CSE203-Logic and Proof Final Project Defense - Nim Game

Yubo Cai and Junyuan Wang

Ecole Polytechnique

2022-2023

Winning Strategy of Nim Game

Propersition

In a normal Nim game, the player making the first move has a winning strategy if and only if the nim-sum of the sizes of the heaps is not zero. Otherwise, the second player has a winning strategy. The winning strategy is to make the nim sum becomes 0 after each move.

Here we denote s is the state before move and s' is the state after move. Also, the number here means nim sum.

- **Lemma 1.** If $s = 0$, then $s' \neq 0$ no matter what move is made. (**Lemma** z2nz in Coq)
- **Lemma 2.** If $s \neq 0$, it is possible to make a move so that $s' = 0$. (**Lemma** nz2z in Coq)

Structure of the code for project

- **Part 1.** Numerical Lemma on List, binary numbers and bxor Operations...
- **Part 2.** Definition for state, rows, bijective relation...
- **Part 3.** Operations and Lemma on weights
- **Part 4.** Proof for **turn_weight**, **z2nz**, and **nz2z**

Code for Operations and Lemma on weights

This part of code are operations and Lemma on weights, we prove by induction and operations in bxor.

```
Lemma weight_empty : weight (fun=> 0) = 0%:B.

Lemma weight_r0: weight_r nil = bits0.

Lemma weight_r1 (n : nat): weight_r [:: n] = n2b n.

Lemma weight_rS (n : nat) (ns : list nat) :
  weight_r (n :: ns) = n2b n .+ weight_r ns.

Lemma weight_rD (r s : list nat) :
  weight_r (r ++ s) = bxor (weight_r r) (weight_r s).
```

Proof for **z2nz**

We apply contradiction to prove **z2nz** that if $s = 0$, then $s' \neq 0$ no matter what move is made.

```
Lemma z2nz (i : 'I_p) (s1 s2 : state) :
  R i s1 s2 -> weight s1 = 0%:B -> weight s2 <> 0%:B.
```

We need to prove other two Lemma where $x \oplus x = 0$ and $\forall n \in \mathbb{N}, n < n \to$ false in order to create contradiction.

```
Lemma b02bnbb (x : 'I_p) (s : state):
  0%:B = n2b (s x) .+ n2b (s x).

Lemma ltf (n : nat):
  n < n -> false.
```

We have **n2b_inj** that we can deduce that **s2 i** $=$ **s1 i** which is contradiction with the assupmtion that **s2 i** $<$ **s1 i**.

Proof for **nz2z**

We prove if $s \neq 0$, it is possible to make a move so that $s' = 0$ **nz2z** in following steps. We denote $x_1, \cdots, x_n$ is the number for each row before the move, $y_1, \cdots, y_n$ is the number for each row after the move

- d be the position of leftmost nonzero bit in the binary representation of s exists.
- Prove $\exists k$ such that $x_k[d] \neq 0$. We prove this by contradiction
- Se set $y_k = s \oplus x_k$ and assume $y_k < x_k$, then we prove $\forall i, d < i \to x_k = y_k$
- Finish the prove with weight s' = 0%:B or R k s s'