A Calculational Presentation of The Theory of Impartial Two-Person Games

Roland Backhouse*
Diethard Michaelis†

November 4, 2004

Abstract

We develop the theory of two-person impartial games in a calculational style making clear and precise all the logical principles involved.

1 Introduction

The modern world is critically dependent on the reliable functioning of computer software. The sheer scale of software systems makes their design and implementation a highly demanding intellectual activity. The level of rigour, accuracy and effectiveness required in reasoning about software is unprecedented, even when compared with reasoning in mathematics.

Computing scientists have responded to this challenge by developing novel reasoning techniques for designing efficient computer algorithms. These *correct-by-construction* techniques emphasise the *process* of algorithm design, rather than the result. That is, they are about the problem-solving skills that are used in extracting, from an initial, informal, set of requirements, a formal program specification, which is then transformed by a series of design steps to a working, provably correct implementation of the specification. Reliability of the process is ensured by emphasising *calculational* skills.

Teaching this new style of doing mathematics poses massive challenges in modern "fast-food" societies. Students who are weaned on software tools designed to hide the complexities of computation find it difficult to appreciate the immense intellectual demands of developing new software. Curricula and assessment methods often focus on

*School of Computer Science and Information Technology, University of Nottingham, Nottingham NG8 1BB, England
†Beethovenstr. 55, 90513 Zirndorf, Germany

acquisition and repetition of knowledge, rather than the creative skills of constructive reasoning. Problem-solving skills are rarely taught explicitly; too often, they are not taught at all. And, mathematics is often seen as too abstract and irrelevant.

In recent years, we have been studying combinatorial game theory with the goal of using it to teach what we call "algorithmic problem solving". Our aim is to use simple, easily understood, games to develop students' skills in analysing problems, formulating them mathematically, and developing efficient algorithms for their solution. Game theory fits well because, at its core, it is very algorithmic in nature. After all, playing games is about winning — finding strategies that guarantee success and can be successfully applied in possibly adverse circumstances. Also, it is easy to find examples of games that are easy to describe yet challenging to analyse. Last but not least, motivation is for free!

In this paper, we present a calculational formulation of the Sprague-Grundy theory of two-person, impartial games [GS56]. Although the theory is well-known, our presentation is radically different from the standard [BCG82, Con76] in that we develop the theory from first principles, focussing on how the specification of the so-called "mex" number of a game arises from an algorithmic specification of a winning strategy, and how the definition of the "sum" of two mex numbers (originally due to Bouton [Bou02]) is derived. Standard presentations of the theory simply state the definitions *out of the blue* giving students the impression that mathematics is the stuff of geniuses and beyond their own abilities.

For us, as newcomers to game theory, it has been a delight to discover just how many mathematical skills the Sprague-Grundy theory demonstrates. At the heart of reasoning about impartial games is the use of mathematical induction (because a fundamental assumption is that all games are guaranteed to terminate) and the predicate calculus. The notion of an equivalence relation also plays a fundamental role, as does the notion of a congruence relation. Most surprisingly, the theorem that every vector space has a basis turns out to be the key to constructing a definition of mex sum. It can truly be said that the Sprague-Grundy theory provides a very convincing example of the effectiveness of mathematical analysis — provided it is presented in a way that gives students the skills and confidence to create their own mathematical theories.

Although the goal of this paper is to contribute to the teaching of algorithmic problem solving, it is not written in a textbook style suitable for presentation to students as is. The paper provides a basis for teaching material, but does not include (concrete) examples or exercises , or the prose that we would deem necessary in a set of lecture notes or textbook. The reader is referred to the first author's lecture notes on "Algorithmic Problem Solving" (see `http://www.cs.nott.ac.uk/~rcb/G5AAPS.html`) for an illustration of how some of the material is currently presented to first-year undergraduates.

Section 2 begins the discussion by formalising the notion of an impartial game in terms of an induction principle for reasoning about winning and losing positions. This is followed, in section 3, by the introduction of the notion of "summing" games. The section is about analysing the properties of game summation, leading to the identification of an equivalence relation on games. An important element in this section is the construction of winning strategies by maintaining a "strategy invariant". The invariants are not difficult to identify, so that motivating the importance of invariants in algorithm design is facilitated.

Section 4 introduces the "mex" number of a game. It is here that our presentation is most radically different from standard presentations. We derive a specification of the mex function by analysing the specification of an algorithm that guarantees winning an impartial game. Basic principles of algorithm design —reasoning about nondeterministic conditional statements, and the use of invariant properties in loop design— are employed in this analysis. By deriving the specification in this way, we believe that it provides a convincing and enduring example of the effectiveness of good algorithm-design principles.

The notion of "mex" number is taken further in section 5. Here, we construct the definition of mex sum. The key to the construction is that mex numbers form a vector space; constructing the definition of mex sum thus amounts to constructing a basis of the vector space. In this section, insights gained in the calculational method come to the fore. Specifically, a careful choice of notation facilitates the exploitation of the algebraic properties of mex sum, with considerable improvement in the effectiveness of the calculations.

Throughout the paper we use notational conventions of the so-called "calculational method". These have been developed in the context of correct-by-construction algorithm design, and are distinguished from traditional mathematical notation by three characteristics.

- Exploitation of the associativity of boolean equality [DS90]. As we shall see, this is particularly relevant in the context of impartial games.

- The use of a single, uniform notation for quantified expressions. Mathematical notation is very unsystematic in this respect. See [GS93, Bac03] for further discussion.

- The use of a systematic notation (due to Wim Feijen) for presenting calculations, emphasising the inclusion of "hints" accompanying calculation steps. This style of presenting calculations is becoming widespread among computing scientists.

For those unfamiliar with the calculational method, we strongly recommend Van Gasteren's [vG90] proposals for radically improving the clarity and effectiveness of mathematical arguments. Some discussion of the benefits of the calculational method, in the context of this paper, is included in the concluding section.

2 Winning and Losing

We consider impartial, two-person games with complete information — *impartial games* for short. A game is specified by a set of *positions* and a set of *moves* from one position to another, the rules for deciding what is a valid move being fixed in advance. The two players take it in turn to make a move. The game *ends* when it is no longer possible to make a move; the player whose turn it is to move is the *loser*, and the other player is the *winner*. (This is the so-called *normal-play* rule.) We assume, in addition, that, starting from any position, a sequence of moves is always finite. In other words, any play is guaranteed to end no matter how the players choose their moves.

"Impartial" means that rules for moving apply equally to both players. (Chess, for example, is not impartial, because white can only move white pieces, and black can only move black pieces.) "Complete information" means that both players know the complete state of the game. In contrast, in card games like poker, it is usual that each player does not know the cards held by the other player; the players have incomplete information about the state of the game.

Formally, an impartial game is completely defined by a relation on positions, called the *move relation*. We denote the move relation by an infix arrow ("$\mapsto$"). Occasionally, when we apply point-free reasoning to the move relation, we denote it by M.

A *play* is a sequence of positions, each connected to the next by the move relation. The assumption that every play is finite means that a play is given by a number n and a sequence G_0, G_1, ..., G_n such that, for all i, $0 \le i < n$, $G_i \mapsto G_{i+1}$. The *length* of the play is n. (The length of the play is the number of moves.) A *complete play* is a play G_0, G_1, ..., G_n such that there are no moves from G_n, the last position in the sequence.

A player beginning in position G_0 wins the complete play G_0, G_1, ..., G_n if n is odd; vice-versa, the player loses if n is even. A player can guarantee to win, starting from position G, if they have a *winning strategy* — a method of choosing moves that forces every complete play beginning with G to have odd length. Conversely, a player will inevitably lose from position G if there is a strategy that guarantees that every complete play beginning at G has even length. More formally, a *winning strategy* for a player beginning in position G is given by a subset of the move relation — the choice of moves made by the winning player. Let the subset be S and let us call the play G_0, G_1, ..., G_n an S-*play* if every move of the form $G_{2j} \mapsto G_{2j+1}$, for some j, is a move in S. That is, every alternate move, beginning with the first, is a move in S. Then, S must have the following property in order to be a winning strategy for a player beginning in the position G:

(1) Every complete S-play beginning with G has odd length.

A requirement on winning strategies, which is useful for reasoning about them, is that they contain only moves "relevant" to winning. Formally, in addition to (1), we require that:

(2) If $H \mapsto K$ is a move in S, then $G \mapsto^* H$.

If G is a position such that there is a winning strategy for a player beginning in position G, we call G a *winning position*.

A position G is a *losing position* if, starting from G, losing is inevitable against a perfect player. That is, G is a losing position if it is an end position (i.e. there are no moves from G, and so all plays beginning in G have zero length) or there are moves from G, but every such move is to a position H from which the opponent can guarantee that all complete plays have odd length. Such positions H are, by definition, winning positions.

We can extract from this semi-formal account of winning strategies a characterisation of winning and losing positions that forms the basis of formal reasoning about combinatorial games. Let us denote the predicate "winning" by W, and the predicate "losing" by L. Then, as we have just argued,

(3) $L.G \;\equiv\; \langle \forall H : G \mapsto H : W.H \rangle$.

(Formally, we have

$$
\begin{array}{ll}
 & L.G \\
= & \quad \{ \quad \text{informal account above} \quad \} \\
 & \neg \langle \exists H :: G \mapsto H \rangle \;\vee\; (\langle \exists H :: G \mapsto H \rangle \;\wedge\; \langle \forall H : G \mapsto H : W.H \rangle) \\
= & \quad \{ \quad \text{De Morgan and absorption} \quad \} \\
 & \langle \forall H : G \mapsto H : \mathsf{false} \rangle \;\vee\; \langle \forall H : G \mapsto H : W.H \rangle \\
= & \quad \{ \quad \text{golden rule} \quad \} \\
 & \langle \forall H : G \mapsto H : \mathsf{false} \rangle \;\equiv\; \langle \forall H : G \mapsto H : W.H \rangle \;\equiv\; \langle \forall H : G \mapsto H : \mathsf{false} \rangle \wedge \langle \forall H : G \mapsto H : W.H \rangle \\
= & \quad \{ \quad \text{associativity and symmetry of conjunction} \quad \} \\
 & \langle \forall H : G \mapsto H : \mathsf{false} \rangle \;\equiv\; \langle \forall H : G \mapsto H : W.H \rangle \;\equiv\; \langle \forall H : G \mapsto H : \mathsf{false} \wedge W.H \rangle \\
= & \quad \{ \quad \text{calculus} \quad \} \\
 & \langle \forall H : G \mapsto H : W.H \rangle \quad .)
\end{array}
$$

An equation similar to (3) can be derived for W. First, we have:

(4) $W.G \;\Rightarrow\; \langle \exists H : G \mapsto H : L.H \rangle$.

This is established as follows. Assume $W.G$, and let S be a winning strategy for plays beginning in position G. Then, G satisfies property (1). It follows that a position H exists such that $G{\mapsto}H$ is a move in S. This is because every S-play beginning at G has length at least one. It also follows that either there are no moves from H, or for every K such that there is a move $H{\mapsto}K$, every complete S-play beginning in K has odd length. That is, H is a losing position.

We also have:

$$(5) \qquad W.G \;\Leftarrow\; \langle \exists H : G{\mapsto}H : L.H \rangle \quad .$$

To prove this, we prove the equivalent:

$$\langle \forall H : L.H \wedge G{\mapsto}H : W.G \rangle \quad .$$

Suppose $L.H$ and $G{\mapsto}H$. By (3), $\langle \forall K : H{\mapsto}K : W.K \rangle$. Suppose $H{\mapsto}K$ and suppose $S.K$ is a winning strategy for plays beginning in position K. Define S by

$$(6) \qquad S \;=\; \langle \cup K : H{\mapsto}K : S.K \rangle \cup \{G{\mapsto}H\} \quad .$$

We claim that S is a winning strategy for plays beginning in position G. That is, it satisfies the properties (1) and (2). First, we check property (2) for each move in S. This we do in two parts, corresponding to the left and right arguments of the set union in the definition of S. For the left argument, we have that, for all K such that $H{\mapsto}K$ and for all moves $J{\mapsto}L$ in $S.K$, $K \mapsto^{+} J$; but, $G \mapsto^{+} K$; so, $G \mapsto^{+} J$. For the right argument, we have $G \mapsto^{*} G$ (because $\mapsto^{*}$ is reflexive). Second, property (1) is satisfied, because every S-play begins with the move $G{\mapsto}H$ — S cannot contain any other move from G; otherwise, on account of (2), $G \mapsto^{+} G$ contradicting the well-foundedness of the move relation— and, for all K such that $G{\mapsto}H{\mapsto}K$, all complete $S.K$-plays have odd length. Thus, all complete S-plays have odd length too.

Combining (4) and (5), we have that

$$(7) \qquad W.G \;\equiv\; \langle \exists H : G{\mapsto}H : L.H \rangle \quad .$$

(A proof by mutual implication is unavoidable because, for the "if" part, it is necessary to construct the winning strategy. It is interesting to note that the assumption of well-foundedness of the move relation permeates all aspects of the above. Without the assumption, it seems to be much more difficult to establish (5). In particular, the definition of S in (6) does not necessarily give a winning strategy; it is not enough to move to a losing position in order to guarantee a win. A concrete example is given by the "lollipop game" in [BM04].)

Combining (7) with (3), we have that L satisfies the equation

$$(8) \qquad X:: \qquad \langle \forall G \;::\; X.G \;\equiv\; \langle \forall H : G{\mapsto}H : \langle \exists K : H{\mapsto}K : X.K \rangle\rangle\rangle \quad .$$

We recognise this as a fixed-point equation. In point-free predicate-transformer algebra, denoting the move relation by M (rather than $\mapsto$) for greater clarity, (8) is rewritten as

$$(9) \qquad X:: \qquad X = (\mathcal{All}.M \circ \mathcal{Some}.M).X$$

where X ranges over predicates on game positions, the predicate transformer $\mathcal{All}.M$ is defined by, for all predicates X and all positions G,

$$\mathcal{All}.M.X.G \equiv \langle \forall H : G\,M\,H : X.H \rangle \quad ,$$

and the predicate transformer $\mathcal{Some}.M$ is defined by

$$\mathcal{Some}.M.X.G \equiv \langle \exists H : G\,M\,H : X.H \rangle \quad .$$

The assumption that the move relation is well-founded has the important consequence that equation (9) (equivalently, (8)) has a unique solution.

In order to prove this fact, we use the following induction principle: for all predicates p on positions G of the game,

$$(10) \qquad \langle \forall G :: p.G \rangle \quad \equiv \quad \langle \forall G :: p.G \Leftarrow \langle \forall H : G \mapsto H : p.H \rangle \rangle \quad .$$

In words, p holds of all positions G equivales , for all positions G, $p.G$ follows from the induction hypothesis $\langle \forall H : G \mapsto H : p.H \rangle$.

In fact, we use a point-free formulation of the induction principle. (We use the pointwise formulation later.) Specifically, we use the fact that, if relation R on positions is well-founded then, for all predicates p on positions G of the game,

$$(11) \qquad [p] \quad \equiv \quad [p \Leftarrow \mathcal{All}.R.p] \quad .$$

The following theorem embodies the induction principle in a way that is more directly relevant to the goal of winning.

Theorem 12 (Winning Principle) A player starting in position G is guaranteed to lose if the opponent can determine a predicate P on positions such that G satisfies P and, for every position H satisfying P, every move $H \mapsto K$ can be answered by a move $K \mapsto J$ re-establishing P.

Formally, a predicate P is called a *strategy invariant* if

$$[P \Rightarrow (\mathcal{All}.M \circ \mathcal{Some}.M).P] \quad .$$

If P is a strategy invariant, and G satisfies P, then G is a losing position.

Conversely, a player starting in position G is guaranteed to win if there is a move from G to a position satisfying such a predicate P.

□

Theorem 12 is an immediate consequence of the following lemma. (Note that L is an instance of the dummy Q in the lemma.)

Lemma 13 Suppose P is a strategy invariant and Q satisfies the equation (9). Then $[\mathsf{P} \Rightarrow \mathsf{Q}]$.

Proof Motivated by the two occurrences of M in the equation, we use induction on the relation $\mathsf{M}\bullet\mathsf{M}$. ($\mathsf{M}\bullet\mathsf{M}$ is a subset of M^+ and so is well-founded.)

$$
\begin{array}{ll}
 & [\mathsf{P} \Rightarrow \mathsf{Q}] \\
\Leftarrow & \{ \quad \text{induction on } \mathsf{M}\bullet\mathsf{M}\text{, with induction hypothesis } \mathsf{P} \Rightarrow \mathsf{Q}\,. \quad \} \\
 & [(\mathsf{P} \Rightarrow \mathsf{Q}) \;\Leftarrow\; \mathcal{A}ll.(\mathsf{M}\bullet\mathsf{M}).(\mathsf{P} \Rightarrow \mathsf{Q})] \\
= & \{ \quad \text{predicate calculus} \quad \} \\
 & [\mathsf{Q} \;\Leftarrow\; \mathcal{A}ll.(\mathsf{M}\bullet\mathsf{M}).(\mathsf{P} \Rightarrow \mathsf{Q}) \wedge \mathsf{P}] \quad .
\end{array}
$$

The proof now continues with just the right side:

$$
\begin{array}{ll}
 & \mathcal{A}ll.(\mathsf{M}\bullet\mathsf{M}).(\mathsf{P} \Rightarrow \mathsf{Q}) \;\wedge\; \mathsf{P} \\
\Rightarrow & \{ \quad \text{assumption:} \quad \mathsf{P} \text{ is a strategy invariant,} \\
 & \quad\;\; \text{i.e.} \quad [\mathsf{P} \;\Rightarrow\; (\mathcal{A}ll.\mathsf{M} \circ \mathcal{S}ome.\mathsf{M})\,.\,\mathsf{P}] \quad \} \\
 & \mathcal{A}ll.(\mathsf{M}\bullet\mathsf{M}).(\mathsf{P} \Rightarrow \mathsf{Q}) \;\wedge\; (\mathcal{A}ll.\mathsf{M} \circ \mathcal{S}ome.\mathsf{M}).\mathsf{P} \\
= & \{ \quad \text{rewriting in order to identify common factor } \mathcal{A}ll.\mathsf{M} \\
 & \quad\;\; \text{specifically, } [\mathcal{A}ll.(\mathsf{M}\bullet\mathsf{N})\,.\,r \;\equiv\; (\mathcal{A}ll.\mathsf{N} \circ \mathcal{A}ll.\mathsf{M})\,.\,r] \quad \} \\
 & (\mathcal{A}ll.\mathsf{M} \circ \mathcal{A}ll.\mathsf{M})\,.\,(\mathsf{P} \Rightarrow \mathsf{Q}) \;\wedge\; (\mathcal{A}ll.\mathsf{M} \circ \mathcal{S}ome.\mathsf{M})\,.\,\mathsf{P} \\
= & \{ \quad \mathcal{A}ll.\mathsf{M} \text{ distributes through conjunction} \quad \} \\
 & \mathcal{A}ll.\mathsf{M}\,.\,(\mathcal{A}ll.\mathsf{M}.(\mathsf{P} \Rightarrow \mathsf{Q}) \;\wedge\; \mathcal{S}ome.\mathsf{M}.\mathsf{P}) \\
\Rightarrow & \{ \quad \text{calculus} \quad \} \\
 & \mathcal{A}ll.\mathsf{M}\,.\,(\mathcal{S}ome.\mathsf{M}.((\mathsf{P} \Rightarrow \mathsf{Q}) \wedge \mathsf{P})) \\
\Rightarrow & \{ \quad \text{calculus} \quad \} \\
 & \mathcal{A}ll.\mathsf{M}\,.\,(\mathcal{S}ome.\mathsf{M}.\mathsf{Q}) \\
= & \{ \quad \text{assumption:} \quad \mathsf{Q} \text{ satisfies (9)} \quad \} \\
 & \mathsf{Q} \quad .
\end{array}
$$

□

Corollary 14 $[L \equiv \neg W]$.

Proof Clearly, any solution of (9) is also a strategy invariant. So, of course, L is a strategy invariant. Also, by De Morgan's rule, $\neg W$ satisfies (9), and so is a strategy invariant. Applying lemma 13 twice, once with L as the strategy invariant, and once with $\neg W$ as the strategy invariant, we get $[L \Rightarrow \neg W]$ and $[\neg W \Rightarrow L]$. That is, $[L \equiv \neg W]$.
□

In programming terms, the requirement on P in theorem 12 is that, starting from a position G satisfying P, the assertions made in the following program segment are valid; in particular, P is an invariant of the loop body.

```
{       P.G   }
do  ⟨□H
          :   G↦H
          :   G:=H  ;
              {  ⟨∃H :: G↦H ∧ P.H⟩   }
              if ⟨□H : G↦H ∧ P.H : G:=H⟩ fi
              {   P.G   }
    ⟩
od  .
```

In the program segment, the variable G is the current position in the game. The assumption is that, initially, G satisfies P. Executing the loop body is predicated on the existence of a position H such that $G \mapsto H$; if this is the case, a non-deterministic choice of such a position is made, and G is re-assigned to it. This first step represents the fact that the losing player is allowed to make an arbitrary move, if one exists. The requirement on P is that, after this move, there is always a choice of move from the current position to a new position that re-establishes P. That is, the winning strategy must guarantee that

```
{  ⟨∃H :: G↦H⟩  ∧  P.G   }
if ⟨□H : G↦H : G:=H⟩ fi
{  ⟨∃H :: G↦H ∧ P.H⟩   }  .
```

If so, that $P.G$ is an invariant of the loop body is automatically satisfied.

Termination is guaranteed because the move relation is assumed to be well-founded (that is, no infinite sequences of moves are possible). Termination occurs after an even number of moves, and, so, the game ends in a loss for the first player. Briefly, the winning strategy is to choose moves that maintain the invariance of P on the opponent's turn to move.

Many simple games illustrate the principle. For example, the game in which 1 thru M matches may be removed from a single pile of matches at each move is won by maintaining invariant: the number of matches is a multiple of $M{+}1$. In other games, P expresses some form of symmetry. We see how this is used in a general way in section 4.

3 "Summing" Games

A central notion in combinatorial game theory is the "sum" of a finite number of games. The notion arose as a way of breaking a complex game down into more manageable components. (See Conway's remarks on "Go" endgames [Con76].) Conversely, it is a way of composing different games to form a more complicated game. Indeed, the famous game of Nim is quite difficult to win —for anyone not conversant with the theory— but is, in fact, just the "sum" of three copies of a game that is so trivial it would not be called a "game" by the lay public.

Mathematically, the notion of "summing" games is very important because it is the basis of an equivalence relation on game positions. Analysis of the equivalence classes gives an effective way of determining winning strategies.

In this section, various properties of game sum are derived, leading up to the definition of a relation on games (20), and theorem 21, which establishes that it is an equivalence relation.

A *sum of games* consists of two *component games*. A *sum position* is a pair of component positions taken from each of the component games. Moving in a sum of games consists of choosing one component of the sum position, and moving in that component, the other component being left unchanged. The sum of positions is denoted by an infix "$+$" and is postulated to be associative and symmetric. Formally, the move relation is defined by, for all positions G , H , J and K ,

(15) $\quad G{+}H \mapsto J{+}K \;\equiv\; (G{\mapsto}J \wedge H{=}K) \vee (G{=}J \wedge H{\mapsto}K)$.

(Note that "$+$" has precedence over "$\mapsto$".) We do not distinguish between the three move relations in this definition as there is no danger of confusion. This is because, when referring to a position, it must be made clear what the move relation pertaining to that position is. For example, a single pile of matches does not define a position; we also have to state the rule for taking matches away. It is the combination of the state and the allowed moves that defines a position.

To illustrate "summing" positions, suppose a position in one game is a pile of matches, from which a move is to remove 1 thru M matches, and suppose a position in another game is a pile of matches, from which a move is to remove 1 thru N matches. Then, a position in the sum game is two piles of matches, from which a move is to either remove 1 thru M matches from the left pile, or remove 1 thru N matches from the right pile.

We are dealing with well-founded relations here, so we are obliged to show that the sum of two games is well-founded equivales both of the component games are well-founded. It is obvious that both components of a well-founded sum game are well-founded. For the converse, we have to show that the move relation on a sum of well-founded games admits an induction rule. Such a rule is derived as follows. For an arbitrary predicate p, we have:

$$\begin{array}{ll}
 & \langle\forall G,H :: p.(G+H)\rangle \\
= & \{\quad \text{nesting} \quad\} \\
 & \langle\forall H :: \langle\forall G :: p.(G+H)\rangle\rangle \\
= & \{\quad \text{induction on moves in the left summand:} \\
 & \qquad \text{specifically, (10) with } p := \langle G :: p.(G+H)\rangle \quad\} \\
 & \langle\forall H :: \langle\forall G :: p.(G+H) \Leftarrow \langle\forall K : G\mapsto K : p.(K+H)\rangle\rangle\rangle \\
= & \{\quad \text{nesting} \quad\} \\
 & \langle\forall G :: \langle\forall H :: p.(G+H) \Leftarrow \langle\forall K : G\mapsto K : p.(K+H)\rangle\rangle\rangle \\
= & \{\quad \text{induction again, this time on moves in the} \\
 & \qquad \text{right summand, noting that the proof requirement} \\
 & \qquad \text{has the form } \langle\forall H :: q.H\rangle \quad\} \\
 & \langle\forall G :: \\
 & \qquad \langle\forall H :: \\
 & \qquad\qquad\qquad (p.(G+H) \Leftarrow \langle\forall K : G\mapsto K : p.(K+H)\rangle) \\
 & \qquad\qquad \Leftarrow \quad \langle\forall L : H\mapsto L : p.(G+L) \Leftarrow \langle\forall K : G\mapsto K : p.(K+L)\rangle\rangle \\
 & \qquad \rangle \\
 & \rangle \\
\Leftarrow & \{\quad \text{calculus} \quad\} \\
 & \langle\forall G,H :: p.(G+H) \Leftarrow \langle\forall K : G\mapsto K : p.(K+H)\rangle \wedge \langle\forall L : H\mapsto L : p.(G+L)\rangle\rangle \\
\Leftarrow & \{\quad \text{definition of move from a sum of positions: (15)} \quad\} \\
 & \langle\forall G,H :: p.(G+H) \Leftarrow \langle\forall J : G+H \mapsto J : p.J\rangle\rangle \quad .
\end{array}$$

That is, the move relation on the sum of two games admits induction. It follows (by induction on the number of games) that the sum of any finite number of games admits induction.

A simple observation is that a position of the form $G{+}G$ is a losing position — because any move played in one component can always be copied by the opponent in the other component.

Lemma 16

$$L.(G{+}G) \quad .$$

Proof We use the winning principle of theorem 12. For the strategy invariant, define

$$P.(G{+}H) \;\equiv\; G = H \quad .$$

We thus have to show that, for any G,

$$\langle \forall H \,:\, G{\mapsto}H \,:\, \langle \exists K :: G{+}H \mapsto K{+}K \vee H{+}G \mapsto K{+}K \rangle\rangle \quad .$$

This clearly follows by choosing H for the value of K in the existential quantification.
□

A sketch of how to implement the winning strategy in lemma 16 is shown below.

$\{\quad \langle \exists H : G = H{+}H : \langle \exists K :: H{\mapsto}K \rangle\rangle \quad \}$

if $\quad \langle \Box\, H,K$

$\qquad\qquad : \quad G = H{+}H \wedge H{\mapsto}K$

$\qquad\qquad : \qquad G\,,\mathit{left}\,,h\,,k := K{+}H\,,\mathrm{true}\,,H\,,K$

$\qquad\qquad\quad \Box \quad G\,,\mathit{left}\,,h\,,k := H{+}K\,,\mathrm{false}\,,H\,,K$

$\quad \rangle$

fi

$\{\quad h{\mapsto}k \;\wedge\; ((\mathit{left} \wedge G = k{+}h) \vee (\neg\mathit{left} \wedge G = h{+}k)) \quad \}$

$\{\quad G \mapsto k{+}k \quad \}$

The conditional statement models the loser's choice of an arbitrary move; at the same time, it uses the local variables left, h and k to determine the winning strategy. The variable left records in which component the loser makes a move. The variables h and k record the move that is made. The response is then to move in the opposite component, so that, after execution of the loop body the position is $k{+}k$.

Another simple observation is that a position of the form $G{+}H$, where G and H are losing positions, is a losing position — because any move played in one component always offers the opponent a winning move in the same component.

Lemma 17 For all G , H ,

$$\mathsf{L}.(\mathsf{G}+\mathsf{H}) \;\Leftarrow\; \mathsf{L}.\mathsf{G} \wedge \mathsf{L}.\mathsf{H} \quad .$$

Equivalently, for all G , H ,

$$\mathsf{W}.(\mathsf{G}+\mathsf{H}) \;\Rightarrow\; \mathsf{W}.\mathsf{G} \vee \mathsf{W}.\mathsf{H} \quad .$$

(The equivalence of the two statements is obvious from (14). In this lemma, and in several that follow, we rephrase a property of losing/winning in terms of a property of winning/losing, using (14). This is useful in calculations, as well as postponing the decision on which of winning or losing one should focus.)

Proof Again, we use the winning principle of theorem 12. For the strategy invariant, define

$$\mathsf{P}.(\mathsf{G}+\mathsf{H}) \;\equiv\; \mathsf{L}.\mathsf{G} \wedge \mathsf{L}.\mathsf{H} \quad .$$

We have to show that

$$\langle \forall \mathsf{X},\mathsf{Y} \;:\; \mathsf{G}+\mathsf{H} \mapsto \mathsf{X}+\mathsf{Y} \;:\; \langle \exists\, \mathsf{J},\mathsf{K} : \mathsf{X}+\mathsf{Y} \mapsto \mathsf{J}+\mathsf{K} : \mathsf{L}.\mathsf{J} \wedge \mathsf{L}.\mathsf{K} \rangle\rangle \quad .$$

The proof is as follows:

$$\begin{array}{cl}
 & \mathsf{G}+\mathsf{H} \mapsto \mathsf{X}+\mathsf{Y} \\
= & \{ \quad \text{definition of a move in a sum game} \quad \} \\
 & (\mathsf{G}\mapsto\mathsf{X} \wedge \mathsf{H}=\mathsf{Y}) \vee (\mathsf{G}=\mathsf{X} \wedge \mathsf{H}\mapsto\mathsf{Y}) \\
\Rightarrow & \{ \quad \text{assumption: } \mathsf{L}.\mathsf{G} \wedge \mathsf{L}.\mathsf{H}, \quad (3) \quad \} \\
 & (\mathsf{W}.\mathsf{X} \wedge \mathsf{H}=\mathsf{Y}) \vee (\mathsf{G}=\mathsf{X} \wedge \mathsf{W}.\mathsf{Y}) \\
= & \{ \quad (7) \quad \} \\
 & (\langle \exists \mathsf{J} : \mathsf{X}\mapsto\mathsf{J} : \mathsf{L}.\mathsf{J} \rangle \wedge \mathsf{H}=\mathsf{Y}) \vee (\mathsf{G}=\mathsf{X} \wedge \langle \exists \mathsf{K} : \mathsf{Y}\mapsto\mathsf{K} : \mathsf{L}.\mathsf{K} \rangle) \\
\Rightarrow & \{ \quad \text{first disjunct, } \mathsf{K}:=\mathsf{H}, \\
 & \quad\;\; \text{second disjunct, } \mathsf{J}:=\mathsf{G} \quad \} \\
 & \langle \exists\, \mathsf{J},\mathsf{K} : \mathsf{X}+\mathsf{Y} \mapsto \mathsf{J}+\mathsf{K} : \mathsf{L}.\mathsf{J} \wedge \mathsf{L}.\mathsf{K} \rangle \quad .
\end{array}$$

□

Lemma 17 suggests another property: G+H is a winning position if $\mathsf{W}.\mathsf{G} \not\equiv \mathsf{W}.\mathsf{H}$. The strategy is to choose a winning move in the winning component in order to reach a position in which both components are losing positions. The formal proof follows.

Lemma 18 For all positions G and H,

$$W.(G+H) \Leftarrow (W.G \not\equiv W.H) \quad .$$

Equivalently, for all G and H,

$$W.(G+H) \vee W.G \;\equiv\; W.(G+H) \vee W.H \quad ,$$

$$L.(G+H) \Rightarrow (L.G \equiv L.H) \quad ,$$

$$L.(G+H) \wedge L.G \;\equiv\; L.(G+H) \wedge L.H \quad .$$

Proof We have:

$$\begin{array}{ll}
 & W.(G+H) \\
\Leftarrow & \{ \quad (7) \text{ and definition of move relation } (15) \quad \} \\
 & \langle \exists G' : G \mapsto G' : L.(G'+H) \rangle \\
\Leftarrow & \{ \quad \text{calculus and lemma 17} \quad \} \\
 & \langle \exists G' : G \mapsto G' : L.G' \wedge L.H \rangle \\
= & \{ \quad \text{distributivity of } \wedge \text{ over } \vee \quad \} \\
 & \langle \exists G' : G \mapsto G' : L.G' \rangle \;\wedge\; L.H \\
= & \{ \quad (7) \quad \} \\
 & W.G \wedge L.H \quad .
\end{array}$$

Thus,

$$W.(G+H) \Leftarrow W.G \wedge L.H \quad .$$

Symmetrically,

$$W.(G+H) \Leftarrow L.G \wedge W.H \quad .$$

The lemma is the conjunction of these two properties.
□

Combining lemmas 17 and 18 we get:

Lemma 19 For all positions G and H,

$$L.(G+H) \wedge L.G \;\equiv\; L.G \wedge L.H \quad .$$

Equivalently: for all G and H,

$$(L.(G+H) \;\equiv\; L.H) \Leftarrow L.G \quad ,$$

$$W.(G+H) \vee W.G \;\equiv\; W.G \vee W.H \quad ,$$

$$(W.(G+H) \not\equiv W.H) \Rightarrow W.G \quad .$$

Proof

$$
\begin{array}{ll}
 & \mathsf{L.(G{+}H) \wedge L.G} \\
= & \{ \quad \text{lemma 18, idempotence of } \wedge \quad \} \\
 & \mathsf{L.(G{+}H) \wedge L.G \wedge L.H} \\
= & \{ \quad \text{lemma 17} \quad \} \\
 & \mathsf{L.G \wedge L.H} \quad .
\end{array}
$$

The rest follows from (14) and predicate calculus.
□

The property that $(\mathsf{L.(G{+}H) \equiv L.G}) \Leftarrow \mathsf{L.H}$ can be read informally as a sort of modularity property: modulo winning/losing, adding a losing position H to a position G has no effect. Experience with equivalence/congruence relations strongly suggests defining the relation $\cong$ on positions by, for all G and H,

(20) $\quad \mathsf{G \cong H} \;\equiv\; \mathsf{L.(G{+}H)}$,

and investigating whether it is a congruence relation on positions. Indeed, it is:

Theorem 21 The relation $\cong$ is a congruence relation on positions. (That is, it is an equivalence relation that is preserved by addition.)

Proof Lemma 16 establishes reflexivity of the relation. The symmetry of sum establishes its symmetry. Transitivity is proved as follows:

$$
\begin{array}{ll}
 & \mathsf{G \cong H \;\wedge\; H \cong K} \\
= & \{ \quad \text{definition (20)} \quad \} \\
 & \mathsf{L.(G{+}H) \;\wedge\; L.(H{+}K)} \\
\Rightarrow & \{ \quad (14) \quad \} \\
 & \mathsf{L.(G{+}H{+}H{+}K)} \\
= & \{ \quad \text{lemma 16} \quad \} \\
 & \mathsf{L.(G{+}H{+}H{+}K) \;\wedge\; L.(H{+}H)} \\
= & \{ \quad \text{lemma 19 with } \mathsf{G\,,H := G{+}K\;,\;H{+}H} \\
 & \qquad \text{(and associativity and symmetry of sum)} \quad \} \\
 & \mathsf{L.(G{+}K) \;\wedge\; L.(H{+}H)} \\
= & \{ \quad \text{lemma 16 and definition (20)} \quad \} \\
 & \mathsf{G \cong K} \quad .
\end{array}
$$

The proof that the relation is preserved by addition, i.e. that

$$G \cong H \wedge K \cong J \Rightarrow G{+}K \cong H{+}J \quad ,$$

is a shorter exercise in the use of (20) and (14).
□

We have already remarked that the sum operator is associative and symmetric. This is an important algebraic property that we should endeavour to exploit to the full. In the following lemma, we identify a related algebraic property:

Lemma 22 For all G, H and K, the following four statements are all equivalent:

- $L.(G{+}H{+}K)$
- $G \cong H{+}K$
- $H \cong K{+}G$
- $K \cong G{+}H$

Proof Immediate from (20) and the associativity and symmetry of the sum operator.
□

The import of lemma 22 is that, if we derive a property of the form $L.(G{+}H{+}K)$, we immediately get three equivalences between games "for free". (That is a slight exaggeration. Sometimes such a property is established by deriving, for example, $G \cong H{+}K$. In that case, only two equivalences are "for free".) Giving notational preference to statements of the form $L.(G{+}H{+}K)$, rather than statements of the equivalence between games, leads to a substantial gain in the effectiveness of reasoning about games. So, this is what we do.

A comparison with Dijkstra and Scholten's [DS90] revolutionary formalisation of the predicate calculus is in order. They observe that boolean equality ("equivales") is associative and symmetric, and has unit $true$. In order to exploit the associativity to the full, they define $p \equiv q \equiv r$ to mean $(p \equiv q) \equiv r$, or equally, $p \equiv (q \equiv r)$, rather than $(p \equiv q) \wedge (q \equiv r)$, which is the conventional meaning. They go on to introduce an "everywhere" operator on boolean-valued functions, which they denote by square brackets. In this way, if p and q are bolean-valued functions on some state space, $[p \equiv q]$ is the statement that p and q are equal. Most importantly, a statement of the form $[p \equiv q \equiv r]$ can be read in three different ways: p and $q \equiv r$ are equal, q and $r \equiv p$ are equal, and r and $p \equiv q$ are equal. The calculus of game summation is identical: replace "$\equiv$" in the Dijkstra-Scholten calculus by "$+$" and the square brackets by "L". (Another way of saying this is that the summation of games is a model of Dijkstra and Scholten's axiomatisation of boolean equality.)

4 The MEX Function

In this section, we derive the specification of a function mex on games that satisfies: for all positions G and H,

$$(23) \quad \mathsf{L}.(\mathsf{G}{+}\mathsf{H}) \;\equiv\; mex.\mathsf{G} = mex.\mathsf{H} \quad .$$

The principle for identifying winning and losing positions (see section 2) drives the derivation.

The first step is to consider end positions. Since G+H is an end position of the sum game exactly when G is an end position of the left game and H is an end position of the right game, it is a requirement that the mex value of all end positions is the same.

Second, every allowed move from a losing position —a position G+H satisfying $mex.\mathsf{G} = mex.\mathsf{H}$— , that is not an end position, should result in a winning position —a position G+H satisfying $mex.\mathsf{G} \neq mex.\mathsf{H}$— . That is,

$\{ \quad mex.\mathsf{G} = mex.\mathsf{H} \;\wedge\; (\mathsf{G}$ is not an end position $\vee$ H is not an end position$) \quad \}$

if G is not an end position $\rightarrow$ change G

$\square$ H is not an end position $\rightarrow$ change H

fi

$\{ \quad mex.\mathsf{G} \neq mex.\mathsf{H} \quad \}$.

Third, applying the winning strategy, from a winning position —a position G+H satisfying $mex.\mathsf{G} \neq mex.\mathsf{H}$— should result in a losing position —a position G+H satisfying $mex.\mathsf{G} = mex.\mathsf{H}$—. That is,

$\{ \quad mex.\mathsf{G} \neq mex.\mathsf{H} \quad \}$

apply winning strategy

$\{ \quad mex.\mathsf{G} = mex.\mathsf{H} \quad \}$.

We can satisfy the first and second requirements if we define mex to be a function with range the set of natural numbers, and require that:

- For end positions G and H of the respective games, $mex.\mathsf{G} = mex.\mathsf{H}$.
- For every J such that there is a move from G to J in the left game, $mex.\mathsf{G} \neq mex.\mathsf{J}$. Similarly, for every K such that there is a move from H to K in the right game, $mex.\mathsf{H} \neq mex.\mathsf{K}$.

Note that, at this stage, the choice of the natural numbers as range of the functions is quite arbitrary. The advantage of this choice arises from the third requirement. If m and n are different natural numbers, either $m<n$ or $n<m$. This allows us to refine the process of applying the winning strategy, by choosing to move in the right game when $mex.G<mex.H$ and choosing to move in the left game when $mex.H<mex.G$. (See below.)

$$\{\ \ mex.G \neq mex.H\ \ \}$$
$$\text{if}\ \ mex.G < mex.H \ \to\ \text{change } H$$
$$\square\ \ mex.H < mex.G \ \to\ \text{change } G$$
$$\text{fi}$$
$$\{\ \ mex.G = mex.H\ \ \}\ .$$

For this to work, we require that:

- For any number m less than $mex.H$, it is possible to move from H to a position K such that $mex.K=m$. Similarly, for any number n less than $mex.G$, it must be possible to move from G to a position J such that $mex.J=n$.

In summary, the requirements on the mex function are satisfied by the following definition.

> The mex value of position G, denoted $mex.G$, is a natural number, n, such that
>
> **falsify invariant** For every position H such that $G{\mapsto}H$, $mex.H\neq n$.
>
> **truthify invariant** For every natural number m less than n, there is a move from G to a position H satisfying $mex.H=m$.

The labels refer to the origin of the requirement. The requirement labelled "**falsify invariant**" obliges the losing player to falsify the invariant (that the mex values of the sum components are equal), and requirement labelled "**truthify invariant**" gives the strategy whereby the winning player can win (by truthifying the property that the mex values of the sum components are equal).

An immediate consequence of this definition is that the mex value of end positions is 0 (since **falsify invariant** is vacuously true for end positions, and **truthify invariant** is also true for end positions when m is taken to be 0 — noting that 0 is the smallest natural number).

For positions other than the end positions, it is not immediately obvious that the mex value is well defined. Indeed, it need not be! An additional assumption needs to be introduced, namely that the move relation is finitely branching. That is, for each position G there is a *finite* number of positions H such that $G \mapsto H$. (This property is clearly preserved by game sum.)

(Formally, the need for an additional assumption arises in the proof of (26) below — without the assumption, more care needs to be given to the definition of the minimum operator. In [Con76] , the assumption is not made, and mex numbers may be transfinite.)

For calculational purposes, two characterisations of the mex function are useful. Property (25) expresses most directly the constructive nature of the mex function (the fact that it embodies a winning strategy); consequently, it is most useful for reasoning about the function. Property (26), on the other hand, is used to calculate its value at specific positions.

Lemma 24 For all positions G and all natural numbers m,

(25) $\quad m \leq mex.G \;\equiv\; \langle \forall n : n < m : \langle \exists H : G \mapsto H : n = mex.H \rangle\rangle$.

Equivalently,

(26) $\quad mex.G \;=\; \langle \Downarrow n : \langle \forall H : G \mapsto H : n \neq mex.H \rangle : n \rangle$.

(" $\Downarrow$ " denotes the minimum operator.)

Proof We have:

$$
\begin{array}{ll}
 & m \leq mex.G \\
= & \{ \quad \text{integer inequalities} \quad \} \\
 & \langle \forall n : n < m : n < mex.G \rangle \\
\Rightarrow & \{ \quad \text{requirement } \textbf{truthify invariant} \quad \} \\
 & \langle \forall n : n < m : \langle \exists H : G \mapsto H : n = mex.H \rangle\rangle \\
\Rightarrow & \{ \quad \text{requirement } \textbf{falsify invariant} \quad \} \\
 & \langle \forall n : n < m : \langle \exists H : G \mapsto H : n = mex.H \rangle \wedge n \neq mex.G \rangle \\
\Rightarrow & \{ \quad \text{predicate calculus (weakening a conjunction)} \quad \} \\
 & \langle \forall n : n < m : n \neq mex.G \rangle \\
\Rightarrow & \{ \quad \text{by induction on } m\text{, using that} \\
 & \quad\quad mex.G \text{ is a natural number for the base case} \quad \} \\
 & m \leq mex.G \quad .
\end{array}
$$

This proves (25). Now for (26), we have:

$$\langle\forall n : n<m : \langle\exists H : G\mapsto H : n=mex.H\rangle\rangle$$

$$= \quad \{ \quad \text{inequalities, De Morgan} \quad \}$$

$$\langle\forall n : \neg(m\leq n) : \neg\langle\forall H : G\mapsto H : n\neq mex.H\rangle\rangle$$

$$= \quad \{ \quad \text{trading range and term} \quad \}$$

$$\langle\forall n : \langle\forall H : G\mapsto H : n\neq mex.H\rangle : m\leq n\rangle$$

$$= \quad \{ \quad \text{definition of } \Downarrow \quad \}$$

$$m \leq \langle\Downarrow n : \langle\forall H : G\mapsto H : n\neq mex.H\rangle : n\rangle \quad .$$

Combining the above calculation with (25), we have shown that

$$\langle\forall m :: m\leq mex.G \;\equiv\; m\leq\langle\Downarrow n : \langle\forall H : G\mapsto H : n\neq mex.H\rangle : n\rangle\rangle \quad .$$

Property (26) follows by the rule of indirect equality.
□

As already mentioned, "mex" is short for "minimal excludant". In words, (26) expresses the mex number of a position G as the minimal number that is excluded from the mex numbers of positions H to which a move can be made from G. Mex numbers are also called *Sprague-Grundy numbers* [GS56].

Consider a game in which there is one pile of matches, and a move is to remove some strictly positive number of matches from the pile. Starting from the position in which the pile has m matches, it is possible to leave the opponent with n matches, for any n less than m, but it is not possible to leave the opponent with a pile of m matches. It follows (formally, by induction on m) that this position has mex number m. This is the "canonical" game position with mex number m. Henceforth, we denote it by $^*m$.

The position $^*m$ has the following properties:

- $mex.{}^*m = m$
- For all (natural numbers) n, $^*m\mapsto{}^*n \;\equiv\; m>n$.
- For all (natural numbers) n, $^*m\cong{}^*n \;\equiv\; m=n$.
- For all G, $G\cong{}^*(mex.G)$.

The last two of these are easily verified by applying the winning principle of theorem 12. The first two are by definition of the mex function. We also have:

Lemma 27

$$mex.G=0 \;\equiv\; L.G \quad .$$

Proof Immediate from (23) and $mex.({}^*0)=0$.
□

5 MEX Sum

This section is about deriving an operator $\oplus$ such that, for all positions G and H,

(28) $\quad mex.(G{+}H) \;=\; mex.G \oplus mex.H \quad .$

We call $\oplus$ the *mex sum* operator.

Property (28) gives a clue as to how to define mex sum. Formally, we define the operator $\oplus$ by the equation:

(29) $\quad m{\oplus}n \;=\; mex.({}^*m + {}^*n)$

With this definition, (28) can be established for all positions G and H. First, we need a lemma.

Lemma 30 For all positions G,

$$L.(G + {}^*(m{\oplus}n)) \;\equiv\; L.(G + {}^*m + {}^*n) \quad .$$

Proof

$$
\begin{array}{ll}
 & L.(G + {}^*(m{\oplus}n)) \\
= & \{ \quad (23) \quad \} \\
 & mex.G \;=\; mex\,.{}^*(m{\oplus}n) \\
= & \{ \quad mex.({}^*k) = k,\ (29) \quad \} \\
 & mex.G \;=\; mex.({}^*m + {}^*n) \\
= & \{ \quad (23) \quad \} \\
 & L.(G + {}^*m + {}^*n) \quad .
\end{array}
$$

□

Theorem 31 For all positions G and H,

$$mex.(G{+}H) \;=\; mex.G \oplus mex.H \quad .$$

Proof

$$
\begin{array}{ll}
 & mex.(G{+}H) \;=\; mex.G \oplus mex.H \\
= & \{ \quad (23) \text{ and } mex.({}^*k) = k \ \ (\text{with } k := mex.G \oplus mex.H\,) \quad \} \\
 & L.(G + H + {}^*(mex.G \oplus mex.H)) \\
= & \{ \quad \text{lemma 30} \quad \}
\end{array}
$$

$$L.(G+H+{}^*(mex.G)+{}^*(mex.H))$$

$\Leftarrow$ { lemma 17
(and associativity and symmetry of game sum) }

$$L.(G+{}^*(mex.G)) \wedge L.(H+{}^*(mex.H))$$

$=$ { for all G, $G \cong {}^*(mex.G)$ }

true .

□

Corollary 32 Mex sum is associative and symmetric. It has unit element 0 and satisfies $m \oplus m = 0$ for all m.

Proof Symmetry is obvious from the definition of mex sum, (29), and the fact that game sum is symmetric. It is easy to check that distributivity of mex through position sum (theorem 31) guarantees that mex sum inherits the properties of associativity from position sum. Here is one half of the proof:

$$m \oplus (n \oplus p)$$

$=$ { $m = mex.{}^*m$, definition of mex sum: (29) }

$$mex.{}^*m \oplus mex.({}^*n + {}^*p)$$

$=$ { distributivity: theorem 31 }

$$mex.({}^*m + ({}^*n + {}^*p))$$

$=$ { $+$ is associative }

$$mex.(({}^*m + {}^*n) + {}^*p) \ .$$

The distributivity property combined with $mex\,.{}^*0 = 0$ gives the remaining two properties.

□

Theorem 33 The mex numbers form a vector space over the field with two elements. The number 0 is the zero element of the space.

(There is a unique field with two elements. It is called $GF(2)$ in the mathematical literature. Naming the elements 0 and 1, multiplication is the same as in arithmetic. Addition is "different from". That is, the addition of two equal values is 0 and the addition of two different values is 1. The product of a field element with a mex number is as expected: the product of 0 (the field element) with mex number m is the mex number 0, and the product of the field element 1 with mex number m is the mex number m.)

□

The verification of theorem 33 is very easy, but tedious. (The definition of a vector space has a lot of clauses, each of which is easy to check in this case.) We do not prove it here because we do not apply the theorem. The significance of theorem 33 is that every vector space has a basis; this is the motivation for the discussion that now follows.

Suppose $\mathbf{b}$ is a basis of the mex numbers, indexed by some set I. Then every mex number can be written as

$$\langle \bigoplus i : i \in I : m_i \mathbf{b}_i \rangle$$

where, for each i, m_i is a scalar (thus 0 or 1) and juxtaposition denotes scalar-vector multiplication. Such a representation of vectors facilitates addition because it can be computed "componentwise". That is

$$\langle \bigoplus i : i \in I : m_i \mathbf{b}_i \rangle \;\oplus\; \langle \bigoplus i : i \in I : n_i \mathbf{b}_i \rangle \;\;=\;\; \langle \bigoplus i : i \in I : (m_i \not\equiv n_i) \mathbf{b}_i \rangle \quad .$$

(The symbol "$\not\equiv$" denotes addition in $\mathrm{GF}(2)$. Specifically, $(0 \not\equiv 1) = 1 = (1 \not\equiv 0)$, and $(0 \not\equiv 0) = 0 = (1 \not\equiv 1)$. The choice of symbol anticipates the use of propositional calculus later.) Our problem is to determine a suitable basis for the mex numbers.

The mex numbers can obviously be enumerated in the order of the natural numbers: 0, 1, 2, etc. An inductive method of determining a basis is as follows. The induction hypothesis is that $\mathbf{b}$ is a set of independent vectors indexed by a set of size n. We extend $\mathbf{b}$ by one element by adding to it the first non-zero mex number that is independent of all the elements of $\mathbf{b}$. (It must always be possible to extend $\mathbf{b}$ in this way because there are infinitely many mex numbers. However, the field $\mathrm{GF}(2)$ is finite, which means that a finite number of vectors can span only a finite space.)

In the calculations, we write $[m \oplus n \oplus p]$ to mean $m \oplus n \oplus p = 0$. The reason for this is to take full advantage of the algebraic properties of mex sum: the equivalent properties $m \oplus n = p$, $n \oplus p = m$ and $p \oplus m = n$ all exhibit an unwelcome asymmetry. The replacement of "$=0$" by square brackets is for brevity.

We now begin the process of constructing a basis $\mathbf{b}$, as outlined above. Initially $\mathbf{b}$ is empty. The first extension of $\mathbf{b}$ is to add 1 to it (since every vector is independent of an empty set, and 1 is the first non-zero mex number in our chosen enumeration).

Now, it is easy to determine the space spanned by $\{1\}$; we have

$$[1 \oplus 1 \oplus 0] \quad .$$

from which we immediately deduce that the space spanned is $\{0,1\}$. So, the next number to be added to $\mathbf{b}$ is 2. (This fulfills the requirement that we extend $\{0,1\}$ by one element by adding to it the first non-zero mex number that is independent of all the elements of $\{0,1\}$.) We now consider how to extend $\{0,1,2\}$. The space spanned by this set is $\{0,1,2,1\oplus 2\}$. This means we have to calculate $1\oplus 2$, which by definition is $mex.({}^*1+{}^*2)$.

We calculate the value of $mex.({}^*1+{}^*2)$ using lemma 25:

$$
\begin{array}{ll}
 & mex.({}^*1+{}^*2) \;\geq\; m \\
= & \{ \quad mex.G \geq m \;\equiv\; \langle \forall n : n<m : \langle \exists H : G \mapsto H : n = mex.H \rangle\rangle \quad \} \\
 & \langle \forall n : n<m : \langle \exists H : {}^*1+{}^*2 \mapsto H : n = mex.H \rangle\rangle \\
= & \{ \quad \text{by definition of the move relation for sums,} \\
 & \qquad\quad {}^*1+{}^*2 \mapsto H \\
 & \qquad \equiv \quad {}^*0+{}^*2 = H \vee {}^*1+{}^*1 = H \vee {}^*1+{}^*0 = H \quad \} \\
 & \langle \forall n : n<m : n = mex.({}^*0+{}^*2) \vee n = mex.({}^*1+{}^*1) \vee n = mex.({}^*1+{}^*0) \rangle \\
= & \{ \quad \text{for all } k,\; {}^*0+{}^*k = {}^*k \text{ and } k = mex.({}^*k) \quad \} \\
 & \langle \forall n : n<m : n=2 \vee n=0 \vee n=1 \rangle \\
= & \{ \quad \text{inequalities} \quad \} \\
 & 3 \geq m \quad .
\end{array}
$$

By indirect equality, it follows that $mex.({}^*1+{}^*2)$ equals 3. The space spanned by $\{0,1,2\}$ is thus $\{0,1,2,3\}$, and the next number to be added to the basis is 4. That is, the current value of the basis is $\{1,2,4\}$.

Exercise 34 Generalise the above calculation by showing that, for all m,

$$[1 \oplus 2m \oplus (2m+1)] \quad .$$

□

At this stage, we make a major conjecture. We conjecture that a basis for the vector space of mex numbers is the set of powers of two. This is a reasonable conjecture because the vector space spanned by a set of 2^k elements has at most 2^{k+1} elements when the underlying field has just two elements.

If the conjecture is right, then each mex number is represented in the vector space by its representation as a binary numeral. Let us use the notation m_i for the ith bit in the binary representation of m. That is,

$$m \;=\; \langle \Sigma i :: m_i 2^i \rangle$$

(where " Σ " denotes the normal arithmetic addition of numbers). The conjecture is that

$$m \;=\; \langle \bigoplus i :: m_i 2^i \rangle$$

where $\bigoplus$ is the quantifier corresponding to mex addition. (Here, of course, $m_i 2^i$ denotes the scalar-vector multiplication of the field element m_i and the mex number 2^i.) Also, it means that mex addition is componentwise addition in $\mathsf{GF}(2)$ of the coefficients. That is,

$$m \oplus n \;=\; \langle \bigoplus i :: m_i 2^i \rangle \oplus \langle \bigoplus i :: n_i 2^i \rangle \;=\; \langle \bigoplus i :: (m_i \not\equiv n_i) 2^i \rangle \quad .$$

In order to prove this conjecture, we exploit to the full the algebraic properties of associativity and symmetry. In addition, by observing the isomorphism of $\mathsf{GF}(2)$ with the booleans, where multiplication is conjunction and addition is inequivalence, we are able to exploit the substitution properties of boolean equality.

Specifically, we interpret 0 in $\mathsf{GF}(2)$ as the boolean false and 1 in $\mathsf{GF}(2)$ as the boolean true. The addition $m_i \not\equiv n_i$ of the two binary digits m_i and n_i of the mex numbers m and n is then, indeed, boolean inequality (as anticipated by the notation), and our conjecture becomes that, for all m, n and p,

(35) $\quad [m \oplus n \oplus p] \;\equiv\; \langle \forall i :: m_i \not\equiv n_i \not\equiv p_i \equiv \mathsf{false} \rangle \quad .$

For more effective calculation, we replace the inequivalences by equivalences (using that $a \not\equiv b \not\equiv c$ and $a \equiv b \equiv c$ are equal). (It is always easier to work with equalities than with inequalities! Note that continued boolean equalities should, of course, be read associatively.)

Our proof is by induction on tuples of numbers (m,n,p) ordered by the pointwise extension of the at-most relation on numbers. Formally, the ordering relation $\preceq$ is defined by

$$(m,n,p) \preceq (r,s,t) \;\equiv\; m \leq r \wedge n \leq s \wedge p \leq t \quad .$$

(We do not use the notation, only the fact that the corresponding strict ordering relation $\prec$ admits induction.) The induction hpothesis is

(36) $\quad \neg [m \oplus n \oplus p] \;\equiv\; \langle \exists i :: m_i \equiv n_i \equiv p_i \rangle \quad .$

(Formally, (36) is obtained from (35) using De Morgan's rule and

$$\begin{array}{ll}
 & \neg(m_i \not\equiv n_i \not\equiv p_i \equiv \mathsf{false}) \\
= & \{ \quad \text{definition of negation and inequivalence} \quad \} \\
 & \mathsf{false} \equiv m_i \equiv n_i \equiv p_i \equiv \mathsf{false} \equiv \mathsf{false} \equiv \mathsf{false} \\
= & \{ \quad \text{calculus} \quad \} \\
 & m_i \equiv n_i \equiv p_i \quad .)
\end{array}$$

Note that, by combining the definition of the square brackets with (29), we have:

(37) $\quad [m \oplus n \oplus p] \;\equiv\; L.({}^*m + {}^*n + {}^*p)$.

We use (37) frequently below.

The induction step is to verify (36) assuming it is true for all smaller tuples. We use a ping-pong argument. (A ping-pong argument is probably unavoidable because one direction involves the construction of a winning strategy.)

First,

$$
\begin{array}{ll}
 & \neg\,[m \oplus n \oplus p] \\
= & \{ \quad \text{definition of square brackets, (29)} \quad \} \\
 & \neg L.({}^*m + {}^*n + {}^*p) \\
= & \{ \quad \text{(9) and (7)} \quad \} \\
 & \quad \langle \exists k : k < m : L.({}^*k + {}^*n + {}^*p) \rangle \\
 & \vee \;\; \langle \exists k : k < n : L.({}^*m + {}^*k + {}^*p) \rangle \\
 & \vee \;\; \langle \exists k : k < p : L.({}^*m + {}^*n + {}^*k) \rangle \\
= & \{ \quad L.({}^*k + {}^*n + {}^*p) \;\equiv\; [k \oplus n \oplus p] \\
 & \quad\;\; \text{(and similarly for the other disjuncts),} \\
 & \quad\;\; \text{induction hypothesis} \quad \} \\
 & \quad \langle \exists k : k < m : \neg\,\langle \exists i :: k_i \equiv n_i \equiv p_i \rangle \rangle \\
 & \vee \;\; \langle \exists k : k < n : \neg\,\langle \exists i :: m_i \equiv k_i \equiv p_i \rangle \rangle \\
 & \vee \;\; \langle \exists k : k < p : \neg\,\langle \exists i :: m_i \equiv n_i \equiv k_i \rangle \rangle \\
\Rightarrow & \{ \quad \neg\,\langle \exists i :: k_i \equiv n_i \equiv p_i \rangle \;\equiv\; \langle \forall i :: \neg k_i \equiv n_i \equiv p_i \rangle \\
 & \quad\;\; k < m \;\Rightarrow\; \langle \exists i :: \neg k_i \equiv m_i \rangle \quad \} \\
 & \quad \langle \exists k : \langle \exists i :: \neg k_i \equiv m_i \rangle : \langle \forall i :: \neg k_i \equiv n_i \equiv p_i \rangle \rangle \\
 & \vee \;\; \langle \exists k : \langle \exists i :: \neg k_i \equiv n_i \rangle : \langle \forall i :: m_i \equiv \neg k_i \equiv p_i \rangle \rangle \\
 & \vee \;\; \langle \exists k : \langle \exists i :: \neg k_i \equiv p_i \rangle : \langle \forall i :: m_i \equiv n_i \equiv \neg k_i \rangle \rangle \\
\Rightarrow & \{ \quad \text{substitution of equals for equals} \quad \} \\
 & \langle \exists i :: m_i \equiv n_i \equiv p_i \rangle \quad .
\end{array}
$$

In the second part of the proof, we exhibit a winning strategy.

$$\langle \exists i :: m_i \equiv n_i \equiv p_i \rangle$$

$$
\begin{array}{ll}
= & \{\quad j := \langle \Uparrow i : m_i \equiv n_i \equiv p_i : i\rangle \\
& \quad (\,j \text{ exists because, for sufficiently large } i\,, \\
& \quad m_i\,,\ n_i \text{ and } p_i \text{ are all false: i.e. the bits are zero)} \quad \} \\
& \langle \exists j :: (m_j \equiv n_j \equiv p_j) \wedge \langle \forall i : j < i : \neg(m_i \equiv n_i \equiv p_i)\rangle\rangle \\
= & \{\quad \text{calculus} \quad \} \\
& \quad \langle \exists j :: m_j \wedge (n_j \equiv p_j) \wedge \langle \forall i : j < i : \neg(m_i \equiv n_i \equiv p_i)\rangle\rangle \\
& \vee \ \ \langle \exists j :: n_j \wedge (p_j \equiv m_j) \wedge \langle \forall i : j < i : \neg(m_i \equiv n_i \equiv p_i)\rangle\rangle \\
& \vee \ \ \langle \exists j :: p_j \wedge (m_j \equiv n_j) \wedge \langle \forall i : j < i : \neg(m_i \equiv n_i \equiv p_i)\rangle\rangle \quad .
\end{array}
$$

Continuing with just one of the three disjuncts, we have:

$$
\begin{array}{ll}
& \langle \exists j :: m_j \wedge (n_j \equiv p_j) \wedge \langle \forall i : j < i : \neg(m_i \equiv n_i \equiv p_i)\rangle\rangle \\
\Rightarrow & \{\quad \text{Define number } r \text{ by } \langle \forall i :: r_i \equiv \neg(n_i \equiv p_i)\rangle\,. \\
& \quad \text{This makes } r \text{ a number that is smaller than } m \\
& \quad (\text{because } \langle \exists j :: m_j \wedge \neg r_j \wedge \langle \forall i : j < i : m_i \equiv r_i\rangle\rangle\,, \\
& \quad \text{i.e. at the highest-numbered bit, } j\,\text{, at which } m \text{ and } r \text{ differ,} \\
& \quad m_j \text{ is } 1 \text{ and } r_j \text{ is } 0\,). \quad \} \\
& \langle \exists r : r < m : \langle \forall i :: \neg(r_i \equiv n_i \equiv p_i)\rangle\rangle \\
= & \{\quad \text{induction hypothesis} \quad \} \\
& \langle \exists r : r < m : [r \oplus n \oplus p]\rangle \\
= & \{\quad \text{definition of brackets and mex sum} \quad \} \\
& \langle \exists r : r < m : L.({}^*r + {}^*n + {}^*p)\rangle \\
\Rightarrow & \{\quad (7) \text{ and } (14) \quad \} \\
& \neg L.({}^*m + {}^*n + {}^*p) \\
= & \{\quad \text{definition of brackets} \quad \} \\
& \neg\,[m \oplus n \oplus p] \quad .
\end{array}
$$

Symmetrically,

$$\langle \exists j :: n_j \wedge (p_j \equiv m_j) \wedge \langle \forall i : j < i : \neg(m_i \equiv n_i \equiv p_i)\rangle\rangle \ \Rightarrow\ \neg\,[m \oplus n \oplus p]$$

and

$$\langle \exists j :: p_j \wedge (m_j \equiv n_j) \wedge \langle \forall i : j < i : \neg(m_i \equiv n_i \equiv p_i)\rangle\rangle \ \Rightarrow\ \neg\,[m \oplus n \oplus p] \quad .$$

It follows that

$$\langle \exists i :: m_i \equiv n_i \equiv p_i \rangle \;\Rightarrow\; \neg\, [m \oplus n \oplus p] \quad .$$

The winning strategy is to determine the largest coefficient i such that $m_i \equiv n_i \equiv p_i$, and then choose to move in one of the three games for which the coefficient is one. Then a move is chosen to a position r that makes the mex sum of the three games equal to zero. (Either just one can be chosen, or any of the three can be chosen. For example, in the game of Nim —three piles of matches from each of which any number of matches can be removed— if the piles have 5, 6 and 7 matches, 4 matches should be removed, but which pile is chosen is of no consequence.)

6 Conclusion

The theory of combinatorial games offers excellent opportunities for teaching the mathematics of program construction. In this paper, we have shown how the Bouton-Sprague-Grundy theory of mex numbers can be developed using modern principles of program construction and the calculational method.

Of course, the theory of mex numbers is well-known in the mathematical literature. Nevertheless, this investigation seems to have uncovered a number of novelties. The fact that the mex numbers form a vector space, with the powers of two as basis, is obvious (to professional mathematicians) once pointed out, but it does not seem to have been observed elsewhere. In particular, the relevance of the theorem that every vector space has a basis to the construction of an efficient means of calculating mex sums appears to be novel.

An important aspect of our development is the calculational reasoning with boolean equalities, combining associativity and symmetry properties with the use of Leibniz's rule (substitution of equals for equals). We continue to be surprised and delighted by the power, simplicity and effectiveness of the Dijkstra-Scholten formulation of predicate calculus.

References

[Bac03] Roland Backhouse. *Program Construction. Calculating Implementations From Specifications.* John Wiley Sons, Ltd., 2003.

[BCG82] Elwyn R. Berlekamp, John H. Conway, and Richard K. Guy. *Winning Ways*, volume I and II. Academic Press, 1982.

[BM04] Roland Backhouse and Diethard Michaelis. Fixed-point characterisation of winning strategies in impartial games. In Rudolf Berghammer, Bernhard Möller, and Georg Struth, editors, *Relational and Kleene-Algebraic Methods in Computer Science, 7th International Symposium on Relational Methods in Computer Science and 2nd International Workshop on Applications of Kleene Algebra, Revised Selected Papers*, volume LNCS 3051, pages 34–47. Springer, 2004.

[Bou02] Charles L. Bouton. Nim, a game with a complete mathematical theory. *Ann. of Math., Princeton*, 3(2):35–39, 1901-02.

[Con76] J.H. Conway. *On Numbers and Games*. Academic Press, 1976.

[DS90] E.W. Dijkstra and C.S. Scholten. *Predicate Calculus and Program Semantics*. Springer-Verlag, Berlin, 1990.

[GS56] P.M. Grundy and C.A.B. Smith. Disjunctive games with the last player losing. *Proc. Cambridge Philos. Soc.*, 52:527–533, 1956.

[GS93] David Gries and Fred B. Schneider. *A Logical Approach to Discrete Math*. Springer-Verlag, 1993.

[vG90] A.J.M. van Gasteren. *On the Shape of Mathematical Arguments*. Number 445 in LNCS. Springer-Verlag, 1990.