious transfer [1].

The set of authorised coalitions is said to be the access structure. A scheme is called perfect if it gives no information to non-authorised coalitions whatsoever. A perfect scheme has the shortest possible shares if the lengths of the shares in bits are the same as the length of the secret [13]; such schemes are called ideal.

However, not all access structures can carry an ideal secret sharing scheme [3, 20]. Finding a description of those which can carry appeared to be quite difficult. A major milestone in this direction was the paper by Brickell and Davenport [5] who showed that all ideal secret sharing schemes can be obtained from matroids. Not all matroids, however, define ideal schemes [17] so the problem is reduced to classifying those matroids that do. There was little further progress, if any, in this direction.

Several authors, however, successfully classified all ideal access structures in several subclasses of secret sharing schemes. These include access structures defined by graphs [5], weighted (threshold) access structures [2, 9], hierarchical access structures [9], bipartite and tripartite access structures [8, 15, 16]. While in the classes of bipartite and tripartite access structures the ideal ones were given explicitly, for the case of weighted access structures, Beimel, Tassa and Weinreb [2] suggested a new kind of description. Their method uses the operation of composition of access structures [14]. The idea is that sometimes all users can be classified into ‘strong’ users and ‘weak’ users and the access structure can be decomposed into the main access structure that contains the strong users and the auxiliary access structure which contains the weak users. The operation of composition of access structures used here was suggested by Martin [14] and was a particular

case of the construction suggested by Shapley [19]. Under this approach the first task is obtaining a characterisation of indecomposable structures. Beimel, Tassa and Weinreb [2] proved that every ideal indecomposable secret sharing scheme is either disjunctive hierarchical or tripartite. Farràs and Padró [9, 10] later described seven classes of access structures (one unipartite, three bipartite and three tripartite) to which an indecomposable ideal secret sharing scheme may belong. However, Farràs and Padró did not investigate which access structures from these classes were actually indecomposable. We do this in the present paper.

If a composition of two weighted access structures were again a weighted structure there will not be need to do anything else. However, we will show that this is not true. Since the composition of two weighted access structures may not be again weighted, it is not clear which indecomposable structures and in which numbers can be combined to obtain more complex weighted access structures. To answer this question in this paper we undertake a thorough investigation of the operation of composition. Since the access structure of any secret sharing scheme is a simple game in the sense of von Neumann and Morgenstern [22], we found it more convenient to use game-theoretic methods and terminology.

Section 2 of the present paper gives the background in secret sharing and simple games. We introduce some important concepts from game theory, like Isbel's desirability relation on players, which will play in this paper an important role. We remind the reader of the concept of complete simple game which is a simple game for which Isbel's desirability relation is complete. (In [9] such games are called hierarchical.) We introduce the technique of trading transforms and certificates of non-weightedness [12] for deciding if a simple game is weighted or not.

In Section 3, we give the motivation for the concept of composition $C = G \circ_g H$ of two games G and H over an element $g \in G$, give the definition and examples. The essence of this construction is as follows: in the first game G we choose an element $g \in G$ and replace it with the second game H . The winning coalitions in the new game are of two types. Firstly, every winning coalition in G that does not contain g remains winning in C . A winning coalition in G which contained g needs a winning coalition of H to be added to it to become winning in C . We prove several properties of this operation, in particular, we prove that the operation of composition of games is associative.

Section 4 presents preliminary results regarding the compositions of ideal games and weighted games in general. We start with reminding the reader that the composition of two games is ideal if and only if the two games being composed are ideal [2]. Then we show that if a weighted game is composed of two games, then the two composed games are also weighted. Finally, we prove the first sufficient condition for a composition to be weighted.

Section 5 is devoted to compositions in the class of complete games. We prove that, with few possible exceptions, the composition of two complete games is complete if and only if the composition is over the weakest player relative to the desirability relation of the first game. We show that the composition of two weighted simple games may not be weighted even if we compose over the weakest player. We give some sufficient conditions for the composition of two weighted games to be weighted.

In Section 6 we recap the description of the seven classes of ideal weighted simple games given by Farràs and Padró [9] to which an indecomposable ideal weighted game must belong. According to [9] all ideal indecomposable games are either k -out-of- n games or belong to one of the six classes: \mathbf{B}_1 , \mathbf{B}_2 , \mathbf{B}_3 , \mathbf{T}_1 , \mathbf{T}_2 , \mathbf{T}_3 . We show that some of the games in these classes are in fact decomposable and, in particular, the whole class \mathbf{T}_2 , and hence obtain an exact account of all indecomposable ideal weighted simple games.

In Section 7 we investigate which of the indecomposable ideal weighted simple games can be composed to obtain a new ideal weighted simple game. The result is quite striking; the composition of two indecomposable weighted games is weighted only in two cases: when the first game is a k -out-of- n game, or if the first game is of type \mathbf{B}_2 (from the Farràs and Padró list) and the second game is an anti-unanimity game where all players are passers, i.e., players that can win without forming a coalition with other players. This has a major implication for the refinement of the Beimel–Tassa–Weinreb–Farràs–Padró theorem.

In Section 8, using the results of Section 7, we show that a game G is an ideal weighted simple game if and only if it is a composition

$$G = H_1 \circ \cdots \circ H_s \circ I \circ A_n,$$

where H_i is an indecomposable k_i -out-of- n_i game (these are classified) for each $i = 1, 2, \dots, s$, and A_n is an anti-unanimity game, and I is an indecomposable game of types B_1, B_2, B_3, T_1 , and T_3 . Any of these may be absent but A_n may appear only if I is of type B_2 . The main surprise in this result is that in the decomposition there may be at most one game of types B_1, B_2, B_3, T_1, T_3 .

2 Preliminaries

2.1 Secret sharing schemes

Suppose n agents from set $A = \{1, 2, \dots, n\}$ agreed to share a secret in such a way that only some specified coalitions (subsets) of A are authorised to know the secret. In other words a certain access structure to the secret is put in place. An *access structure* is any subset $\emptyset \neq W \subseteq 2^A$ such that

$$\text{if } X \in W \text{ and } X \subseteq Y, \text{ then } Y \in W, \quad (2.1)$$

reflecting the fact that if a smaller coalition knows the secret, then the larger one will know it too. The access structure is public knowledge and all agents know it. Due to the monotonicity requirement (2.1) the access structure is completely defined by its minimal authorised coalitions. It is normally assumed that every agent participates in at least one minimal authorised coalition.

Let S_0, S_1, \dots, S_n be finite sets where S_0 will be interpreted as a set of all possible secrets and S_i is the set of all possible ‘shares of the secret’ that can be given to agent i . Any subset

$$\mathcal{T} \subseteq S_0 \times S_1 \times \dots \times S_n$$

will be called a *distribution table*. If a secret $s_0 \in S_0$ is to be distributed among agents, then an n -tuple

$$(s_0, s_1, \dots, s_n) \in \mathcal{T}$$

is chosen by the dealer at random according to some probability distribution among those tuples whose first coordinate is s_0 and then agent i gets the share $s_i \in S_i$. A *secret sharing scheme* is a family of triples $\mathcal{S} = (W, \mathcal{T}, f_X)_{X \in W}$, where W is an access structure, \mathcal{T} is a distribution table, and for every authorised coalition $X = \{i_1, \dots, i_k\} \in W$ the function (algorithm)

$$f_X: S_{i_1} \times \dots \times S_{i_k} \rightarrow S_0$$

satisfies $f_X(s_{i_1}, s_{i_2}, \dots, s_{i_k}) = s_0$ for every $(s_0, s_1, \dots, s_n) \in \mathcal{T}$. The family $(f_X)_{X \in W}$ is said to be the *family of secret recovery functions*.

Example 2.1. Consider the following secret sharing scheme with n users for which the only authorised coalition will be the grand coalition, that is the set $A = \{1, 2, \dots, n\}$. We take a group G and set $S_i = G$ for all $i = 0, 1, \dots, n$. Given a secret $s \in G$ to share, the dealer may, for example, generate $n - 1$ random elements $s_1, \dots, s_{n-1} \in G$, set $g_i = s_i$ for $i = 1, \dots, n - 1$, and calculate $g_n = s - (g_1 + \dots + g_{n-1})$. Then he may give share g_i to agent i . The distribution table \mathcal{T} will consist of all n -tuples (g_0, g_1, \dots, g_n) such that $\sum_{i=1}^n g_i = g_0$ and the secret recovery function (the only one since we have only one authorised coalition) will be

$$f_A(g_1, \dots, g_n) = g_1 + \dots + g_n.$$

Definition 2.2. A secret sharing scheme $\mathcal{S} = (W, \mathcal{T}, f_X)_{X \in W}$ is called *perfect* if for every non-authorised subset $\{j_1, \dots, j_m\} \subset A$, for every sequence of elements $s_{j_1}, s_{j_2}, \dots, s_{j_m}$, such that $s_{j_r} \in S_{j_r}$, and for every two secrets $s, s' \in S_0$ the probability of a tuple $(s, \dots, s_{j_1}, \dots, s_{j_m}, \dots)$ is the same as the probability of a tuple $(s', \dots, s_{j_1}, \dots, s_{j_m}, \dots)$.

In a perfect scheme a non-authorised coalition has no information about the secret whatsoever. The scheme from Example 2.1 is obviously perfect. Another perfect secret sharing scheme is the famous Shamir’s secret sharing.

Example 2.3 (Shamir 1979). Suppose that we have n agents and the access structure is now

$$W = \{X \subseteq A \mid |X| \geq k\},$$

i.e. a coalition is authorised if it contains at least k agents. Let F be a large finite field and we will have $S_i = F$ for $i = 0, 1, 2, \dots, n$. Let a_1, \dots, a_n be distinct fixed nonzero elements of F .

Suppose $s \in F$ is the secret to share. The dealer sets $t_0 = s$ and generates randomly $t_1, \dots, t_{k-1} \in F$. He forms the polynomial $p(x) = t_0 + t_1x + \dots + t_{k-1}x^{k-1}$. Then he gives the share $s_i = p(a_i)$ to agent i . (Note that $p(0) = s_0 = s$.) Suppose now $X = \{i_1, \dots, i_k\}$ is a minimal authorised coalition. Then the secret recovery function is

$$f_X(s_{i_1}, \dots, s_{i_k}) = \sum_{r=1}^k s_{i_r} \prod_{j \neq r} \frac{a_{i_j}}{a_{i_j} - a_{i_r}}.$$

This is the value at zero of Lagrange's interpolation polynomial

$$\sum_{r=1}^k p(a_{i_r}) \prod_{j \neq r} \frac{a_{i_j} - x}{a_{i_j} - a_{i_r}},$$

which is equal to $p(x)$.

The access structure from Example 2.3 is called *threshold access structure* or k -out-of- n access structure. It is not difficult to see that it is perfect. It is known [3] that for any access structure W there exists a perfect secret sharing scheme which realises W .

Karnin, Greene and Hellman [13] showed that in a perfect secret sharing scheme $|S_i| \geq |S_0|$ for all $i = 1, \dots, n$; so a secret sharing scheme has the shortest possible shares if the domain of the secrets and the domains of users' shares are of the same size.

Definition 2.4. A secret sharing scheme $\mathcal{S} = (W, \mathcal{T}, f_X)_{X \in W}$ is called *ideal* if it is perfect and $|S_i| = |S_0|$ for all $i = 1, \dots, n$.

Shamir's secret sharing scheme is obviously ideal.

Classification of ideal secret sharing schemes have been a central topic of the theory of secret sharing for some time and the problem is far from being solved. Brickell and Davenport [5] showed that there is a unique matroid associated with every ideal secret sharing scheme. At the same time there are matroids that do not correspond to any. The problem appeared to be easier in the subclass of weighted secret sharing schemes to which this paper is devoted. At the end we will give a complete classification.

2.2 Simple games

The main motivation for this work comes from secret sharing. However, the access structure on the set of users is a *simple game* on that set, so we will use game-theoretic terminology.

Definition 2.5 (von Neumann and Morgenstern 1944). A simple game is a pair $G = (P_G, W_G)$, where P_G is a set of players and $\emptyset \neq W_G \subseteq 2^{P_G}$ is a nonempty set of coalitions which satisfies the monotonicity condition:

$$\text{if } X \in W_G \text{ and } X \subseteq Y, \text{ then } Y \in W_G.$$

Coalitions from set W_G are called *winning*, the remaining ones are called *losing*.

We will say that a coalition X is a *minimal winning coalition* if every proper subset of X is losing.

A typical example of a simple game is the United Nations Security Council, which consists of five permanent members and ten non-permanent. The passage of a resolution requires that all five permanent members vote for it, and also at least nine members in total. The book by Taylor and Zwicker [21] gives many other interesting examples.

A simple game will be called just a game. The set W_G of winning coalitions of a game G is completely determined by the set W_G^{\min} of its minimal winning coalitions. A player which does not belong to any minimal winning coalitions is called a *dummy*. He can be removed from any winning coalition without making it losing. A player who is contained in every minimal winning coalition is called a *vetoer*. A game with a unique minimal winning coalition is called an *oligarchy*. In an oligarchy every player is either a vetoer or a dummy. A player who alone forms a winning coalition is called a *passer*. A game in which all minimal winning coalitions are singletons is called *anti-oligarchy*. In an anti-oligarchy every player is either a passer or a dummy.

Definition 2.6. A simple game G is called *weighted game* if there exist nonnegative weights w_1, \dots, w_n and a real number q , called *quota*, such that

$$X \in W_G \Leftrightarrow \sum_{i \in X} w_i \geq q.$$

This game is denoted $[q; w_1, \dots, w_n]$. We call such a game simply *weighted*.

It is easy to see that the United Nations Security Council can be defined in terms of weights as

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

In secret sharing weighted access structures were introduced by Shamir and Blakley [4, 18].

For $X \subset P$ we will denote its complement $P \setminus X$ by X^c .

Definition 2.7. Let $G = (P, W)$ be a simple game and $A \subseteq P$. Let us define subsets

$$W_{sg} = \{X \subseteq A^c \mid X \in W\}, \quad W_{rg} = \{X \subseteq A^c \mid X \cup A \in W\}.$$

Then the game $G_A = (A^c, W_{sg})$ is called a *subgame* of G and $G^A = (A^c, W_{rg})$ is called a *reduced game* of G .

The two main concepts of the theory of games that we will need here are as follows.

Given a simple game G on the set of players P we 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 ,

$$X \cup \{j\} \in W_G \Rightarrow X \cup \{i\} \in W_G. \quad (2.2)$$

In such case we will say that i is at least as *desirable* (as a coalition partner) as j . In the United Nations Security Council every permanent member will be more desirable than any non-permanent one. This relation is reflexive and transitive but not always complete (total) (e.g., see [6]). The corresponding equivalence relation on $[n]$ will be denoted by \sim_G and the strict desirability relation by $>_G$. If this can cause no confusion, we will omit the subscript G .

Definition 2.8. Any game with complete desirability relation is called *complete*.

Example 2.9. Any weighted game is complete.

We note that in (2.2) we can choose X which is minimal with this property in which case $X \cup \{i\}$ will be a minimal winning coalition. Hence the following is true.

Proposition 2.10. Given a complete simple game G on the set of players P and two players $i, j \in P$, the relation $i >_G j$ is equivalent to the existence of a minimal winning coalition X which contains i but not j such that $(X \setminus \{i\}) \cup \{j\}$ is losing.

Proof. Suppose $i >_G j$. Then there exists a coalition Y such that $Y \cup \{j\}$ is losing but $Y \cup \{i\}$ is winning. We can take a minimal coalition Y with this property. Then Y is a losing coalition, otherwise $Y \cup \{j\}$ would be also winning. We see now that $X = Y \cup \{i\}$ is winning but becomes losing if any of its elements is removed. It also becomes losing if i is replaced by j . So X is the coalition sought for. The converse is clear due to completeness of G . \square

Let $G = (P, W)$ be a game. A sequence of coalitions of even length

$$\mathcal{T} = (X_1, \dots, X_j; Y_1, \dots, Y_j) \quad (2.3)$$

is a *trading transform* if $|\{i : a \in X_i\}| = |\{i : a \in Y_i\}|$ for all $a \in P$ (see [21]). It is worth noting that while in (2.3) we can consider that no X_i coincides with any of Y_k (otherwise both can be removed), it is perfectly possible that the sequence X_1, \dots, X_j has some equal terms; the sequence Y_1, \dots, Y_j can also contain equal terms.

Elgot [7] proved (see also [21]) the following fundamental fact.

Theorem 2.11. *A game G is a weighted game if and only if for no integer j there exists a trading transform (2.3) such that all coalitions X_1, \dots, X_j are winning and all Y_1, \dots, Y_j are losing.*

Due to this theorem any trading transform (2.3) where all coalitions X_1, \dots, X_j are winning and all Y_1, \dots, Y_j are losing is called a *certificate of non-weightedness* [12].

Completeness can also be characterised in terms of trading transforms [21].

Theorem 2.12. *A game G is complete if and only if no certificate of non-weightedness exists of the form*

$$\mathcal{T} = (X \cup \{x\}, Y \cup \{y\}; X \cup \{y\}, Y \cup \{x\}). \quad (2.4)$$

We call (2.4) a *certificate of incompleteness*. This theorem says that completeness is equivalent to the impossibility for two winning coalitions to swap two players and become both losing. This latter property is also called *swap robustness*.

A complete game $G = (P, W)$ can be compactly represented using multisets. All its players are split into equivalence classes of players of equal desirability. If, say, we have m equivalence classes, i.e., $P = P_1 \cup P_2 \cup \dots \cup P_m$ with $|P_i| = n_i$, then we can think that P is the multiset $\{1^{n_1}, 2^{n_2}, \dots, m^{n_m}\}$. A submultiset $\{1^{\ell_1}, 2^{\ell_2}, \dots, m^{\ell_m}\}$ will then denote the class of coalitions where ℓ_i players come from P_i , $i = 1, \dots, m$. They are either all winning or all losing. We may enumerate classes so that $1 \succ_G 2 \succ_G \dots \succ_G m$. The game with m classes is called *m-partite*.

If a game G is complete, then we define *shift-minimal* [6] winning coalitions as follows. By a *shift* we mean a replacement of a player of a coalition by a less desirable player which did not belong to it. Formally, given a coalition X , player $p \in X$ and another player $q \notin X$ such that $q \prec_G p$, we say that the coalition $(X \setminus \{p\}) \cup \{q\}$ is obtained from X by a *shift*. A winning coalition X is *shift-minimal* if every coalition strictly contained in it and every coalition obtained from it by a shift are losing. A complete game is fully defined by its shift-minimal winning coalitions.

Now we will define the following three classes of games that play a crucial role in classification of ideal weighted secret sharing schemes [2, 9].

Unipartite games. Let $H_{n,k}$ be the game where there are n players and it takes k or more to win. Such games are called *k-out-of-n games*. Alternatively they can be characterised as the class of complete unipartite games, i.e., the games with a single class of equivalent players. The game $H_{n,n}$ is special and is called the *unanimity game* on n players. We will denote it as U_n . The game $H_{n,1}$ does not have a name in the literature. We will call it *anti-unanimity game* and denote A_n .

Bipartite games. Here we introduce two important types of bipartite games. A hierarchical disjunctive game $H_{\exists}(\mathbf{n}, \mathbf{k})$ with $\mathbf{n} = (n_1, n_2)$ and $\mathbf{k} = (k_1, k_2)$ on a multiset $P = \{1^{n_1}, 2^{n_2}\}$ is defined by the set of winning coalitions

$$W_{\exists} = \{\{1^{\ell_1}, 2^{\ell_2}\} \mid (\ell_1 \geq k_1) \vee (\ell_1 + \ell_2 \geq k_2)\},$$

where $1 \leq k_1 < k_2$, $k_1 \leq n_1$ and $k_2 - k_1 < n_2$. A hierarchical conjunctive game $H_{\forall}(\mathbf{n}, \mathbf{k})$ with $\mathbf{n} = (n_1, n_2)$ and $\mathbf{k} = (k_1, k_2)$ on a multiset $P = \{1^{n_1}, 2^{n_2}\}$ is defined by the set of winning coalitions

$$W_{\forall} = \{\{1^{\ell_1}, 2^{\ell_2}\} \mid (\ell_1 \geq k_1) \wedge (\ell_1 + \ell_2 \geq k_2)\},$$

where $1 \leq k_1 < k_2$, $k_1 \leq n_1$ and $k_2 - k_1 < n_2$. In both cases, if the restrictions on \mathbf{n} and \mathbf{k} are not satisfied, the game becomes unipartite or get dummies [11].

Tripartite games. Here we introduce two types of tripartite games. Let $\mathbf{n} = (n_1, n_2, n_3)$ and $\mathbf{k} = (k_1, k_2, k_3)$, where n_1, n_2, n_3 and k_1, k_2, k_3 are positive integers. The game $\Delta_1(\mathbf{n}, \mathbf{k})$ is defined on the multiset $P = \{1^{n_1}, 2^{n_2}, 3^{n_3}\}$ with the set of winning coalitions

$$\{\{1^{\ell_1}, 2^{\ell_2}, 3^{\ell_3}\} \mid (\ell_1 \geq k_1) \vee [(\ell_1 + \ell_2 \geq k_2) \wedge (\ell_1 + \ell_2 + \ell_3 \geq k_3)]\},$$

where

$$k_1 < k_3, \quad k_2 < k_3, \quad n_1 \geq k_1, \quad n_2 > k_2 - k_1 \quad \text{and} \quad n_3 > k_3 - k_2. \quad (2.5)$$

These, in particular, imply $n_1 + n_2 \geq k_2$.

The game $\Delta_2(\mathbf{n}, \mathbf{k})$ is for the case when $n_2 \leq k_2 - k_1$, and it is defined on the multiset $P = \{1^{n_1}, 2^{n_2}, 3^{n_3}\}$ with the set of winning coalitions

$$\{1^{\ell_1}, 2^{\ell_2}, 3^{\ell_3} \mid (\ell_1 + \ell_2 \geq k_2) \vee [(\ell_1 \geq k_1) \wedge (\ell_1 + \ell_2 + \ell_3 \geq k_3)]\},$$

where

$$k_1 < k_2 < k_3, \quad n_1 + n_2 \geq k_2, \quad n_3 > k_3 - k_2 \quad \text{and} \quad n_2 + n_3 > k_3 - k_1. \quad (2.6)$$

These conditions, in particular, imply $n_1 \geq k_1$ and $n_3 \geq 2$.

In both cases, if the restrictions on \mathbf{n} and \mathbf{k} are not satisfied, the game either contains dummies or becomes 2-partite or even unipartite (see a justification of this claim in Appendix A).

3 The operation of composition of games

The most general type of compositions of simple games was defined by Shapley [19]. We need a very partial case of that concept here which, in the context of secret sharing, was introduced by Martin [14].

Definition 3.1. 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 $C = G \circ_g H$ by setting $P_C = (P_G \setminus \{g\}) \cup P_H$ 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 $X_H = X \cap P_H$.

This is a ‘substitution’ of the game H instead of a single element g of the first game. All winning compositions in G not containing g remain winning in C . If a winning coalition of G contains g , then it remains winning in C if g is replaced with a winning coalition of H . One might imagine that, when a certain issue is voted in C , voters of H vote first and then their collective vote is counted in the first game as if it was a vote of player g . Such situation appears, for example, if a very experienced expert resigns from a company, they might wish to replace him with a group of experts.

Suppose $G = (P, W)$ and $G' = (P', W')$ are two games and $\sigma: P \rightarrow P'$ is a bijection. We say that σ is an *isomorphism* of G and G' , denoted $G \cong G'$, if $X \in W$ if and only if $\sigma(X) \in W'$.

Given a game $G = (P, W)$, by $|G|$ we denote the number of players in P . It is easy to see that if $|H| = 1$, then $H \circ_h K \cong K$, and if $|K| = 1$, then $H \circ_h K \cong H$.

Definition 3.2. A game G is said to be *indecomposable* if there do not exist two games H and K and $h \in P_H$ such that $\min(|H|, |K|) > 1$ and $G \cong H \circ_h K$. Otherwise, it is called *decomposable*.

Example 3.3. Let $G = (P, W)$ be a simple game and $A \subseteq P$ be the set of all vetoers in this game. Let $|A| = m$. Then $G \cong U_{m+1} \circ_u G^A$, where u is any player of U_{m+1} . So any game with some (but not all) vetoers is decomposable.

Example 3.4. Let $G = (P, W)$ be a simple game and $A \subseteq P$ be the set of all passers in this game. Let $|A| = m$. Then $G \cong A_{m+1} \circ_a G_A$, where a is any player of A_{m+1} . So any game with passers is decomposable.

Proposition 3.5. Let G, H be two games defined on disjoint sets of players and $g \in P_G$. Then

$$W_{G \circ_g H}^{\min} = \{X \mid X \in W_G^{\min} \text{ and } g \notin X\} \cup \{X \cup Y \mid X \cup \{g\} \in W_G^{\min} \text{ and } Y \in W_H^{\min} \text{ with } g \notin X\}.$$

Proof. Follows directly from the definition. □

Proposition 3.6. Let G, H, K be three games defined on disjoint sets 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 compositions are isomorphic.

Proof. Let us classify the minimal winning coalitions of the game $(G \circ_g H) \circ_h K$. By Proposition 3.5 they can be of the following types:

- $X \in W_G^{\min}$ with $g \notin X$;
- $X \cup Y$, where $X \cup \{g\} \in W_G^{\min}$ and $Y \in W_H^{\min}$ with $g \notin X$ and $h \notin Y$;
- $X \cup Y \cup Z$, where $X \cup \{g\} \in W_G^{\min}$, $Y \cup \{h\} \in W_H^{\min}$ and $Z \in W_K^{\min}$ with $g \notin X$ and $h \notin Y$.

It is easy to see that the game $G \circ_g (H \circ_h K)$ has exactly the same minimal winning coalitions. \square

Proposition 3.7. Let G, H be two games defined on disjoint sets of players. Then $G \circ_g H$ has no dummies if and only if both G and H have no dummies.

Proof. Straightforward. \square

4 Decompositions of weighted games and ideal games

The following result was proved in [2].

Proposition 4.1. Let $C = G \circ_g H$ be a decomposition of a game C into two games G and H over an element $g \in P_G$, which is not dummy. Then, C is ideal if and only if G and H are also ideal.

Suppose we have a class of games \mathcal{C} such that if the composition $G \circ_g H$ belongs to \mathcal{C} , then both G and H belong to \mathcal{C} . This proposition means that in any class of games \mathcal{C} with the above property we may represent any ideal game as a composition of indecomposable ideal games also belonging to \mathcal{C} . The following lemma shows that the class of weighted games satisfies the above property. Hence, if we would like to describe ideal games in the class of weighted games, we should look at indecomposable weighted games first.

Lemma 4.2. Let $C = G \circ_g H$ be a decomposition of a game C into two games G and H over an element $g \in P_G$, which is not dummy. Then, if C is weighted, then G and H are weighted.

Proof. Suppose C is weighted, $G = \{g_1, \dots, g_k, g\}$ and $H = \{h_1, \dots, h_m\}$. Suppose u_1, \dots, u_k are the weights of g_1, \dots, g_k in C , v_1, \dots, v_m are the weights of h_1, \dots, h_m in C and q is the threshold in C . Let also X be any minimal winning coalition of G containing g (since g is not a dummy, it exists). Then we give g the weight $q - u(X \setminus \{g\})$, where $u(X \setminus \{g\})$ is the total weight of coalition X without g and set $q' = q - u(X \setminus \{g\})$ also as a threshold for H leaving the weights of elements of H as they were in C . It is easy to see that G and H become weighted. \square

Corollary 4.3. Every weighted game is a composition of indecomposable weighted games.¹

The converse is however not true. As we will see in the next section, the composition $C = G_1 \circ_g G_2$ of two weighted games G_1 and G_2 is seldom weighted. Thus we will pay attention to those cases where compositions are weighted. One of those which we will now consider is when G_1 is a k -out-of- n game. In this case all players of G_1 are equivalent and we will often omit g and write the composition as $C = G_1 \circ G_2$.

Theorem 4.4. Let $G_1 = H_{n,k}$ be a k -out-of- n game and G_2 a weighted simple game. Then $C = G_1 \circ G_2$ is also a weighted game.

¹ As usual we assume that if a game G is indecomposable, its decomposition into a composition of indecomposable games is $G = G$, i.e., trivial.

Proof. Let $G_2 = [q; w_1, \dots, w_\ell]$ and $w = w_1 + \dots + w_\ell$. Then the weighted representation for C will be

$$C = [(k-1)w + q; \underbrace{w, \dots, w}_{n-1}, w_1, \dots, w_\ell].$$

This means that every player of C from G_1 gets the weight w equal to the sum of all weights of players in G_2 . We note that $q \leq w$. To achieve the threshold $(k-1)w + q$, a coalition of C must have either k players of weight w or $k-1$ of them plus a group of players from G_2 of total weight at least q . This proves the theorem. \square

5 Compositions of complete games

We will start with the following observation. It says that if $g \in P_G$ is not the least desirable player of G , then the composition $G \circ_g H$ is almost never swap robust, hence is almost never complete.

Lemma 5.1. *Let G, H be two games on disjoint sets of players. Let H be neither an oligarchy nor an anti-oligarchy. 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.*

Proof. As g is more desirable than g' , there exists a coalition $X \subseteq P_G$, containing neither g nor g' such that $X \cup \{g\} \in W_G$ and $X \cup \{g'\} \notin W_G$. We may take X to be minimal with this property, then $X \cup \{g\}$ is a minimal winning coalition of G . Since g' is not dummy, there exists a minimal winning coalition Y containing g' . The coalition Y may contain g or may not. Firstly, assume that it does contain g . Since H is not an oligarchy, there exist two distinct minimal winning coalitions of H , say Z_1 and Z_2 . Then we can find $z \in Z_1 \setminus Z_2$. Then the coalitions $U_1 = X \cup Z_1$ and $U_2 = (Y \setminus \{g\}) \cup Z_2$ are winning in $G \circ_g H$ and coalitions $V_1 = (X \cup \{g'\}) \cup (Z_1 \setminus \{z\})$ and $V_2 = Y \setminus \{g, g'\} \cup (Z_2 \cup \{z\})$ are losing in this game since $Z_1 \setminus \{z\}$ is losing in H and $Y \setminus \{g'\} = Y \setminus \{g, g'\} \cup \{g\}$ is losing in G . Since V_1 and V_2 are obtained when U_1 and U_2 swap players z and g' , the sequence of sets $(U_1, U_2; V_1, V_2)$ is a certificate of incompleteness for $G \circ_g H$.

Suppose now Y does not contain g . Let Z be any minimal winning coalition of H that has more than one player (it exists since H is not an anti-oligarchy). Let $z \in Z$. Then

$$(X \cup Z, Y; X \cup \{g'\} \cup (Z \setminus \{z\}), Y \setminus \{g'\} \cup \{z\})$$

is a certificate of incompleteness for $G \circ_g H$. \square

This lemma shows that if a composition $G \circ_g H$ of two weighted games is weighted, then almost always g is one of the least desirable players of G .

Lemma 5.2. *Let $G = (P_G, W_G)$ and $H = (P_H, W_H)$ be two simple games and $C = G \circ_g H$.*

- (i) *For $x, y \in P_G \setminus \{g\}$ it holds that $x \succeq_G y$ if and only if $x \succeq_C y$. Moreover, $x \succ_G y$ if and only if $x \succ_C y$.*
- (ii) *For $x, y \in P_H$ it holds that $x \succeq_H y$ if and only if $x \succeq_C y$. Moreover, $x \succ_H y$ if and only if $x \succ_C y$.*

Proof. (i) Suppose $x \succeq_G y$ but not $x \succeq_C y$. Then there exists $Z \subseteq C$ such that $Z \cup \{y\} \in W_C$ but $Z \cup \{x\} \notin W_C$. We can take Z minimal with this property. Consider $Z' = Z \cap P_G$. Then either $Z' \cup \{y\}$ is winning in G , or else $Z' \cup \{y\}$ is losing in G but $Z' \cup \{y\} \cup \{g\}$ is winning in G . In the latter case $Z \cap P_H \in W_H$. In the first case, since $x \succeq_G y$, we have also $Z' \cup \{x\} \in W_G$, which contradicts $Z \cup \{x\} \notin W_C$. Similarly, in the second case we have $Z' \cup \{x\} \cup \{g\} \in W_G$ and since $Z \cap P_H \in W_H$, this contradicts $Z \cup \{x\} \notin W_C$ also. Hence $x \succeq_C y$.

Suppose now $x \succeq_C y$ and consider a subset $S \subseteq P_G$ such that $S \cup \{y\} \in W_G$. We need to show that $S \cup \{x\} \in W_G$ as well. If $g \notin S$, the result is clear. If $g \in S$, we take a minimal winning coalition T of H and consider the coalition $R = S \setminus \{g\} \cup T$ in C . Then $R \cup \{y\}$ is winning in C , hence $R \cup \{x\}$ is also winning in C due to the fact that $x \succeq_C y$. From this we deduce that $S \cup \{x\} \in W_G$, whence $x \succeq_G y$.

(ii) This case is similar to the previous one. Suppose $x \succeq_H y$ but not $x \succeq_C y$. Then there exists $Z \subseteq C$ such that $Z \cup \{y\} \in W_C$ but $Z \cup \{x\} \notin W_C$. We can take Z minimal with this property. Obviously, $Z \cap P_G$ is not winning in G but wins together with g . Since $Z \cup \{y\}$ is winning in G , for $K = Z \cap P_H$ we have $K \cup \{y\} \in W_H$. But since $x \succeq_H y$, we have also $K \cup \{x\} \in W_H$. This contradicts the fact that $Z \cup \{x\} \notin W_C$.

The proof of the strict versions of (i) and (ii) is similar. \square

Theorem 5.3 shows that if G has no dummies and we compose two weighted games over the weakest player of the first game, the result will be always complete, however, it will not always be weighted (plenty of examples will be given in Section 7.1).

Theorem 5.3. Let $G = (P_G, W_G)$ and $H = (P_H, W_H)$ be two simple games, g be one of the least desirable players in G but not a dummy, and $C = G \circ_g H$. Let $x \in P_G \setminus \{g\}$ and $y \in P_H$.

- (i) $x \succeq_C y$; in particular, C is complete if and only if G and H are complete.
- (ii) $x \sim_C y$ if and only if $x \sim_G g$ and y is a passer in H .

Proof. (i) We have $x \succeq_G g$ since g is from the least desirable class in G . Let us consider a coalition $Z \subset C$ such that $Z \cap \{x, y\} = \emptyset$, and suppose $Z \cup \{y\} \in W_C$ but $Z \cup \{x\} \notin W_C$. Then Z must be losing in C , and hence $Z \cap P_G$ cannot be winning in G , but $(Z \cap P_G) \cup \{g\}$ must be winning in G . However, since $x \succeq_G g$, the coalition $(Z \cap P_G) \cup \{x\}$ is also winning in G . But then $Z \cup \{x\}$ is winning in G and hence in C , a contradiction. This shows that if $Z \cup \{y\}$ is winning in C , then $Z \cup \{x\}$ is also winning in C , meaning $x \succeq_C y$. Thus in view of Lemma 5.2, C is a complete game if and only if both G and H are.

(ii) If it is not true that $x \sim_G g$, then $x \succ_G g$. Then there exists a coalition $Z \subseteq G$ such that $Z \cup \{x\} \in W_G$ but $Z \cup \{g\} \notin W_G$. Then $Z \cup \{x\} \in W_C$ but $Z \cup \{y\} \notin W_C$ and the equivalence $x \sim_C y$ does not hold.

Suppose now $x \sim_G y$. Let $Z \subseteq C$ be a subset of $(P_G \setminus \{g\}) \cup P_H$ which contains neither x nor y . Suppose $Z \cap P_G \cup \{x\}$ is winning in G . Then, as $x \sim_G y$, we have $Z \cap P_G \cup \{g\}$ is winning in G . Hence $Z \cap P_G \cup \{y\}$ is winning in C if and only if y is a passer in H in which case $x \sim_C y$. \square

Corollary 5.4. A game $H_{n,k}$ for $n > k > 1$ is indecomposable.

Proof. Suppose $H_{n,k}$ is decomposable into $H_{n,k} = K \circ_g L$, where $K = (P_K, W_K)$, $L = (P_L, W_L)$ with $n_1 = |P_K| \geq 2$ and $n_2 = |P_L| \geq 2$. By Theorem 5.3 all elements of game L are passers, so $L \cong U_{n_2}$ and K is a unipartite game so $K = H_{n_1,k}$. This is however impossible since any two elements of L together with any $k - 2$ elements of $K \setminus \{g\}$ will lose in the composition. \square

6 Indecomposable ideal weighted simple games

The following theorem was proved in [9, p. 234] by Farràs and Padró and will be of a major importance in this section. We reformulate this theorem in our terminology, leaving its content and notation unchanged.

Theorem 6.1. Any indecomposable ideal weighted simple game belongs to one of the seven following types:

\tilde{H} Simple majority or k -out-of- n games.

\tilde{B}_1 Hierarchical conjunctive games $H_{\forall}(\mathbf{n}, \mathbf{k})$ with $\mathbf{n} = (n_1, n_2)$ and $\mathbf{k} = (k_1, k_2)$, where $k_1 < n_1$ and $k_2 - k_1 = n_2 - 1 > 0$. Such games have only one shift-minimal winning coalition $\{1^{k_1}, 2^{k_2-k_1}\}$.

B_2 Hierarchical disjunctive games $H_{\exists}(\mathbf{n}, \mathbf{k})$ with $\mathbf{n} = (n_1, n_2)$ and $\mathbf{k} = (k_1, k_2)$, where $1 < k_1 \leq n_1$, $k_2 \leq n_2$ and $k_2 = k_1 + 1$. The shift-minimal winning coalitions have the forms $\{1^{k_1}\}$ and $\{2^{k_2}\}$.

B_3 Hierarchical disjunctive games $H_{\exists}(\mathbf{n}, \mathbf{k})$ with $\mathbf{n} = (n_1, n_2)$ and $\mathbf{k} = (k_1, k_2)$, where $k_1 \leq n_1$, $k_2 > n_2 > 2$ and $k_2 = k_1 + 1$. The shift-minimal winning coalitions have the forms $\{1^{k_1}\}$ and $\{1^{k_2-n_2}, 2^{n_2}\}$.

T_1 Tripartite games $\Delta_1(\mathbf{n}, \mathbf{k})$ with $\mathbf{n} = (n_1, n_2, n_3)$ and $\mathbf{k} = (k_1, k_2, k_3)$ where $k_1 > 1$, $k_2 < n_2$, $k_3 = k_1 + 1$ and $n_3 = k_3 - k_2 + 1 > 2$. They have two types of shift-minimal winning coalitions: $\{1^{k_1}\}$ and $\{2^{k_2}, 3^{k_3-k_2}\}$. It follows from (2.5) that $k_1 \leq n_1$ and $k_3 - k_2 \leq n_3$.

T_2 Tripartite games $\Delta_1(\mathbf{n}, \mathbf{k})$ with $\mathbf{n} = (n_1, n_2, n_3)$ and $\mathbf{k} = (k_1, k_2, k_3)$ where $n_3 = k_3 - k_2 + 1 > 2$ and $k_3 = k_1 + 1$. They have two types of shift-minimal winning coalitions: $\{1^{k_1}\}$ and $\{1^{k_2-n_2}, 2^{n_2}, 3^{k_3-k_2}\}$. It follows from (2.5) that $k_1 \leq n_1$, $k_2 - n_2 \leq k_1$ and $k_3 - k_2 \leq n_3$.

T_3 Tripartite games $\Delta_2(\mathbf{n}, \mathbf{k})$ with $\mathbf{n} = (n_1, n_2, n_3)$ and $\mathbf{k} = (k_1, k_2, k_3)$ where $k_3 - k_1 = n_2 + n_3 - 1$, $k_3 = k_2 + 1$, $k_2 - n_2 > k_1$ and $n_3 > 1$. They have two types of shift-minimal winning coalitions: $\{1^{k_2-n_2}, 2^{n_2}\}$ and $\{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3}\}$ (the case when $k_3 - k_1 = n_3$ and $n_2 = 1$ is not excluded). It follows from (2.6) that $k_1 \leq n_1$, $k_2 - n_2 \leq n_1$ and $k_3 - k_1 - n_3 < n_2$.

Moreover, any game in these seven classes is weighted.

As we already noted we follow [9] in describing these classes (tildes over \mathbf{H} and \mathbf{B}_1 will be explained shortly). In [10] Farràs and Padró wrote these families more compactly. However, we found it more convenient to use their earlier description.

The list above contains some decomposable games as we will now show.

Proposition 6.2. *The game of type \mathbf{B}_1 for $k_2 - k_1 = n_2 - 1 = 1$ is decomposable.*

Proof. The decomposition is as follows: Assume $k_2 - k_1 = n_2 - 1 = 1$, so $n_2 = 2$ and $k_2 = k_1 + 1$, then we have $\mathbf{k} = (k_1, k_1 + 1)$, $\mathbf{n} = (n_1, 2)$, and the only shift-minimal winning coalition here is $\{1^{k_1}, 2\}$. Let the first game $G = (P_G, W_G)$ be unipartite with $P_G = \{1^{n_1+1}\}$, $W_G = \{1^{k_1+1}\}$, and let the second game be $H = (P_H, W_H)$ with $P_H = \{2^2\}$, $W_H = \{2\}$. Then the composition $G \circ_1 H$ over a player $1 \in P_G$ gives two minimal winning coalitions $\{1^{k_1+1}\}$ and $\{1^{k_1}, 2\}$, of which only $\{1^{k_1}, 2\}$ is shift-minimal. Hence the composition is of type \mathbf{B}_1 . This proves that a game of type \mathbf{B}_1 is decomposable in this case. \square

Proposition 6.3. *The unanimity games U_n and anti-unanimity games A_n for $n > 2$ are decomposable. U_2 and A_2 are indecomposable.*

Proof. We note that

$$U_n \circ U_m \cong U_{n+m-1}$$

for any $u \in U_n$. In particular, the only indecomposable unanimity game is U_2 . Similarly,

$$A_n \circ A_m \cong A_{n+m-1}$$

for any $a \in A_n$ with the only indecomposable anti-unanimity game A_2 . \square

Proposition 6.4. *All games of type \mathbf{T}_2 are decomposable.*

Proof. Let $\Delta = \Delta_1(\mathbf{n}, \mathbf{k})$ be of type \mathbf{T}_2 . Then we have the following decomposition for it. The first game will be $G = (P_G, W_G)$, which is bipartite with the multiset representation on $\{1^{n_1}, 2^{n_2+1}\}$ and shift-minimal winning coalitions of types $\{1^{k_1}\}$ and $\{1^{k_2-n_2}, 2^{n_2+1}\}$. The second game will be $(k_3 - k_2)$ -out-of- n_3 game $H = (P_H, W_H)$, with the multiset representation on $\bar{P}_H = \{3^{n_3}\}$ and shift-minimal winning coalitions of type $\{3^{k_3-k_2}\}$. The composition is over a player $p \in P_G$ from level 2. Then we can see that $G \circ_p H$ has shift-minimal winning coalitions of types $\{1^{k_1}\}$ and $\{1^{k_2-n_2}, 2^{n_2}, 3^{k_3-k_2}\}$, hence is exactly Δ . \square

We now refine classes $\tilde{\mathbf{H}}$ and $\tilde{\mathbf{B}}_1$ as follows:

H Games of this type are A_2, U_2 and $H_{n,k}$, where $1 < k < n$.

B₁ Hierarchical conjunctive games $H_v(\mathbf{n}, \mathbf{k})$ with $\mathbf{n} = (n_1, n_2)$, $\mathbf{k} = (k_1, k_2)$, where $k_1 < n_1$ and $k_2 - k_1 = n_2 - 1 > 1$.

The following is now an if-and-only-if statement.

Theorem 6.5. *A game is ideal weighted and indecomposable if and only if it belongs to one of the following types: $\mathbf{H}, \mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, \mathbf{T}_1, \mathbf{T}_3$.*

Proof. Due to Theorem 6.1 and Propositions 6.2–6.4 all that remains to show is that the remaining cases are indecomposable. We have already noted in Corollary 5.4 that the games of type \mathbf{H} are indecomposable. The same idea can be applied to all other cases.

For example, let us prove indecomposability of \mathbf{B}_1 . Let G be of this type. By Theorem 5.3 if G is decomposable, then there are two possibilities: (a) $G = H \circ_g K$ for some unipartite games H and K having $n_1 + 1$ and n_2 elements, respectively, or (b) $G = H \circ_g A_s$, where H is bipartite and A_s is an anti-unanimity game with at least two players. In the latter case all elements of A_s will be equivalent to the elements of the lower level of H . In case (a) we know that $k_1 < n_1$ and $k_2 - k_1 < n_2$. If we choose a subset H_1 of k_1 elements from H and a subset K_1 of $k_2 - k_1$ elements from K , we must obtain a winning coalition while H_1 is not winning by itself. This means that $H_1 \cup \{g\}$ is winning in H . As g is the weakest in H , this means that H is a $k_1 + 1$ -out-of- n_1 game. So any $k_1 + 1$ elements from H form a winning coalition in G . However this cannot be the case since $k_2 > k_1 + 1$.

In case (b) let us consider the set Z of $s \geq 2$ elements from A_s and the set H_1 of $k_2 - s$ elements from H which include the set H_2 of k_1 elements from the senior level. Then $H_1 \cup \{g\}$ must be winning in H and hence any coalition of $|H_1| + 1$ players must be winning in H (since g is the weakest). But $|H_1| \leq k_2 - 2$ which gives us a contradiction.

We leave proving indecomposability of the remaining cases to the reader. \square

Let us compare this theorem with Theorem 6.1. We narrowed the class **H**, we excluded the case $n_2 = 2$ in **B**₁ and removed class **T**₂.

7 Compositions of ideal weighted indecomposable games

Suppose from now on that we have a composition $G = G_1 \circ_g G_2$, where both G_1 and G_2 are ideal and weighted, and G_1 is indecomposable. The plan now is to fix G_1 and analyse what happens when we compose it with an arbitrary ideal weighted game G_2 . Since G_1 is ideal weighted and indecomposable, then it belongs to one of the six types of games listed in Theorem 6.5. So we carry out the analysis case by case for all possibilities of G_1 .

The key result that will lead us to the main theorem of this paper is the following.

Theorem 7.1. *Let G be a game with no dummies which has a nontrivial decomposition $G = G_1 \circ_g G_2$, such that G_1 and G_2 are both ideal and weighted, and G_1 is indecomposable. Then G is ideal weighted if and only if either*

- (i) G_1 is of type **H**, or
- (ii) G_1 is of type **B**₂ and G_2 is A_n , $n \geq 2$, and the composition is over a player g from level 2 of G_1 .

We will prove this theorem in several steps. Firstly, we will consider all cases where g is from the least desirable level of G_1 . Secondly, in Appendix A, we will deal with the hypothetical cases when g is not from the least desirable level. This is because, unfortunately, Lemma 5.1 still leaves a possibility that for some special cases of G_2 this decomposition may be over g which is not the least desirable in G_1 .

The case (i) was treated in Theorem 4.4. The following proposition deals with case (ii).

Proposition 7.2. *Let $G_1 = (P_1, W_1)$ be a weighted simple game of type **B**₂, g a player from level 2 of P_1 , and let G_2 be A_n , $n > 1$. Then $G = G_1 \circ_g G_2$ is a weighted simple game.*

*Proof.*² Let G_1 be of type **B**₂ and let its two thresholds be k_1 and $k_2 = k_1 + 1$. It has two levels. The composition game G has the third level composed from members of game G_2 . It is easy to see that if we set the threshold $q = k_1$ and introduce the weights $1, 1 - \frac{1}{2nk_1}, \frac{1}{2n}$ for players from levels 1, 2, 3, respectively, then G will be a weighted game with these weights and the threshold q . \square

In the next section we analyse the remaining cases of compositions $G = G_1 \circ_g G_2$ in terms of G_1 , where the composition is over a player g from the least desirable level of G_1 . We will show that none of them is weighted. The remaining cases are in Appendix A.

7.1 All other compositions are non-weighted

Here we will consider two cases:

- (i) G_2 has at least one minimal winning coalition with cardinality at least 2.
- (ii) $G_2 = A_n$, where $n \geq 2$.

We will start with the following general statement which will help us to resolve the first case.

² We are grateful to an anonymous referee for this simple proof.

Definition 7.3. Let $G = (P, W)$ be a simple game and $g \in P$. We say that a coalition X is g -winning if $g \notin X$ and $X \cup \{g\} \in W$.

Every winning coalition is of course g -winning but not the other way around.

Lemma 7.4. Let G be a game for which there exist coalitions X_1, X_2, Y_1, Y_2 such that both X_1 and X_2 do not contain g ,

$$(X_1, X_2; Y_1, Y_2) \quad (7.1)$$

is a trading transform, X_1 is winning, X_2 is g -winning, and Y_1 and Y_2 are losing in G . Let also H be a game with a minimal winning coalition U which has at least two elements. Then $C = G \circ_g H$ is not weighted.

Proof. If X_2 is winning in G , then there is nothing to prove since (7.1) is a certificate of non-weightedness for C . So assume X_2 is not winning in G . Let $U = U_1 \cup U_2$, where U_1 and U_2 are losing in H . Then it is easy to check that

$$(X_1, X_2 \cup U; Y_1 \cup U_1, Y_2 \cup U_2)$$

is a certificate of non-weightedness for C . Indeed, X_1 and $X_2 \cup U$ are both winning in C and $Y_1 \cup U_1$ and $Y_2 \cup U_2$ are both losing. \square

The only exception in this case is when H consists of passers and dummies. We will have to consider this case separately.

Lemma 7.5. If G is of type B_1, B_2 or B_3 , g is any element from level 2, and H has a minimal winning coalition X which has at least two elements, then $G \circ_g H$ is not weighted.

Proof. Suppose G is of type B_1 . Then let us consider the following trading transform:

$$(\{1^{k_1}, 2^{k_2-k_1}\}, \{1^{k_1}, 2^{k_2-k_1-1}\}; \{1^{k_1-1}, 2^{k_2-k_1+1}\}, \{1^{k_1+1}, 2^{k_2-k_1-2}\})$$

(note that $k_2 - k_1 + 1 = n_2$ and $k_1 + 1 \leq n_1$ so there is enough capacity in both equivalence classes to make all coalitions involved legitimate). It is easy to check that the first coalition in this sequence is winning, the second is g -winning and the remaining two are losing. By Lemma 7.4 the result holds.

Suppose now G is of type B_2 , then $k_2 = k_1 + 1 \leq n_2$. Let $k_1 = k$. Then we can apply Lemma 7.4 to the trading transform

$$(\{1^k\}, \{2^k\}; \{1^{\lfloor \frac{k}{2} \rfloor}, 2^{\lceil \frac{k}{2} \rceil}\}, \{1^{\lceil \frac{k}{2} \rceil}, 2^{\lfloor \frac{k}{2} \rfloor}\}),$$

where $\{1^k\}$ is winning, $\{2^k\}$ is g -winning and the remaining two coalitions are losing.

If G is of type B_3 , then $n_2 < k_2 = k_1 + 1$. We again let $k = k_1$. In this case we can apply Lemma 7.4 to the trading transform

$$(\{1^k\}, \{1^{k-2}, 2^2\}; \{1^{k-1}, 2\}, \{1^{k-1}, 2\}),$$

where the first coalition is winning, the second is g -winning (we use $n_2 \geq 3$ here) and the two remaining coalitions are losing. \square

Lemma 7.6. If G is of type T_1 or T_3 , g is any element from level 3, and H has a minimal winning coalition X which has at least two elements, then $C = G \circ_g H$ is not weighted.

Proof. If G is of type T_1 . Then let us consider the following trading transform:

$$(\{1^{k_1}\}, \{2^{k_2}, 3^{k_3-k_2-1}\}; \{1^{k_1-1}, 2\}, \{1, 2^{k_2-1}, 3^{k_3-k_2-1}\}).$$

Lemma 7.4 is applicable to it, so C is not weighted.

Suppose G is of type T_3 . Then let us consider the following trading transform:

$$(\{1^{k_2-n_2}, 2^{n_2}\}, \{1^{k_1}, 2^{n_2-1}, 3^{n_3-1}\}; \{1^{k_2-n_2}, 2^{n_2-1}, 3\}, \{1^{k_1}, 2^{n_2}, 3^{n_3-2}\}).$$

Since $n_3 > 1$, all coalitions exist. Lemma 7.4 is now applicable and shows that C is not weighted. This proves the lemma. \square

We will now deal with the second case. Denote players of A_n by P_{A_n} .

Proposition 7.7. *Let G_1 be an ideal weighted indecomposable simple game of types B_1 , B_3 , T_1 , and T_3 , and g be a player from the least desirable level of G_1 , then $G = G_1 \circ_g A_n$ is not weighted.*

Proof. Let G_1 be of type B_1 . The only shift-minimal winning coalition of G_1 is of the form $\{1^{k_1}, 2^{k_2-k_1}\}$, where $n_1 > k_1 > 0$ and $k_2 - k_1 = n_2 - 1 > 1$. Composing over a player from level 2 of G_1 gives shift-minimal winning coalitions of types $\{1^{k_1}, 2^{k_2-k_1}\}$ and $\{1^{k_1}, 2^{k_2-k_1-1}, 3\}$. Thus the game is not weighted due to the following certificate of non-weightedness:

$$(\{1^{k_1}, 2^{k_2-k_1}\}, \{1^{k_1}, 2^{k_2-k_1-1}, 3\}; \{1^{k_1-1}, 2^{k_2-k_1+1}, 3\}, \{1^{k_1+1}, 2^{k_2-k_1-2}\}).$$

Since in a game of type B_1 we have $k_2 - k_1 + 1 = n_2$ and $k_1 + 1 \leq n_1$, all coalitions in this trading transform exist.

Now consider B_3 . Its shift-minimal winning coalitions have types $\{1^{k_1}\}$ and $\{1^{k_2-n_2}, 2^{n_2}\}$. Composing over a player from level 2 of G_1 gives winning coalitions of types $\{1^{k_1}\}$ and $\{1^{k_2-n_2}, 2^{n_2-1}, 3\}$ in G . The game is not weighted due to the following certificate of non-weightedness:

$$(\{1^{k_2-n_2}, 2^{n_2-1}, 3\}, \{1^{k_2-n_2}, 2^{n_2-1}, 3\}; \{1^{k_2-n_2+1}, 2^{n_2-2}\}, \{1^{k_2-n_2-1}, 2^{n_2}, 3^2\}).$$

Note that $k_2 - n_1 + 1 < k_1 \leq n_1$ and $n_2 > 2$ in B_3 , so all coalitions in this transform exist.

Now consider T_1 . Since its levels 2 and 3 form a subgame of type B_1 , composing it with A_n over a player from level 3, as was proved, will result in a non-weighted game.

Let us consider T_3 , where the shift-minimal winning coalition are $\{1^{k_2-n_2}, 2^{n_2}\}$, $\{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3}\}$. If we compose over a player from level 3 of G_1 , then the resulting game will have shift-minimal coalitions of the following type $\{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3-1}, 4\}$, where now elements of $G_2 = A_n$ will form level 4. Then we can show that the composition $G_1 \circ G_2$ is not weighted due to the following certificate of non-weightedness:

$$(\{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3-1}, 4\}, \{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3-1}, 4\}; \{1^{k_1+1}, 2^{k_3-k_1-n_3}, 3^{n_3-2}\}, \{1^{k_1-1}, 2^{k_3-k_1-n_3}, 3^{n_3}, 4^2\}).$$

The coalition $\{1^{k_1+1}, 2^{k_3-k_1-n_3}, 3^{n_3-2}\}$ is losing because in T_3 we have $k_3 - k_1 - n_3 = n_2 - 1$ and also $k_2 - n_2 > k_1$, meaning $(k_1 + 1) + (k_3 - k_1 - n_3) = k_1 + 1 + n_2 - 1 \leq k_2 - n_2 + n_2 - 1 = k_2 - 1$. Also in total it contains less than k_3 elements. The coalition $\{1^{k_1-1}, 2^{k_3-k_1-n_3}, 3^{n_3}, 4^2\}$ is easily seen to be losing as well. \square

Now all that remains for the proof of Theorem 7.1 is to consider the cases when g is not from the least desirable level of G_1 which may happen only when it is of types T_1 and T_3 . These cases are similar to those that have been already considered and we delegate them to Appendix A.

8 The main theorem

At the outset we will deal with two results that will guarantee the uniqueness of the decomposition. Firstly, we note that the first component of the composition is a k -out-of- n game, there is always uniqueness of decomposition.

Theorem 8.1. *Let H_{n_1, k_1} and H_{n_2, k_2} be two k_i -out-of- n_i games ($i = 1, 2$) which are not unanimity games.*

- (i) *If $G = H_{n_1, k_1} \circ G_1 = H_{n_2, k_2} \circ G_2$ with G_1 and G_2 having no passers, then $n_1 = n_2$, $k_1 = k_2$ and $G_1 = G_2$.*
- (ii) *If $G = U_{n_1} \circ G_1 = U_{n_2} \circ G_2$ and G_1 and G_2 do not have vetoers, then $n_1 = n_2$ and $G_1 = G_2$.*

Proof. Suppose that we know that $G = H \circ G_1$, where H is a k -out-of- n game but not a unanimity game. Then all winning coalitions in G of smallest cardinality have k players, so k in this case can be recovered unambiguously.

If G_1 does not have passers, then n can be also recovered since the set of all players that participate in winning coalitions of size k will have cardinality $n - 1$. So there cannot exist two decompositions $G = H_{n_1, k_1} \circ G_1$ and $G = H_{n_2, k_2} \circ G_2$ of G , where $k_1 \neq k_2$ with $k_1 \neq n_1$ and $k_2 \neq n_2$.

Let us consider now the game $G = U \circ G_1$, where U is a unanimity game. Due to Example 3.3 if G_1 does not have vetoers, then U consists of all vetoers of G and is uniquely recoverable. \square

Proposition 8.2. *Let H be a game of type H , B be a game of type B_2 with b being a player from level 2 of B , G be an ideal weighted simple game, and A_n be an anti-unanimity game. Then $H \circ G \neq B \circ_b A_n$.*

Proof. We note that by Theorem 5.3 both compositions are complete. Recall that isomorphisms preserve Isbel's desirability relation [6]. An isomorphism preserves completeness and maps shift-minimal winning coalitions of a complete game onto shift-minimal winning coalitions of another game.

Let $H = H_{k,n}$. Consider first the composition $H \circ G$. Any minimal winning coalition in this composition will have either k or $k - 1$ players from the most desirable level.

Now consider $B \circ_b A_n$. Let the two types of shift-minimal winning coalitions of B be of the forms $\{1^\ell\}$ and $\{2^{\ell+1}\}$. Then there will be a minimal winning coalition in $B \circ_b A_n$ which has ℓ players from the second most desirable level and an element from level 3 with no players from level 1.

The two games therefore cannot be isomorphic. \square

All previous results combined give us the main theorem:

Theorem 8.3. *G is an ideal weighted simple game without dummies if and only if it is a composition*

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

where H_i is an indecomposable game of type H for each $i = 1, \dots, s$. Also, I , which is allowed to be absent, is an indecomposable game of types B_1, B_2, B_3, T_1 and 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 B_2 ; in the latter case the composition $I \circ A_n$ is over a player g of the least desirable level of I . Also, the above decomposition is unique.

Proof. This proof is now easy since the main work has been done in Theorem 7.1. Either G is decomposable or not. If it is not, then by Theorem 6.5 it is either of type H or one of the indecomposable games of types B_1, B_2, B_3, T_1 , and T_3 . So the theorem is trivially true. Suppose now that G is decomposable, so $G = G_1 \circ G_2$. Then by Theorem 7.1 there are only two possibilities:

- (i) G_1 is of type H ;
- (ii) G_1 is of type B_2 , and also $G_2 = A_n$ such that the composition is over a player from level 2 of G_1 .

By Proposition 8.2 these two cases are mutually exclusive. Suppose we have the case (i). By Theorem 8.1 G_1 is uniquely defined and we can apply the induction hypothesis to G_2 . It is also easy to see that in the second case, G_1 and G_2 are uniquely defined. \square

We finally note that the absence of dummies in access structures is normally implicitly assumed in secret sharing. It is easy to add them and give meaningless shares anyway.

A Appendix

A.1 A canonical representation of Δ_1 and Δ_2

Proposition A.1. *The game $\Delta_1(n, k)$ is a tripartite game without dummies if and only if conditions (2.5) are satisfied.*

Proof. It is easy to see from the definition that this game is complete and $1 \succeq_G 2 \succeq_G 3$. Suppose we actually have $1 \succ_G 2 \succ_G 3$ so that the game is tripartite. If the condition $k_1 \leq n_1$ is not satisfied, the condition $\ell_1 \geq k_1$ has no solution and 1 becomes equivalent to 2. So we assume $k_1 \leq n_1$. If $k_2 \geq k_3$, then the condition $\ell_1 + \ell_2 \geq k_2$ is redundant which implies $2 \sim 3$ and the game is bipartite so we assume $k_2 < k_3$. If $k_1 \geq k_3$, then the coalition $\ell_1 + \ell_2 + \ell_3 \geq k_3$ is redundant and 3 is a dummy. Hence we assume $k_1 < k_3$. If we only had $n_2 \leq k_2 - k_1$, then $\ell_1 + \ell_2 \geq k_2$ can be satisfied only if $\ell_1 \geq k_1$ is satisfied. So in this case $\{1^{k_1}\}$ is the only minimal winning coalition, which implies $2 \sim 3$. So $n_2 > k_2 - k_1$. Finally, if $n_3 > k_3 - k_2$ is not satisfied, then $\ell_1 + \ell_2 + \ell_3 \geq k_3$ implies

$\ell_1 + \ell_2 \geq k_2$, in which case the minimal winning coalition must satisfy either $\ell_1 = k_1$ or $\ell_1 + \ell_2 + \ell_3 = k_3$. We get in this case $2 \sim 3$, which is impossible. Hence if $\Delta_1(\mathbf{n}, \mathbf{k})$ is tripartite and has no dummies, the conditions (2.5) are satisfied.

On the other hand, if (2.5) are satisfied, then the game has two shift-minimal winning coalitions $\{1^{k_1}\}$ and either $\{2^{k_2}, 3^{k_3-k_2}\}$ in case $k_2 \leq n_2$ or $\{1^{k_2-n_2}, 2^{n_2}, 3^{k_3-k_2}\}$ in case $k_2 > n_2$. In both cases $1 > 2 > 3$ by Proposition 2.10. \square

Proposition A.2. *The game $\Delta_2(\mathbf{n}, \mathbf{k})$ is a tripartite game without dummies if and only if conditions (2.6) are satisfied.*

Proof. Suppose $\Delta_2(\mathbf{n}, \mathbf{k})$ is tripartite. Like in Proposition A.1 we find that $k_1 < k_3$ and $k_2 < k_3$. However, we also know that $k_2 - k_1 \geq n_2 > 0$. Hence we assume $k_1 < k_2 < k_3$. If $n_1 + n_2 \geq k_2$ is not satisfied, then $\ell_1 + \ell_2 \geq k_2$ is ineffectual and $2 \sim 3$. So we assume $n_1 + n_2 \geq k_2$. In this case we have a shift-minimal winning coalition $C = \{1^{k_2-n_2}, 2^{n_2}\}$ which secures that $2 > 3$ (as $k_2 < k_3$). If $n_3 > k_3 - k_2$ is not satisfied, then $\ell_1 + \ell_2 + \ell_3 \geq k_3$ is redundant and 3 is a dummy. Since $k_3 > k_2$, we have $n_3 \geq k_3 - k_2 + 1 \geq 2$. Since $\Delta_2(\mathbf{n}, \mathbf{k})$ is defined for the case $n_2 \leq k_2 - k_1$, we have $k_1 \leq k_2 - n_2 \leq n_1$ and $n_1 \geq k_1$ follows.

Now, if the coalitions $\{1^{k_1}\}$ and $\{2^{k_3-k_1-n_3+1}\}$ exist, then a replacement of 1 with 2 in a winning coalition $\{1^{k_1-1}, 2^{k_3-k_1-n_3+1}, 3^{n_3}\}$ results in a losing coalition $\{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3}\}$. As the conditions (2.6) imply $k_1 \leq n_1$, the first coalition exists. The second coalition exists since $k_3 - k_1 - n_3 < n_2$ is equivalent to $k_3 - k_1 < n_2 + n_3$. This implies $1 > 2$.

Now, since $n_1 + n_2 \geq k_2$ and $k_2 < k_3$, there exists a minimal winning coalition $\{1^{\ell_1}, 2^{\ell_2}\}$ with $\ell_1 + \ell_2 = k_2$ and $\ell_2 \geq 1$. A replacement of 2 here with a 3 leads to a losing coalition, hence $2 > 3$. \square

A.2 End of proof of Theorem 7.1

Here we have to deal with the hypothetical possibility that G does not fall into categories (i) and (ii). Then we know that G_1 has at least two desirability levels and g is not from the least desirability level. Also Lemma 5.1 implies that in this case $G_2 = A_n$ or $G_2 = U_n$ for some $n \geq 2$. Let us deal with $G_2 = A_n$ first.

Lemma A.3. *Let $G = (P, W)$ be a game where player g is strictly more desirable than player g' . Suppose also that we can find two coalitions X_1 and X_2 in G such that*

$$\begin{aligned} g' \notin X_1, \quad X_1 \cup \{g\} \in W, \quad X_1 \cup \{g'\} \notin W; \\ g' \in X_2, \quad X_2 \cup \{g\} \in W, \quad X_2 \setminus \{g'\} \cup \{g\} \notin W. \end{aligned}$$

Then the composition $C = G \circ_g A_n$, $n \geq 2$, is not complete.

Proof. Let $a, b \in A_n$. We have the following certificate of incompleteness:

$$(X_1 \cup \{a\}, X_2 \cup \{b\}; X_1 \cup \{g'\}, X_2 \setminus \{g'\} \cup \{a, b\}).$$

Indeed, both X_1 and X_2 win with g in G and both $\{a\}$ and $\{b\}$ are winning coalitions in H , so $X_1 \cup \{a\}$ and $X_2 \cup \{b\}$ are winning in C . On the other hand $X_1 \cup \{g'\}$ and $X_2 \cup \{g'\}$ are losing in G and the latter even losing with g , so $X_1 \cup \{g'\}$ and $X_2 \setminus \{g'\} \cup \{a, b\}$ are both losing in C . This proves the lemma. \square

Lemma A.4. *Let G be an indecomposable simple game of one of the types B_1, B_2, B_3, T_1 , and T_3 , and let g be a player of G which is not from the least desirable level. Then the composition $G \circ_g A_n$ is not complete for all $n \geq 2$.*

Proof. Let us first consider the case where g is from the most desirable level of G . We will apply Lemma A.3 to show that $G \circ_g A_n$ is not complete. So in what follows we show that for each case there exist $g, g' \in P$ and coalitions X_1 and X_2 of G which satisfy the conditions of Lemma A.3. In the following three cases, g is a player from level 1 and g' is a player from level 2.

B_1 X_1 is of type $\{1^{k_1-1}, 2^{k_2-k_1}\}$, and X_2 is of type $\{1^{k_1-1}, 2^{k_2-k_1}\}$;

B_2 X_1 is of type $\{1^{k_1-1}\}$, and X_2 is of type $\{2^{k_1}\}$;

B_3 X_1 is of type $\{1^{k_1-1}\}$, and X_2 is of type $\{1^{k_2-n_2}, 2^{n_2-1}\}$.

For the following two cases, g is a player from level 1 and g' is a player from level 3.

T_1 X_1 is of type $\{1^{k_1-1}\}$, and X_2 is of type $\{2^{k_2}, 3^{k_3-k_2-1}\}$;

T_3 X_1 is of type $\{1^{k_2-n_2-1}, 2^{n_2}\}$, and X_2 is of type $\{1^{k_1-1}, 3^{k_3-k_1}\}$.

All is left is to consider composing games of the T types over a player from level 2. We start with T_1 . As we know any game of type T_1 contains a subgame of type B_1 when we restrict it to levels 2 and 3 only. For that subgame, 2 is the most desirable player, so non-completeness follows from the B_1 case.

Finally, we look at T_3 and suppose now g is a player from level 2 and g' is a player from level 3. Here X_1 can be taken of type $\{1^{k_2-n_2}, 2^{n_2-1}\}$. Indeed, if we add g to X_1 , it becomes winning but it loses with g' . Then X_2 can be taken of type $\{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3-1}\}$. We can add g to X_2 since $n_2 \geq k_3 - k_1 - n_3 + 1$ and it becomes winning. We can add g and remove g' from it since $n_3 \geq 2$. The coalition X_2 will remain losing after that. So we can again apply Lemma A.3 to conclude that the composition is not complete. This completes the study of compositions where G_2 is the anti-unanimity game A_n , such that the compositions are not over the least desirable level of G_1 . \square

Finally, we consider compositions where G_2 is the unanimity game U_n . It turns out that none of these compositions give a weighted game either, which is what we show next.

Lemma A.5. *Let $G_1 = (P, W)$ be a simple game of one of the types B_1, B_2, B_3, T_1 , and T_3 and let $g \in P$ be a player not from the least desirable level of G_1 . Then the composition $G = G_1 \circ_g U_n$ is not weighted.*

Proof. Let U_n be defined on P_{U_n} , and let $Z = P_{U_n}$. We start with G_1 being of type B_1 . A shift-minimal winning coalition of G_1 has the only form $\{1^{k_1}, 2^{k_2-k_1}\}$, where $k_1 < n_1$. We compose over level 1 of G_1 . Then G is non-weighted by Lemma 7.4 applied to the following trading transform:

$$(\{1^{k_1}, 2^{k_2-k_1}\}, \{1^{k_1-1}, 2^{k_2-k_1}\}; \{1^{k_1}, 2^{k_2-k_1-1}\}, \{1^{k_1-1}, 2^{k_2-k_1+1}\}).$$

This is because the first coalition is winning, the second coalition is 1-winning and the remaining two are losing. Note that $k_2 - k_1 + 1 = n_2 \geq 2$ in a game of type B_1 , so the coalition $\{1^{k_1-1}, 2^{k_2-k_1+1}\}$ is allowed.

Now let G_1 be of type B_2 . The shift-minimal winning coalitions of G_1 here are $\{1^{k_1}\}, \{2^{k_1+1}\}$, and if we compose with U_n over level 1 of G_1 , then G is non-weighted by Lemma 7.4 applied to the following trading transform:

$$(\{2^{k_1+1}\}, \{1^{k_1-1}\}; \{1^{k_1-1}, 2\}, \{2^{k_1}\}).$$

This is because the first coalition is winning and the second is 1-winning. The remaining two are losing.

Now let G_1 be of type B_3 . Recall that in a game of type B_3 we have $k_1 \leq n_1$, and also $k_2 - n_2 < k_1$. So the shift-minimal winning coalitions of G_1 are $\{1^{k_1}\}, \{1^{k_2-n_2}, 2^{n_2}\}$. If we compose with U_n over level 1 of G_1 , then G is non-weighted by Lemma 7.4 applied to the following trading transform:

$$(\{1^{k_2-n_2}, 2^{n_2}\}, \{1^{k_1-1}\}; \{1^{k_2-n_2}, 2^{n_2-1}\}, \{1^{k_1-1}, 2\}).$$

This is because the second coalition is 1-winning.

Next we look at the games T_1 and T_3 . Since they have three levels each, we need to consider what happens when composing over level 1 and when composing over level 2 separately. Let us start with T_1 .

The shift-minimal winning coalitions of G_1 are $\{1^{k_1}\}$ and $\{2^{k_2}, 3^{k_3-k_2}\}$. Here we need to consider two compositions, one over level 1, and one over level 2.

Case (i). If we compose with U_n over level 1 of G_1 then G is non-weighted by Lemma 7.4 applied to the following trading transform:

$$(\{1^{k_1-1}\}, \{2^{k_2}, 3^{k_3-k_2}\}; \{1^{k_1-1}, 2\}, \{2^{k_2-1}, 3^{k_3-k_2}\}).$$

This is because the first coalition is 1-winning, the second is winning, and the remaining two are losing.

Case (ii). If we compose with U_n over level 2 of G_1 , then G is non-weighted by Lemma 7.4 applied to the following trading transform:

$$(\{1^{k_1}\}, \{2^{k_2-1}, 3^{k_3-k_2}\}; \{1^{k_1-1}, 2\}, \{1, 2^{k_2-2}, 3^{k_3-k_2}\}).$$

This is because the first coalition is winning, the second coalition is 2-winning, and the remaining two are losing.

Finally, suppose G_1 is of type T_3 . The shift-minimal winning coalitions of G_1 are $\{1^{k_2-n_2}, 2^{n_2}\}$ and $\{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3}\}$. Here we again need to consider two compositions, one over level 1, one over level 2.

Case (i). If we compose G_1 with U_n over level 1 of G_1 , then since $k_1 \leq n_1$, the game G is non-weighted by Lemma 7.4 applied to the following trading transform:

$$(\{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3}\}, \{1^{k_1-1}, 2^{k_3-k_1-n_3}, 3^{n_3}\}; \{1^{k_1}, 2^{k_3-k_1-n_3-1}, 3^{n_3}\}, \{1^{k_1-1}, 2^{k_3-k_1-n_3+1}, 3^{n_3}\}).$$

This is because the first coalition is winning, the second coalition is 1-winning, and the two remaining ones are losing. Note that $k_3 - k_1 - n_3 + 1 \leq n_2$ in a game of type T_3 (see Theorem 6.1), so the last coalition exists.

Case (ii). If we compose with U_n over level 2 of G_1 , then G is non-weighted by Lemma 7.4 applied to the following trading transform:

$$(\{1^{k_2-n_2}, 2^{n_2-1}\}, \{1^{k_1}, 3^{k_3-k_1}\}; \{1^{k_2-n_2}, 2^{n_2-1}, 3\}, \{1^{k_1}, 3^{k_3-k_1-1}\}).$$

Indeed, by (2.6), $k_2 - n_2 \leq n_1$ and $k_2 < k_3$. Thus the first coalition exists and is 2-winning, the second is winning, and the remaining two are losing. \square

We see that none of the six games above produces a weighted game when composed with U_n over a player not from the least desirable level of the first game.

References

- [1] A. Beimel, Secret-sharing schemes: A survey, in: *Coding and Cryptology*, Lecture Notes in Comput. Sci. 6639, Springer, Berlin (2011), 11–46.
- [2] A. Beimel, T. Tassa and E. Weinreb, Characterizing ideal weighted threshold secret sharing, *SIAM J. Discrete Math.* **22** (2008), no. 1, 360–397.
- [3] J. Benaloh and J. Leichter, Generalized secret sharing and monotone functions, in: *Advances in Cryptology* (Crypto '88), Lecture Notes in Comput. Sci. 403, Springer, Berlin (1990), 27–35.
- [4] G. R. Blakley, Safeguarding cryptographic keys, in: *Proceedings of the National Computer Conference 1979*, American Federation of Information Processing Societies Proceedings 48, AFIPS Press (1979), 313–317.
- [5] E. Brickell and D. Davenport, On the classification of ideal secret sharing schemes, *J. Cryptology* **4** (1991), 123–134.
- [6] F. Carreras and J. Freixas, Complete simple games, *Math. Social Sci.* **32** (1996), no. 2, 139–155.
- [7] C. C. Elgot, Truth functions realizable by single threshold organs, in: *Proceedings of the Second Annual Symposium on Switching Circuit Theory and Logical Design* (SWCT 1961), AIEE (1961), 225–245.
- [8] O. Farràs, J. Martí-Farré and C. Padró, Ideal multipartite secret sharing schemes, *J. Cryptology* **25** (2012), 434–463.
- [9] O. Farràs and C. Padró, Ideal hierarchical secret sharing schemes, in: *Theory of Cryptography*, Lecture Notes in Comput. Sci. 5978, Springer, Berlin (2010), 219–236.
- [10] O. Farràs and C. Padró, Ideal hierarchical secret sharing schemes, *IEEE Trans. Inform. Theory* **58** (2012), no. 5, 3273–3286.
- [11] T. Gvozdeva, A. Hameed and A. Slinko, Weightedness and structural characterization of hierarchical simple games, *Math. Social Sci.* **65** (2013), no. 3, 181–189.
- [12] T. Gvozdeva and A. Slinko, Weighted and roughly weighted simple games, *Math. Social Sci.* **61** (2011), no. 1, 20–30.
- [13] E. Karnin, J. W. Greene and M. Hellman, On secret sharing systems, *IEEE Trans. Inform. Theory* **29** (1983), no. 1, 35–41.
- [14] K. Martin, New secret sharing schemes from old, *J. Combin. Math. Combin. Comput.* **14** (1993), 65–77.
- [15] C. Padró and G. Sáez, Secret sharing schemes with bipartite access structure, in: *Advances in Cryptology* (Eurocrypt '98), Lecture Notes in Comput. Sci. 1403, Springer, Berlin (1998), 500–511.
- [16] C. Padró and G. Sáez, Correction to “Secret sharing schemes with bipartite access structure”, *IEEE Trans. Inform. Theory* **50** (2004), no. 6, 1373.
- [17] P. Seymour, On secret-sharing matroids, *J. Combin. Theory Ser. B* **56** (1992), no. 1, 69–73.
- [18] A. Shamir, How to share a secret, *Commun. ACM* **22** (1979), 612–613.
- [19] L. S. Shapley, Simple games: An outline of the descriptive theory, *Behavioral Sci.* **7** (1962), no. 1, 59–66.
- [20] D. Stinson, An explication of secret sharing schemes, *Design Code Cryptogr.* **2** (1992), 357–390.
- [21] A. Taylor and W. Zwicker, *Simple Games*, Princeton University Press, Princeton, 1999.
- [22] J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton University Press, Princeton, 1944.