Nimber-Preserving Reduction: Game Secrets And Homomorphic Sprague-Grundy Theorem

Kyle W. Burke
Department of Computer Science, Plymouth State University, NH, USA

Matthew Ferland
Department of Computer Science, University of Southern California, Los Angeles, CA, USA

Shang-Hua Teng
Department of Computer Science, University of Southern California, Los Angeles, CA, USA

Abstract

The concept of nimbers – a.k.a. Grundy-values or nim-values – is fundamental to combinatorial game theory. Beyond the winnability, nimbers provide a complete characterization of strategic interactions among impartial games in disjunctive sums. In this paper, we consider nimber-preserving reductions among impartial games, which enhance the winnability-preserving reductions in traditional computational characterizations of combinatorial games. We prove that Generalized Geography is complete for the natural class, $\mathcal{I}P$, of polynomially-short impartial rulesets, under polynomial-time nimber-preserving reductions. We refer to this notion of completeness as Sprague-Grundy-completeness. In contrast, we also show that not every PSPACE-complete ruleset in $\mathcal{I}P$ is Sprague-Grundy-complete for $\mathcal{I}P$.

By viewing every impartial game as an encoding of its nimber – a succinct game secret richer than its winnability alone – our technical result establishes the following striking cryptography-inspired homomorphic theorem: Despite the PSPACE-completeness of nimber computation for $\mathcal{I}P$, there exists a polynomial-time algorithm to construct, for any pair of games $G_1, G_2$ in $\mathcal{I}P$, a Generalized Geography game $G$ satisfying:

$$\text{nimber}(G) = \text{nimber}(G_1) \oplus \text{nimber}(G_2).$$

1 Introduction

Mathematical games are fun and intriguing. Even with succinct rule sets (which define game positions and the players’ options from each position), they can grow game trees of size exponential in that of the starting positions. A game is typically formulated for two players. They take turns strategically selecting from the current options to move the game state to the next position. In the normal-play convention, the player that faces a terminal position – a position with no feasible options – loses the game. The game tree from a starting position – with the leaves as the terminal positions – naturally captures this alternation of all potential feasible moves.
Over the years, rulesets have been formulated based on graph theory [4, 24, 11], logic [28], topology [25, 19, 27, 30, 10], and other mathematical fields, often inspired by real-world phenomena [21, 1, 20, 13, 32, 8, 2, 33]. These rulesets distill fundamental mathematical concepts, structures, and dynamics. For example:

- **Node Kayles** [28] models a strategic game of growing a maximal independent set: Each position is an undirected graph, and each move consists of removing a node and its neighbors.
- **Generalized Geography** [28, 24] models a two-player game of traversing maximal paths: Each position is defined by a token in a directed graph and a move consists of removing the current vertex from the graph and moving the token to an out-neighbor. (It is often just referred to as Geography.)
- **Atropos** [10] models the dynamic formation of discrete equilibria (panchromatic triangles) in topological maps: Positions are partially colored Sperner triangles, and a move consists of coloring a vertex.

The deep alternation of strategic reasoning also intrinsically connects optimal play in many games to highly intractable complexity classes, most commonly \( \text{PSPACE} \). After Even and Tarjan proved this for a generalization of Nash’s Hex [14], deciding winnability of many natural combinatorial games – including Node-Kayles, Generalized Geography, Avoid True, Proper-\(K\)-Coloring, Atropos, Graph Nim, and Generalized Chomp\(^1\) – have been shown to be PSPACE-complete [28, 24, 11, 3, 10, 30, 22].

### 1.1 A Classical Mathematical Theory for Impartial Games

Mathematical characterizations of combinatorial games emerged prior to the age of modern computational complexity theory. In 1901, Bouton [5] developed a complete theory for Nim, based on an ancient Chinese game Jian Shi Zi (捡石子 - picking stones). A Nim position is a collection of piles of (small) stones. On their turn, a player takes one or more stones from exactly one of the piles. Representing each Nim position by a list of integers, Bouton [5] proved that the current player has a winning strategy in the normal-play setting if and only if the bitwise-exclusive-or of these integers (as binary representations) is not zero. Note that although the game tree of a Nim position could be exponentially tall in the number of bits representing the position, Bouton’s characterization provides a polynomial-time solution for determining the winnability of Nim games.

Nim is an example of an *impartial* ruleset, meaning both players have the same options at every position. Games that aren’t impartial are known as *partisan*. The two graph games, Node-Kayles and Generalized Geography aforementioned, are also impartial.

In the 1930s, Sprague [31] and Grundy [23] independently developed a comprehensive mathematical theory for impartial games. They introduced a notion of *equivalence* among games, characterizing their contributions in the disjunctive sums with other impartial games. Extending Bouton’s theory for Nim, Sprague-Grundy Theory provides a complete mathematical solution to the disjunctive sums of impartial games.

> **Definition 1 (Disjunctive Sum).** For any two game positions \(G\) and \(H\) (respectively, of rulesets \(R_1\) and \(R_2\)), their disjunctive sum, \(G + H\), is a game position in which at each turn, the current player chooses to make a move in exactly one of \(G\) and \(H\), leaving the other unchanged. A sum position \(G + H\) is terminal if and only if both \(G\) and \(H\) are terminal according to their own rulesets.

\(^1\) We consider Generalized Chomp to be Chomp, but on any Directed Acyclic Graph. This is equivalent to Finite Arbitrary Poset Game, when the partial order can be evaluated in polynomial time.
Sprague and Grundy showed that every impartial game $G$ can be equivalently replaced by a single-pile Nim game in any disjunctive sum involving $G$. Thus, they characterized each impartial game by a natural number – now known as the *nimber*, *Grundy value*, or *nim-value* – which corresponds to a number of stones in a single-pile of Nim. Mathematically, the nimber of $G$, which we denote by $\text{nimber}(G)$, can be recursively formulated via $G$’s game tree: (1) if $G$ is terminal, then $\text{nimber}(G) = 0$; otherwise (2) if $\{G_1, \ldots, G_k\}$ is the set options of $G$, letting $\text{mex}$ returns the smallest value of $(\mathbb{Z}^+ \cup \{0\}) \setminus \{\text{nimber}(G_1), \ldots, \text{nimber}(G_k)\}$, then:

$$\text{nimber}(G) = \text{mex}(\{\text{nimber}(G_1), \ldots, \text{nimber}(G_k)\}). \quad (1)$$

Let $\oplus$ denote the *bitwise xor* (*nim-sum*). By Bouton’s Nim theory [5]:

$$\text{nimber}(G + H) = \text{nimber}(G) \oplus \text{nimber}(H) \quad \forall \text{impartial } G, H. \quad (2)$$

Thus, Sprague-Grundy Theory – using Bouton’s Nim solution – provides an instrumental mathematical summary (of the much larger game trees) that enhances the winnability for impartial games: A position is a winning position if and only if its nimber is non-zero. This systematic framework inspired subsequent work in the field, including Berlekamp, Conway, and Guy’s *Winning Ways for Your Mathematical Plays* [4], and Conway’s *On Numbers And Games* [11], which laid the foundation for Combinatorial Game Theory (CGT). This 1930s theory also has an algorithmic implication. Equation (2) provides a polynomial-time framework for computing the nimber of a sum game – and the hence the winnability – from the nimbers of its component games: If the nimbers of two games $G$ and $H$ are tractable, then $\text{nimber}(G + H)$ is also tractable.

### 1.2 Our Main Contributions

Obviously, in spite of this algorithmic implication, Sprague-Grundy Theory does not provide a general-purpose polynomial-time solution for all impartial games, as witnessed by many PSPACE-hard rulesets, including *Node Kayles* and *Generalized Geography* [28, 24]. If one views the nimber characterization of an impartial game as a reduction from that game to a single pile Nim, then Schaefer *et al*’s complexity results demonstrate that this reduction has intractable constructability. In fact, a recent result [9] proved that the nimber of polynomial-time solvable *Undirected Geography* – i.e., *Generalized Geography* on undirected graphs – is also PSPACE-complete to compute. The sharp contrast between the complexity of winnability and nimber computation illustrates a fundamental mathematical-computational divergence in Sprague-Grundy Theory [9]: Nimbers can be PSPACE-hard “secrets of deep alternation” even for polynomial-time solvable games.

Computational complexity theory often gives new perspectives of classical mathematical results. In this work, it also provides us with a new lens for understanding this classical mathematical characterization as well as tools for exploring and identifying new fundamental characterizations in combinatorial game theory.
1.2.1 Polynomial-Time Nimber-Preserving Reduction to Generalized Geography

In this paper, we consider the following natural concept of reduction among impartial games.

Definition 2 (Nimber-Preserving Reduction). A map $\phi$ is a nimber-preserving reduction from impartial ruleset $R_1$ to impartial ruleset $R_2$ if for every position $G$ of $R_1$, $\phi(G)$ is a position of $R_2$ satisfying $\text{nimber}(G) = \text{nimber}(\phi(G))$.

Because an impartial position is a losing position if and only if its nimber is zero, nimber-preserving reductions enhance winnability-preserving reductions in traditional complexity-theoretical characterizations of combinatorial games [14, 28]: Polynomial-time nimber-preserving reductions introduce the following natural notion of “universal” impartial rulesets.

Definition 3 (Sprague-Grundy Completeness). For a family $\mathcal{J}$ of impartial rulesets, we say $R \in \mathcal{J}$ is a Sprague-Grundy-complete ruleset for $\mathcal{J}$ if for any position $Z$ of any ruleset of $\mathcal{J}$, one can construct, in polynomial time, a position $G \in R$ such that $\text{nimber}(G) = \text{nimber}(Z)$.

As the main technical contribution of this paper, we prove the following theorem regarding the expressiveness of Generalized Geography. The natural family of rulesets containing Generalized Geography is $\mathcal{I}^P$, the family of all impartial rulesets whose positions have game trees with height polynomial in the sizes of the positions. We call games of $\mathcal{I}^P$ polynomially-short games. In addition to Generalized Geography, $\mathcal{I}^P$ contains many combinatorial rulesets studied in the literature, including Node Kayles, Chomp, Proper-K-Coloring, Atropos, and Avoid True, as well as Nim and Graph Nim with polynomial numbers of stones.

Theorem 4 (A Complete Geography). Generalized Geography is a Sprague-Grundy complete ruleset for $\mathcal{I}^P$.

In other words, for example, given any Node Kayles or Avoid True game, we can, in polynomial time, generate a Generalized Geography game with the same Grundy value, despite the fact that the Grundy value of the input game could be intractable to compute.

Because nimber-preserving reductions generalize winnability-preserving reductions, every Sprague-Grundy complete ruleset for $\mathcal{I}^P$ must be PSPACE-complete to solve. However, for a simple mathematical reason, we have the following observation:

Proposition 5. Unless $P = \text{PSPACE}$, not every PSPACE-complete ruleset in $\mathcal{I}^P$ is Sprague-Grundy complete for $\mathcal{I}^P$.

In particular, Atropos [10] is PSPACE-complete but not Sprague-Grundy-complete for $\mathcal{I}^P$. Thus, together Theorem 4 and Proposition 5 highlight the fundamental difference between winnability-preserving reductions and nimber-preserving reductions. Our result further illuminates the central role of Generalized Geography – a classical PSPACE-complete ruleset instrumental to Lichtenstein-Sipser’s PSPACE-hard characterization of Go [16] – in the complexity-theoretical understanding of combinatorial games.

In Section 5, when discussing related questions, we also demonstrate the brief corollary:

---

2 This natural concept of reduction in combinatorial game theory can be viewed as the analog of functional-preserving reductions in various fields. To name a few: approximation-preserving, gap-preserving, structure-preserving reductions in complexity and algorithmic theory; hardness-preserving and security-preservation in cryptography; dimension-preserving, metric-preserving, and topology-preserving reductions in data analytics; parameter-preserving reductions in dynamic systems; counterexample-preserving reductions in model checking, query-number-preserving, sample-preserving and high-order-moment-preserving in statistical analysis; and modularity-preserving reductions in network modeling. We are inspired by several of these works.
Corollary 6. **Edge Geography** (formulated in [28] and studied in [17], see Section 5.1 for the ruleset) is also Sprague-Grundy-complete for \( I^P \).

### 1.2.2 Game Secrets: Homomorphic Sprague-Grundy Theorem

In the framework of disjunctive sums, every impartial game \( G \) encodes a secret, i.e., its Grundy value \( \text{nimber}(G) \), which succinctly summarizes \( G \)'s game tree and can be represented by a single-pile Nim. Once this secret is obtained, by Sprague-Grundy theory, one can replace \( G \) by its equivalent single-pile Nim in any disjunctive sum involving \( G \). Even though Nim is expressive enough to provide natural game representations of these game secrets, it does not admit an efficient reduction, even for polynomial-time solvable games, such as Undirected Geography, in \( I^P \).

In contrast, for impartial games in \( I^P \), Theorem 4 shows that **Generalized Geography** provides natural game representations of these game secrets. In conjunction with Sprague-Grundy theory, this Generalized Geography-based encoding of nimbers leads to a surprising cryptography-inspired homomorphic characterization of impartial games.

**Theorem 7 (Homomorphic Sprague-Grundy-Bouton Theorem).** \( I^P \) enjoys the following two contrasting properties:

- **Hard-Core Nimber Secret:** The problem of computing the nimber – i.e., finding \( \text{nimber}(G) \) given a position \( G \) of \( I^P \) – is PSPACE-complete.
- **Homomorphic Game Encoding:** For any pair of positions \( G_1 \) and \( G_2 \) of \( I^P \), one can, in polynomial-time (in the sizes of \( G_1 \) and \( G_2 \)), construct a Generalized Geography game \( G \), such that:

  \[
  \text{nimber}(G) = \text{nimber}(G_1) \oplus \text{nimber}(G_2).
  \]

Like the Sprague-Grundy theory – which represents the game values by natural games – Theorem 7 encodes “nimber secrets” with natural games. The former uses “single-pile” Nim and the later uses “single-graph” Generalized Geography. For both, one can compute, in polynomial time, the representation of the disjunctive sum of any two representations. Because Generalized Geography is not naturally closed under disjunctive sums, genuine computational effort – although feasible in polynomial-time – is required in the homomorphic encoding of the disjunctive sum.

**Figure 1** Two transformations of impartial games \( A \) and \( B \) into a single game equivalent to their disjunctive sum.
1.3 Remarks

This genuineness can be partially captured by Conway’s notion of prime impartial games in his studies of misère games. Let prime impartial games be ones that can’t be expressed as the disjunctive sum of any two other games (see Section 4.1 for the formal definition). Like the role of prime numbers in the multiplicative group over integers, these games are the basic building blocks in the disjunctive-sum-based monoid over impartial games.

In Theorem 20, we will prove that each Generalized Geography game created in the proof of Theorem 7 is indeed a prime game. Thus, in Theorem 7, because $G$ is a natural prime game, the algorithm for “Homomorphic Game Encoding” cannot trivially output the syntactic description of $G_1 + G_2$. Thus, it must use a more “elementary” position to encode nimber ($G_1$) $\oplus$ nimber ($G_2$). In other words, the bitwise-xor of the PSPACE-hard “nimber secrets” encoded in any two impartial games of $\mathcal{I}_P$ can be efficiently re-encoded by a natural prime game of $\mathcal{I}_P$, whose game tree is not isomorphic to that of $G_1 + G_2$.

Conway’s notation of prime games only partially captures the genuineness of the homomorphic encoding in Theorem 7 because one may locally modify the game rule for some zero positions to make the sum game prime without changing the nimber. So the naturalness of Generalized Geography captures more beyond the current concept of prime games. We continue to look for a more accurate characterization.

Note also that the characterization presented in Theorem 7 is cryptography-inspired rather than cryptographically-applicable. In partially homomorphic encryption, the encoding functions, such as RSA encryption and discrete-log, must be one-way functions. Here, we consider a game position as a “natural encoding” of its nimber-secret: The focus of Theorem 7 is on the complexity-based homomorphic property of this encoding (and that it arises naturally from impartial games) rather than the construction of homomorphic “one-way” game-based encryption of secret messages. (See Section, 5 – Conclusion and Open Questions – for more discussion on this.) Thus, in contrast to (partially) homomorphic cryptographic functions – such as discrete-log and RSA – whose secret messages can be recovered in NP (due to a one-way encoding of secrets), “decoding” the nimber-secrets – as they are naturally encoded in combinatorial games of $\mathcal{I}_P$ – is PSPACE-complete in the worst case.

2 Impartial Games and Their Trees: Notation and Definitions

In this section, we review some background concepts and notation. In the paper, we use $\mathcal{I}$ to denote the family of all impartial rulesets; we use $\mathcal{I}_P$ to denote the family of all impartial games – positions – defined by rulesets in $\mathcal{I}$; we use $\mathcal{I}_P$ to denote the family of all polynomially-short impartial games, i.e., positions defined by rulesets in $\mathcal{I}_P$.

Each impartial ruleset $R \in \mathcal{I}$ has two mathematical components $(B_R, \rho_R)$, where $B_R$ represents the set of all possible game positions in $R$ and $\rho_R : B_R \rightarrow 2^{B_R}$ defines the options for each position in $R$. For each position $G \in B_R$, the ruleset $R$ defines a natural game tree, $T_G$, rooted at $G$. $T_G$ recursively branches with feasible options. The root is associated with position $G$ itself. The number of children that the root has is equal to the number of options, i.e., $|\rho_R(G)|$, at $G$. Each child is associated with a position from $\rho_R(G)$ and its sub-game-tree is defined recursively. Thus, $T_G$ contains all reachable positions of $G$ under ruleset $R$. The leaves of $T_G$ are terminal positions under the normal-play setting. Up to isomorphism, the game tree for an impartial game is unique.

Definition 8 (Game isomorphism). Two impartial games, $G$ and $H$, are isomorphic to each other if $T_G$ is isomorphic to $T_H$. 
For any two impartial games \( F \) and \( G \), the game tree \( T_{(F+G)} \) of their disjunctive sum can be more naturally characterized via \( T_F \otimes T_G \), the Cartesian product of \( T_F \) and \( T_G \). Clearly, \( T_F \otimes T_G \) is a directed acyclic graph (DAG) rather than a rooted tree, as a node may have up to two parents. The game tree \( T_{(F+G)} \) can be viewed as a tree-expansion of DAG \( T_F \otimes T_G \).

To turn it into a tree, one may simply duplicate all subtrees whose root has two parents, and give the parents edges to different roots of those two subtrees. We will use \( T_F \boxdot T_G \) to denote this tree expansion of the Cartesian product \( T_F \otimes T_G \), and call it the tree sum of \( T_F \) and \( T_G \).

In combinatorial game theory (CGT), each ruleset usually represents an infinite family of games, each defined by its starting position. For algorithmic and complexity analyses, a size is associated with each game position as the basis for measuring complexity [28, 15, 26, 7]. Examples include: (1) the number of vertices in the graph for \textsc{Node Kayles} and \textsc{Generalized Geography}, (2) the board length of \textsc{Hex} and \textsc{Atropos}, and (3) the number of bits encoding \textsc{Nim}.

The size measure is assumed to be natural \(^3\) with respect to the key components of the ruleset. In particular, for each position \( G \) in a ruleset \( R \):

\begin{itemize}
  \item \( G \) has a binary-string representation of length polynomial in size(\( G \)).
  \item Each position reachable from \( G \) has size upper-bounded by a polynomial function in size(\( G \)).
  \item Determining if a position of \( F \in B_R \) is an option of \( G \) – i.e., whether \( F \in \rho_R(G) \) – takes time polynomial in size(\( G \)).
\end{itemize}

Recall that the family, \( \mathcal{I}^P \), discussed in the introduction is formulated based on the sizes of game positions.

\textbf{Definition 9 (Polynomially-Short Games).} A combinatorial ruleset \( R = (B_R, \rho_R) \) is polynomially short if the height of the game tree \( T_G \) of each position \( G \in B_R \) is polynomial in size(\( G \)). Furthermore, we say \( R \in \mathcal{I}^P \) is polynomially-wide if for each position \( G \in B_R \), the number of options \( |\rho_R(G)| \) is bounded by a polynomial function in size(\( G \)).

We call games of \( \mathcal{I}^P \) polynomially-short games. \textsc{Generalized Geography} and \textsc{Node Kayles} are among the many examples of games that are both polynomially-wide and polynomially-short. \textsc{Nim}, however, is neither polynomially-wide nor polynomially-short due to the binary encoding of the piles. In general, under the aforementioned assumption regarding the size function of game positions, \( |\rho_R(G)| \) could be exponential in size(\( G \)). However, positions in \( \rho_R(G) \) can be enumerated in polynomial space. Therefore, by DFS evaluation of game trees and classical complexity analyses of \textsc{Node Kayles}, \textsc{Generalized Geography} and \textsc{Avoid True}:

\textbf{Proposition 10 (PSPACE-Completeness).} For any polynomially-short impartial ruleset \( R \) and a position \( G \) in \( R \), nimber(\( G \)) can be computed in space polynomial in size(\( G \)). Furthermore, under Cook-Turing reductions, nimber computation for some games in \( \mathcal{I}^P \) is PSPACE-hard.

An impartial ruleset is said to be polynomial-time solvable – or simply, tractable – if there is a polynomial-time algorithm to identify a winning option whenever there exists one (i.e., for the search problem associated with the decision of winnability). If one doesn’t exist, then the algorithm needs to only identify this.

\(^3\) In other words, the naturalness assumption rules out rulesets with embedded hard-to-compute predicate like – as a slightly dramatized illustration – “If P ≠ PSPACE is true, then the feasible options of a position include a special position.”
10:8 Nimber-Preserving Reductions

## 3 Star Atlas: A Complete Generalized Geography

In our analysis, we will use the standard CGT notation for nimbers: \( *k \) for \( k \), except that \( * \) is shorthand for \( *1 \) and \( 0 \) is shorthand for \( *0 \).\(^4\) Mathematically, one can view \( * \) as a map from \( \mathbb{Z}^+ \cup \{0\} \) to (infinite) subfamilies of impartial games in \( \mathbb{Z} \), such that for each \( k \in \mathbb{Z}^+ \cup \{0\} \), nimber \((G) = k \), for all \( G = *k \). In other words, \( * \) is nature’s game encoding of non-negative integers.

Sprague-Grundy Theory establishes that each impartial game’s strategic relevance in disjunctive sums is determined by its nimber (i.e., its star value). In this section, we prove our proof starts with the following basic property of nimbers, which follows from the recursive definition (given in Equation 1):

\[ * \text{Star Atlas: A Complete Generalized Geography} \]

\[ \text{For readability, we restate Theorem 4 to make the needed technical component explicit:} \]

**Theorem 11 (Sprague-Grundy-Completeness of Generalized Geography).** There exists a polynomial-time algorithm \( \phi \) such that for any game \( G \in \mathbb{P} \), \( \phi(G) \) is a Generalized Geography position satisfying \( \text{nimber}(\phi(G)) = \text{nimber}(G) \).

Our proof starts with the following basic property of nimbers, which follows from the recursive definition (given in Equation 1):

**Proposition 12.** For any impartial game \( G \), \( \text{nimber}(G) \) is bounded above by both the height of its game tree, \( h \), and the number of options at \( G \), \( l \). In other words, \( G = *k \), where \( k \leq \min(h,l) \).

To simplify notation, we let \( g = \min(h,l) \). To begin the reduction, we will need a reduction for each decision problem \( Q_i \) = “Does \( G = *i \)?” (\( \forall i \in [g] \)). By Proposition 10, the decision problem \( Q_i \) is in \( \text{PSPACE} \). Thus, we can reduce each \( Q_i \) to an instance in the \( \text{PSPACE-complete QSAT (Quantified SAT)} \), then to a \( \text{Geography} \) instance using the classic reduction, \( f \), from [28, 24]. Referring to the starting node of \( f(Q_i) = s_i \), we add two additional vertices, \( a_i \) and \( b_i \), with directed edges \((b_i, a_i)\) and \((a_i, s_i)\). Now,

- \( s_i \) has exactly two options, so the value of \( f(Q_i) \) is either 0, \( * \), or \( *2 \). By the reduction, it is 0 exactly when \( G \neq s_i \), and in \( \{*,2\} \) when \( G = s_i \).
- \( a_i \) has exactly one option \((s_i)\), so the value of the \( \text{Geography} \) position starting there (instead of at \( s_i \)) is 0 when \( G = s_i \) and \( * \) otherwise.
- \( b_i \) has exactly one option \((a_i)\), so the value of the \( \text{Geography} \) position starting there is \( * \) when \( G = s_i \) and 0 otherwise.

Each of these constructions from \( Q_i \) is shown in Figure 2.

We will combine these \( g + 1 \) \( \text{Geography} \) instances into a single instance, but first we need some utility vertices each equal to one of the nimber values \( 0, \ldots, * (g-2) \). We can build these using a single gadget as shown in Figure 3. This gadget consists of vertices \( t_0, t_1, \ldots, t_{g-2} \) with edges \((t_i, t_j)\) for each \( i > j \). Thus, each vertex \( t_i \) has options to \( t_j \) where \( j < i \) and no other options, exactly fulfilling the requirements for \( t_i \) to have value \( *i \).

Now we build a new gadget to put it all together and combine the \( f(Q_i) \) gadgets, as shown in Figure 4:

- \( \forall i \geq 1 \) : add a vertex \( c_i \) as well as edges \((c_i, b_i)\) and \( \forall j \in [1, i - 2] : (c_i, t_j) \).
- \( \forall i \geq 2 \) : add a vertex \( d_i \) as well as edges \((d_i, b_1)\) and \( \forall j \in [2, i - 1] : (d_i, c_j) \).
- Finally, add a vertex \( \text{start} \) with edges \((\text{start}, b_0), (\text{start}, c_1)\), and \( \forall j \in [2, g] : (\text{start}, d_j) \).

\(^4\) The reason for the \( *0 = 0 \) convention is that it is equivalent to the integer zero in CGT.
Lemma 13. The Geography position starting at each vertex $c_i$ has value $*(i-1)$ if $G \neq *i$, and value 0 otherwise.

Proof. The Geography position starting at $c_i$ has options to $t_j$, $\forall t \in [1, i-2]$. That means that $c_i$ has options with values $*, \ldots, *(i-2)$. If the move to $b_i$ has value 0, then there are moves to $0, *, \ldots, *(i-2)$, so the value at $c_i$ is $*(i-1)$. Otherwise, there is no option from $c_i$ to a zero-valued position, so the value at $c_i$ is 0.

Lemma 14. If $G = 0$, then the Geography position starting at each vertex $d_i$ has value $*i$.

Proof. $d_i$ has moves to $b_1, c_2, \ldots, c_i$. Since $G = 0$, by Lemma 13 none of the vertices $c_j$ have values 0 (and $b_1$ does have value 0), so the options have values $0, *, *2, \ldots, *(i-1)$, respectively. The mex of these $i$'s, so $d_i$ has value $*i$.

Lemma 15. Let $G = *k$, where $k > 0$. Then the Geography position starting at each vertex $d_i$ has value $*i$ if $i < k$, and value $*(k-1)$ if $i \geq k$.

Proof. We need to prove this by cases. We’ll start with $k = 1$, then show it for $k \geq 2$.

When $k = 1$, $d_i$ has moves to $b_1, c_2, \ldots, c_i$. (There is no $d_0$ or $d_1$, so $i > k$.) The value at $b_1$ is $*$, and by Lemma 13, the remainder have values $*, *2, \ldots, *(i-1)$, respectively. 0 is missing from this list, so $d_i = 0 = *(1-1) = *(k-1)$.

For $k \geq 2$, we will split up our analysis into the two cases: $i < k$ and $i \geq k$.

We will next consider the case where $k \geq 2$ and $i < k$. From $d_i$ there are moves to $b_1, c_2, \ldots, c_i$. Since $k > i$, these have values $0, *, *2, \ldots, *(i-1)$, respectively, by Lemma 13. The mex of these is $*i$, so $d_i$ has value $*i$.

Finally, when $k \geq 2$ and $i \geq k$, $d_i$ has options to $b_1, c_2, \ldots, c_{k-1}, c_k, c_{k+1}, \ldots, c_i$. By Lemma 13, these have values $0, *, *2, \ldots, *(k-2), 0, *k, \ldots, *(i-1)$, respectively. $*(k-1)$ doesn’t exist in that list, so that’s the mex, meaning the value of $d_i$ is $*(k-1)$.

Figure 2 Result of the classic QSAT and Geography reductions of the question, $Q_i$, “Does $G = *i$?”, with the added vertices $a_i$ and $b_i$.

Figure 3 Vertices $t_0$ through $t_{g-2}$. Each vertex $t_i$ has edges to $t_0, t_1, \ldots, t_{i-1}$. Thus, the nimber value of the Geography position at vertex $t_i$ is $*i$. 
\textbf{Theorem 16.} Let $G = *k$. Then the \textsc{Geography} position beginning at start equals $*k$.

\textbf{Proof.} The options from \textit{start} are $b_0$, $c_1$, and $\forall i \in [2, g] : d_i$. If $G = 0$, then $b_0$ is $*$, $c_1$ is $*$, and, by Lemma 14, each $d_i$ is $*i$. Since 0 is missing from these options, the value at \textit{start} is $0 = *k$.

If $G = *$, then the move to $b_0$ is 0, the move to $c_1$ is also 0, and, by Lemma 15, the moves to $d_i$ is each also 0, because each $i > k = 1$ and $* (k - 1) = * (1 - 1) = 0$. All the options are to 0, so the value at \textit{start} is $* = *k$.

Finally, if $G = *k$, where $k \geq 2$, then the moves are to $b_0$, $c_1$, $d_2$, $\ldots$, $d_{k-1}$, $d_k$, $d_{k+1}$, $\ldots$, $d_g$. These have values, respectively, 0, $*$, $*2$, $\ldots$, $*(k-1)$, $*(k-1)$, $*(k-1)$, $\ldots$, $*(k-1)$, by Lemma 15. The mex of these is $k$, so the value of \textit{start} is $*k$.

\section{Nimber Secrets: A PSPACE-Complete Homomorphic Encoding}

Mathematically, Sprague-Grundy Theory together with Bouton’s \textsc{Nim} characterization provide an algebraic view of impartial games. Their framework establishes that the Grundy function, $\text{nimmer}(\cdot)$, is a morphism from the monoid $(I, +)$ – impartial games with disjunctive sum – to the monoid $(\mathbb{Z}^+ \cup \{0\}, \oplus)$ – non-negative integers in binary representations with bitwise-xor:

$$\text{nimmer}(G + H) = \text{nimmer}(G) \oplus \text{nimmer}(H) \quad \forall \ G, H \in I.$$

Elegantly,

1. $\text{nimmer}(G)$ can also be represented by a natural game, i.e., a single pile \textsc{Nim} with $\text{nimmer}(G)$ stones, and
2. the sum of two single-pile \textsc{Nim} games can be represented by another single-pile \textsc{Nim} whose game tree can be significantly different from the game tree of the sum.

The only “blemish” – from computational perspective – is that the Grundy function can be intractable to compute [28], even for some tractable games in $\mathbb{P}^9$ [9].
Theorem 11 provides an alternative natural game representation of $\text{nimber}(G)$, for $G \in \mathbb{P}$. In contrast to Nim, Generalized Geography admits a polynomial-time algorithm for computing this representation from $G$ without the need of computing $\text{nimber}(G)$. In fact, using Theorem 11, one can also compute, in polynomial time, a single-graph Generalized Geography representation of the sum of any two (Generalized Geography) games:

**Theorem 17 (Homomorphic Game Encoding of Grundy Values).** For any pair of games $G_1, G_2 \in \mathbb{P}$, one can, in polynomial-time in size($G_1$) + size($G_2$), construct a Generalized Geography game $G$, such that:

$$\text{nimber}(G) = \text{nimber}(G_1) \oplus \text{nimber}(G_2).$$

**Proof.** Given the game functions $\rho_{G_1}$ and $\rho_{G_2}$, in time linear in size($G_1$) + size($G_2$), one can construct a game function $\rho_{(G_1+G_2)}$ for their disjunctive sum $G_1 + G_2$ such that the game tree of $\rho_{(G_1+G_2)}$ is $G_1 \Box G_2$. This theorem follows from Theorem 4 and the following basic fact:

The disjunctive sum $(G_1 + G_2)$ of two polynomially-short games $G_1, G_2 \in \mathbb{P}$ remains polynomially short in terms of size($G_1$) + size($G_2$).

Now we can apply Theorem 4 to $\rho_{(G_1+G_2)}$ to construct a prime Generalized Geography $G$ in time polynomial in size($G_1$)+size($G_2$). $G$ satisfies: $\text{nimber}(G) = \text{nimber}(G_1) \oplus \text{nimber}(G_2)$. The correctness follows from that of Theorem 4 and Sprague-Grundy Theory.

Figuratively, every impartial game $G$ encodes a secret, $\text{nimber}(G)$. The game $G$ itself can be viewed as an “encryption” of its nimber-secret. The players who can uncover this nimber-secret can play the game optimally. For every game $G \in \mathbb{P}$, this secret can be “decrypted” by a DFS-based evaluation of $G$’s game tree in polynomial space. Thus, computing the nimber for $G$ is PSPACE-complete (under the Cook-Turing reduction).

Speaking of encryption, several basic cryptographic functions have homomorphic properties. For example, for every RSA encryption function $\text{ENC}_{\text{RSA}}$, for every pair of its messages $m_1$ and $m_2$, the following holds:

$$\text{ENC}_{\text{RSA}}(m_1 \times m_2) = \text{ENC}_{\text{RSA}}(m_1) \times \text{ENC}_{\text{RSA}}(m_2).$$

Another example is the discrete-log function. For any prime $p$, any primitive element $g \in Z_p^*$, and any two messages $m_1, m_2 \in Z_p^*$:

$$g^{m_1 + m_2} = g^{m_1} \times g^{m_2}.$$  

Assuming RSA encryption and the discrete-log function are computationally intractable to invert, these morphisms state that without decoding the secret messages from their encoding, one can efficiently encode their product or sum, respectively, with the RSA and discrete-log functions. In cryptography, these functions are said to support partially homomorphic encryption.

Together, Theorem 17 and Theorem 11 establish that polynomially-short impartial games are themselves partially homomorphic encodings of their nimber-secrets: Without decoding their nimbers, one can efficiently create a Generalized Geography game encoding the $\oplus$ of their nimbers.

Note again that homomorphic cryptographic functions, such as discrete log and RSA encryption, satisfy an additional property: They are one-way functions, i.e., tractable to compute but are assumed to be intractable to invert. Theorem 7 (and hence Theorem 17)
is inspired by the concept of partially homomorphic encryption. However, its focus is not on a one-way encoding of targeted nimber-values with impartial games in \( \mathbb{P} \). Rather, it characterizes the complexity-theoretical homomorphism in this classical and natural encoding for impartial games. Because of the one-way property, RSA and discrete-log functions are decodable by an NP-oracle. In contrast, the nimber-decoding of impartial games in \( \mathbb{P} \) is in general PSPACE-hard.

### 4.1 Natural Prime Games

Inspired by Conway’s notation with parts within the context of misère games \([11][29]\), we use the following terms to identify what game trees can be described as isomorphically the sum of two other games:

**Definition 18 (Prime Games and Composite Games).** A game \( G \) is a composite game if it is a sum of two games that both have tree-height at least 1. Otherwise, it is prime.

Note that prime games, in a similar manner to prime numbers, can only be summed by a game with tree-height of 0 (i.e., just a single vertex) and itself. It follows from the basic property of Cartesian graph products that each composite game has a unique decomposition into prime games.

**Proposition 19 (Decomposition in Prime Games).** A game \( G \) is isomorphic to a disjunctive sum of two games \( A \) and \( B \) if and only if its game tree \( T_G \) is isomorphic to \( T_A \square T_B \).

In Bouton theory for Nim, for any non-negative integers \( a, b \), even though \( \text{nimmer}(\text{Nim}(a \oplus b)) = \text{nimmer}(\text{Nim}(a)) \oplus \text{nimmer}(\text{Nim}(b)) \), \( \text{Nim}(a \oplus b) \) is not isomorphic to \( \text{Nim}(a) \oplus \text{Nim}(b) \). In fact, \( \text{Nim}(a \oplus b) \) is a natural prime game. Similarly, even though in the proof of Theorem 17, \( \rho(G_1 + G_2) \) simply copies the syntactic game transition function that can generate \( G_1 \square G_2 \), the construction in Theorem 4 generates the homomorphic prime game encoding of \( \text{nimmer}(G_1) \oplus \text{nimmer}(G_2) \).

**Theorem 20 (Prime Geography).** Each Generalized Geography position as created in the reduction in Theorem 11 is a prime game.

**Proof.** Suppose that our game tree is claimed to be \( X \square Y \), with root vertices \( x_0 \) and \( y_0 \), respectively, and both \( X \) and \( Y \) have height at least 1. We will find a contradiction.

Consider vertex \( b_0 \), an option of start. Since \( b_0 \) has only one option, that means that it must correspond to a terminal move in either \( X \) or \( Y \). WLOG, let it correspond to \( x_1 \), a terminal vertex in \( X \). Thus, \( b_0 = (x_1, y_0) \) and is isomorphic to \( Y \), because \( x_1 \) is terminal in \( X \).

The move to \( c_1 \) must be available, since otherwise the \( \text{start} \) would have only one option and thus not be a tree sum. This position also has only one option from itself. There are two cases: it either corresponds to a terminal vertex in \( X \), say \( x_2 \), or a terminal vertex in \( Y \), say \( y_1 \). In the first case, then \( c_1 = (x_2, y_0) \), which is isomorphic to \( Y \). This causes a contradiction, however, because the subtrees generated by \( b_0 \) and \( c_1 \) are not isomorphic. \( b_0 \) has 2 moves to reach \( s_0 \), but \( c_1 \) has 3 moves to reach \( s_1 \).

In the second case, \( c_1 = (x_0, y_1) \), and \( y_1 \) is terminal in \( Y \). Then that means there must be a move from \( c_1 \) to a vertex, \( v \), corresponding to \( (x_1, y_1) \). Since both \( x_1 \) and \( y_1 \) are terminal (in \( X \) and \( Y \)), that means \( v \) will be terminal in the tree sum. However, \( c_1 \) doesn’t have any options to a terminal vertex. This case cannot happen and, without any other possible cases, no such \( X \) and \( Y \) exist as factors for our tree.\[\]
5 Final Remarks and Open Questions

It is expected that PSPACE-complete games encode some valuable secrets. And once revealed, those secrets can help players in their decision making (e.g., under the guidance of Sprague-Grundy Theory). In this work, through the lens of computational complexity theory, we see that all polynomially-short impartial games neatly encode their nimber-secrets, which can be efficiently transferred into prime Generalized Geography games. The game encoding is so neat that the bitwise-xor of any pair of these nimber-secrets can be homomorphically re-encoded into another prime game in polynomial time, without the need to find the secrets first.

We are excited to discover this natural mathematical-game-based PSPACE-complete homomorphic encoding. Recreational mathematics can be simultaneously serious and fun!

The crypto-concept of (partially) homomorphic encryption has inspired us to identify these basic complexity-theoretical properties of this fundamental concept in CGT. It would have been more fulfilling if we could also make our findings useful in cryptography. Currently, we are exploring potential cryptographic applications of this “game encoding of strategic secrets,” particularly on one-way game generation for targeted nimbers. In addition to finding direct cryptographic connections, we are still exploring several concrete CGT questions. Below, we share some of them.

5.1 Expressiveness of Intractable Games: Sprague-Grundy Completeness

In this paper, we have proved that the PSPACE-complete polynomially-short Generalized Geography is prime Sprague-Grundy complete for \( I^P \). We observe that not all games in \( I^P \) with PSPACE-hard nimber computation are Sprague-Grundy complete for the family because:

1. Some intractable games can’t encode nimbers polynomially related to the input size
2. Some games with intractable nimber computation have some nim values which are tractable.

For (1), our first example is Generalized Geography on Degree-Three Graphs. In [24], Lichtenstein and Sipser proved that Generalized Geography is PSPACE-complete to solve even when the game graph is planar, bipartite, and has a maximum degree of three. These graph properties are essential to their analysis of the two-dimensional grid-based Go. Mathematically, the maximum achievable nimber in Generalized Geography on Degree-Three Graphs is three. Thus, there is no nimber-preserving reduction from higher nimber position in \( I^P \) to these low-degree Generalized Geography games. For the same reason, the PSPACE-complete Atropos introduced in [10] cannot be Sprague-Grundy complete.

\[\text{Lemma 21. The value of any Atropos position must be one of these nimbers: } 0, *, *2, \ldots, *7. (And thus, Atropos cannot be Sprague-Grundy complete.)\]

\[\text{Proof. For the details of how Atropos is played, please see [10]. If the last (played) vertex has uncolored neighbors, then there are at most six neighbors, so the highest nimber value is *6.}

\text{If the previously-played vertex is fully surrounded by colored vertices, then there are two possibilities: either all playable vertices have uncolored neighbors, or some of the playable vertices are also fully surrounded. In the first case, there may be options to all nimbers 0, *, *2, \ldots, *6, so the value here could be up to *7.}

---

\[^5\text{In this case, the next player gets a “jump” and gets to play anywhere on the board.}\]
In the second case, the current position, say $G$, is equal to the sum of the portion of the board (say, $H$) without those fully-surrounded (but playable) vertices and the portion of the board with only those vertices. Each of those vertices in $G \setminus H$ changes the value by $\star$. Thus, if there are $k$ of them, $G = H + k \times \star$. Thus, either $G = H$ or $G = H + \star$. By the previous case, the number of $H$ can be up to $\star^7$, so the value of $G$ can also be at most $\star^6$ or $\star^7$.

**Atropos** has a bounded nimber, so it cannot be Sprague-Grundy complete. ▶

For (2), both **Undirected Geography** [17] and **Uncooperative Uno** [12] \footnote{In this game, there are two hands, $H_1$ and $H_2$, which each consist of a set of cards. This is a perfect information game; so both players may see each other’s hands. Each card has two attributes, a color $c$ and a rank $r$. Each card then thus be represented $(c, r)$. A card can only be played in the center (shared) pile if the previous card matches either the $c$ of the current card or the $r$ of the current card.} are not Sprague-Grundy complete for $\mathcal{I}P$ – unless P = PSPACE – despite their nimber intractability, with **Undirected Geography** being known to have polynomially high nimber positions [9]. For **Undirected Geography**, Fraenkel, Scheinerman, and Ullman [17] presented a matching-based characterization to show these games are polynomial-time solvable. For **Uncooperative Uno**, Demaine *et al* [12] presented a polynomial-time reduction to **Undirected Geography**. Thus, any polynomial-time nimber-preserving reduction from $\mathcal{I}P$ to **Undirected Geography** (or **Uncooperative Uno**) would yield a polynomial-time algorithm for solving $\mathcal{I}P$.

Rulesets which have nimber preserving reductions from **Generalized Geography** are Sprague-Grundy complete. A simple example is the vertex version of **DiGraph Nim** [18], in which each node has a Nim pile and players can only move to a reachable node in a directed graph from the current node to pick stones. When every pile has one stone, the game is equivalent to **Generalized Geography** with the underlying graph. An interesting question is whether **Neighboring Nim** (with a polynomial number of stones) – a PSPACE-complete version of Nim played on an undirected graph [6] – is Sprague-Grundy complete.

The edge variant of **Generalized Geography**, known as the **Edge-Geography**, considered in the literature [28, 24, 17] presents a natural extension. This is a version of Geography where instead of deleting the current node after the token moves away, it is the edge traversed by the token that is deleted. **Edge-Geography** and its undirected sub-family, **Undirected Edge-Geography** are both PSPACE-complete. The following proof sketch shows that **Edge-Geography** remains Sprague-Grundy complete.

**Corollary 22.** **Edge-Geography** is prime Sprague-Grundy-complete for $\mathcal{I}P$.

**Proof.** We can follow the early parts of the proof for **Generalized Geography**. We reduce from all polynomially-short games, creating a game of **Edge-Geography** for each. Then, for each game, we again append two “filler” moves to the beginning, to ensure that it is exactly 0 or $\star$.

We can then reuse our scheme from figure 2. Since there are no cycles in that gadget, play between both **Edge-Geography** and **Generalized Geography** is identical.

Of course, the primality section required knowing that the main Geography game didn’t start with an out degree of only one. To fix this, we can simply have $v_b$ go to $v_{a1}$ and $v_{a2}$ which both only have a single edge to $v_s$. ▶

It remains open whether **Undirected Edge-Geography** is Sprague-Grundy complete.

In addition to these rulesets adjacent to **Generalized Geography**, we are interested in the following three well-studied games:

---

6 In this game, there are two hands, $H_1$ and $H_2$, which each consist of a set of cards. This is a perfect information game; so both players may see each other’s hands. Each card has two attributes, a color $c$ and a rank $r$. Each card then thus be represented $(c, r)$. A card can only be played in the center (shared) pile if the previous card matches either the $c$ of the current card or the $r$ of the current card.

In our proof for Generalized Geography, we critically use the “locality” in this graph-theoretical game: The options are defined by the graph-neighbors of the current node. Both Node-Kayles and Avoid True are far more “global”; there is no need for moves to be near the previous move. We are also interested in Generalized Chomp because the hierarchical structures from partial orders could be instrumental to analyses.

Node-Kayles – see below for more discussion – also suggests the following basic structural question:

Is there a natural ruleset in $I^P$ that is Sprague-Grundy-complete for $I^P$ but not prime Sprague-Grundy-complete for $I^P$?

5.2 Game Encoding and Computational Homomorphism

Let’s call a family $H$ of impartial rulesets satisfying Theorem 7 (in place of $I^P$ and with a prime game of $I^P$ in place of Generalized Geography) a computationally-homomorphic family. Note that for any $J$ including Undirected Geography, $J$ satisfies Theorem 7.

Now suppose we “slightly” weaken Theorem 7 by removing the prime-game requirement (in the Homomorphic Game Encoding condition), and call $H$ satisfying the weakened version of Theorem 7 a weakly computationally-homomorphic family. Then, $I^P$ itself is a weakly computationally-homomorphic family, by Sprague-Grundy Theory and the fact that $I^P$ is closed under the disjunctive sum.

Indeed, if a ruleset in $I^P$ is PSPACE-complete and allows a simple way to express the sum of two positions as a single position, then the ruleset is a weakly computationally-homomorphic family. One of the most basic examples of this is Node Kayles. Here, two positions can be trivially summed into a single game by simply taking the two graphs and making them a single (disconnected) graph.

This is a very common property for combinatorial games to have. However, many impartial games with this property aren’t known to be intractable. As an example, Cram is a game that is simply played by placing 2x1 dominoes in either horizontal or vertical orientation on unoccupied tiles of a 2-dimensional grid. Two Cram positions can be added together by surrounding each with a boundary of dominoes, then concatenating the two boards together. Unfortunately, it is not currently known whether Cram is intractable.

Related to the question we asked in Section 5.1, we are curious to know:

Given a pair of Node Kayles positions $G_1$ and $G_2$, can we construct, in polynomial time, a prime Node Kayles position satisfying nimber$(G) = \text{nimber}(G_1) \oplus \text{nimber}(G_2)$?

5.3 Beyond $I^P$

More generally,

Are there analog extensions of our results to polynomially-short partizan games?

Is there a characterization of Sprague-Grundy completeness for $I^P$?

Does the family of PSPACE-solvable impartial games have a natural Sprague-Grundy-complete ruleset?

Does the family of all impartial games have a natural Sprague-Grundy-complete ruleset?

What is the complexity of Graph Nim with an exponential number of stones?

For these last few questions, we may need to go beyond PSPACE as well as polynomially-short games to unlock the nimber secrets.
5.4 Finally

Is there a Bouton analog – i.e., a more clean and direct graph operator – to compute a Generalized Geography game $G$ from two Generalized Geography games $G_1$ and $G_2$ such that $\text{nimber}(G) = \text{nimber}(G_1) \oplus \text{nimber}(G_2)$?

References


