Unrealizable Cores for Reactive Systems Specifications

Shahar Maoz, Rafi Shalom

2021 年 2 月

预备知识

- 单调判据：
  集合 E 子集上的布尔判据是单调的当且仅当对于集合 A、B，$A \subseteq B \subseteq E$，若 A 满足判据，则 B 满足判据。
- 核：
  给定集合 E 和一个在其子集上的单调判据，一个集合 $C \subseteq E$ 是一个核当且仅当 C 满足该判据，且它所有的真子集 $C' \subset C$ 都不满足该判据。
- 不可综合性（对于系统约束）是单调判据：
  如果一个规约是不可综合的，添加系统约束后仍然是不可综合的。
- 最小化算法：从集合中找到满足判据的最小集合。

预备知识

- DDMin（Delta Debugging）：
  - ☞ 将 E 分成多个（初始为 2）部分，对每部分检查是否符合判据，如果符合，对该部分二分，继续递归判断。
  - ☞ 对每部分的补集检查是否符合判据，如果符合，对补集二分，继续递归判断。
  - ☞ 如果都不符合，将 E 分成更多 (翻倍) 部分，重复算法，直到达到 $|E|$。
- QuickXplain：
  另一个递归的增量式最小化算法。
- LinearMin：
  逐个遍历输入集合中的元素，如果去除该元素，判据仍成立，则去除该元素。

预备知识

- 有基最小化：
  给定集合 E 以及它的两个不相交的子集 $Base, A \subseteq E$，以及一个可以基于单调判据 $check$ 检测核的最小化算法 Alg，假设 $Base \cup A$ 满足判据，将 $MinWBase(Alg, E, Base, A, check)$ 记作可以计算出局部最小值 $A' \subseteq A$，使得 $Base \cup A'$ 满足判据的算法。该算法将 Alg 应用于 A，并且用 $check(Base \cup X)$ 替换所有的 $check(X)$。

- 推论：
  - ☞ 如果 $Base$ 是某个核的子集，则 $Base \cup A'$ 是一个核。
  - ☞ 如果 $Base$ 包含一个核，则 $A' = \emptyset$。

- 引理（增量式核计算方法）：
  A 和 B 是 E 的两个不相交子集，且 $E = A \cup B$，E 满足某个单调判据。令 A' 为 A 的局部最小子集，使得 $A' \cup B$ 满足判据，令 B' 是 B 的局部最小自己，使得 $A' \cup B'$ 满足判据，则 $A' \cup B'$ 是 E 的一个核。

QuickCore

- 观察：
  - ☞ 不可综合性（对系统约束）是单调判据。
  - ☞ 可以通过增量方法计算出核。
  - ☞ 更少的公平性条件可显著降低规约不可综合性的检查时间。
  - ☞ 如果规约没有系统公平性约束，则去除环境公平性约束不会改变不可综合规约的不可综合性，也不会改变获胜集合。
  - ☞ 初始约束的最小化只需要对系统获胜集合进行单步计算，增加常数时间的符号计算。

QuickCore

- QuickCore 先后对系统的公平性、安全性和初始约束进行最小化：
  - ☞ 首先检测如果没有公平性条件是否可综合，如果可以则核至少需要一个公平性条件，则对公平性条件进行有基最小化（基为其他约束），求出公平性条件的最小值；反之核的公平性条件为空，环境公平性约束也可以为空。
  - ☞ 然后对系统安全性条件进行有基最小化。
  - ☞ 在公平性、安全行条件最小化的基础上，求出系统获胜集合。利用 LinearMin 逐个检查初始约束是否可去除，求出最小值。

QuickCore

- 算法正确性：
  如果规约没有系统公平性约束，则去除环境公平性约束不会改变不可综合规约的不可综合性，也不会改变获胜集合。
  直观来说：没有系统公平性的规约不可综合，即环境存在一个有限步数内获胜的策略，则去除环境公平性约束不改变不可综合性；对于这种规约，如果系统在有限步内不输，则无论环境公平性是什么，都可以赢得无穷博弈。
  形式化来说：$\bigwedge_{j\in J_e} GFj \rightarrow \top$ 是永真式，j 是什么不影响结果。
- 算法复杂度：
  $O(n^2)$。

Punch

- Punch 可应用于任何单调判据：
  - ☞ 给定集合 E，以及所有核的子集 $K \subseteq E$;
  - ☞ 先找出一个核 C_0，遍历 $C_0 \setminus K$ 里的元素 x，若 $E \setminus \{x\}$ 满足判据则将 x 放入 $Cont$，否则放入 CI;
  - ☞ 遍历 $Cont$ 中的元素 x，对 $E \setminus \{x\}$、$K \cup CI$ 继续执行算法计算核。
- 算法正确性：
  - ☞ CI 是所有核的交集；
  - ☞ 数学归纳法。
- 算法复杂度：
  指数。

谢　谢!

Thank you!