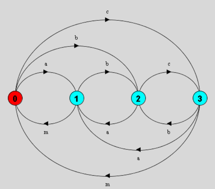
Two-Player Games based Controllers for Cooking Biscotti

Nicolás R. D'Ippolito – ndippolito@dc.uba.ar
LAFHIS - Dpto. de Computación, FCEyN, UBA

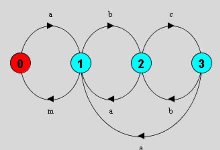
Our Approach

What's our goal?
Automatically generate models satisfying system goals



φ

SGR(1)



The Technique
Safe Generalised Reactivity (1)

- Aligned with Requirements Engineering Best Practices
- Polynomial Time Solution

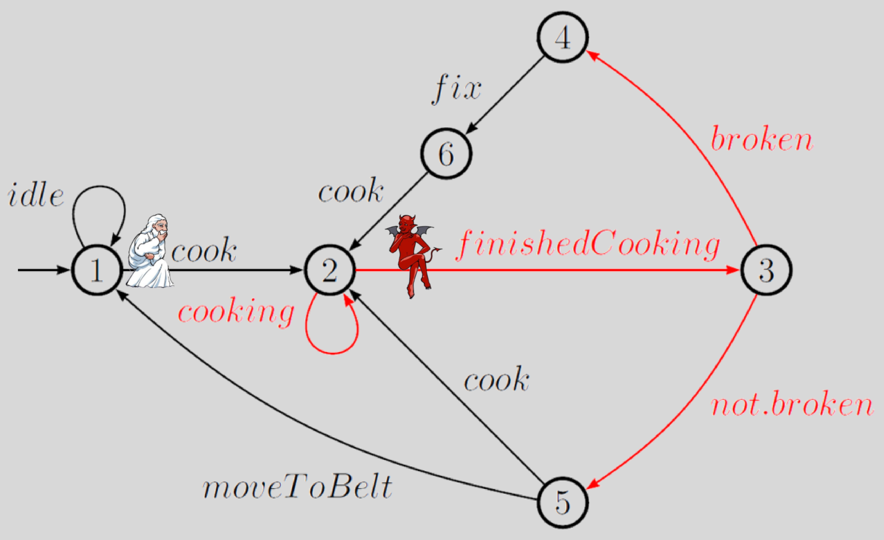
How do we achieve our goal?
Generating strategies for Two-Player Games

+

Winning Condition:
Lineal Temporal Logic

φ

Cooking Biscotti with Synthesised SGR(1) Controllers



$$|| \quad x \quad \models \quad \square(\mathit{moveToBelt} \Rightarrow \mathit{SuccessfullyCookedTwice}) \wedge \square\Diamond\neg \mathit{cooking} \Rightarrow \square\Diamond \mathit{moveToBelt}$$

Assumptions on Failures (i.e broken)

No restriction on failures

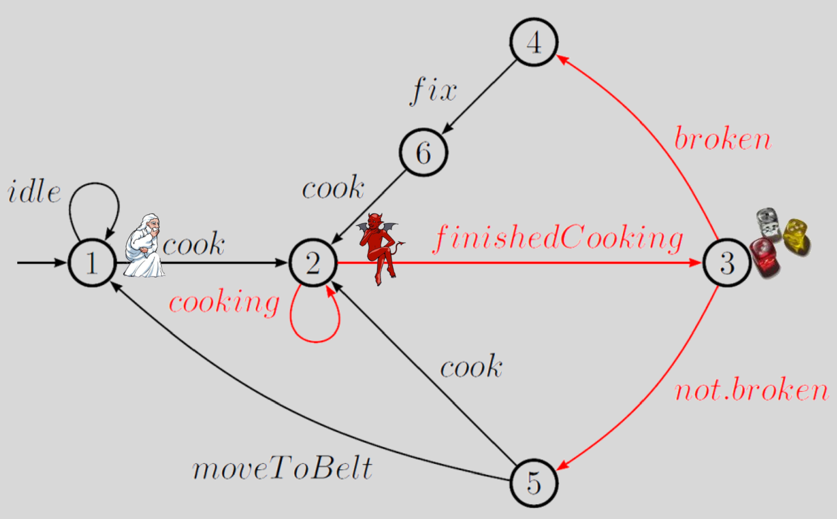
$$\pi = (\mathit{cook}, \mathit{finishCooking}, \mathit{broken}, \mathit{fix})^w \not\models \square(\mathit{moveToBelt} \Rightarrow \mathit{SuccessfullyCookedTwice}) \wedge \square\Diamond\neg \mathit{cooking} \Rightarrow \square\Diamond \mathit{moveToBelt}$$

Strong Fairness on failures

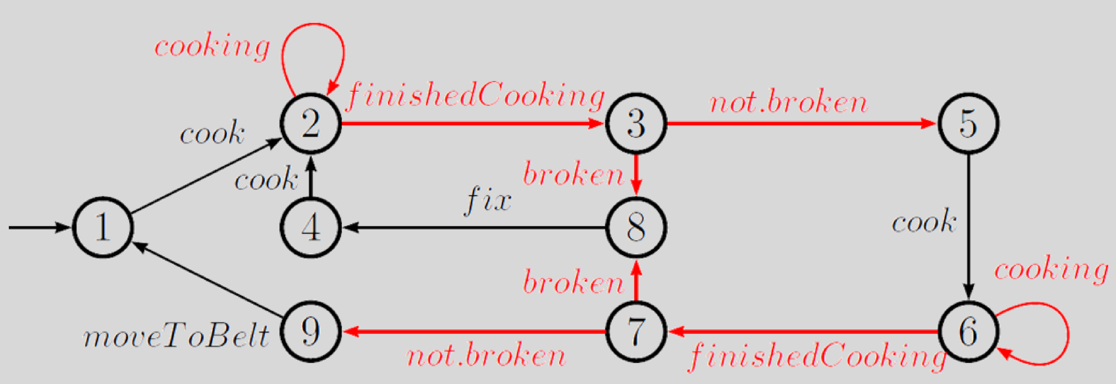
$$\pi = (\mathit{cook}, \mathit{finishCooking}, \mathit{not.broken}, \mathit{cook}, \mathit{finishCooking}, \mathit{broken}, \mathit{fix})^w \not\models \square(\mathit{moveToBelt} \Rightarrow \mathit{SuccessfullyCookedTwice}) \wedge \left(\square\Diamond\neg \mathit{cooking} \wedge \square\Diamond \mathit{cook} \Rightarrow \square\Diamond \mathit{not.broken}\right) \Rightarrow \square\Diamond \mathit{moveToBelt}$$

No Solution

Probabilistic Interpretation of Failures



$||$



$$\models \square(\mathit{moveToBelt} \Rightarrow \mathit{SuccessfullyCookedTwice}) \wedge \square\Diamond\neg \mathit{cooking} \Rightarrow \square\Diamond \mathit{moveToBelt}$$

Fitting Probabilities into SGR(1)

Strong Independent Fairness (SIF)

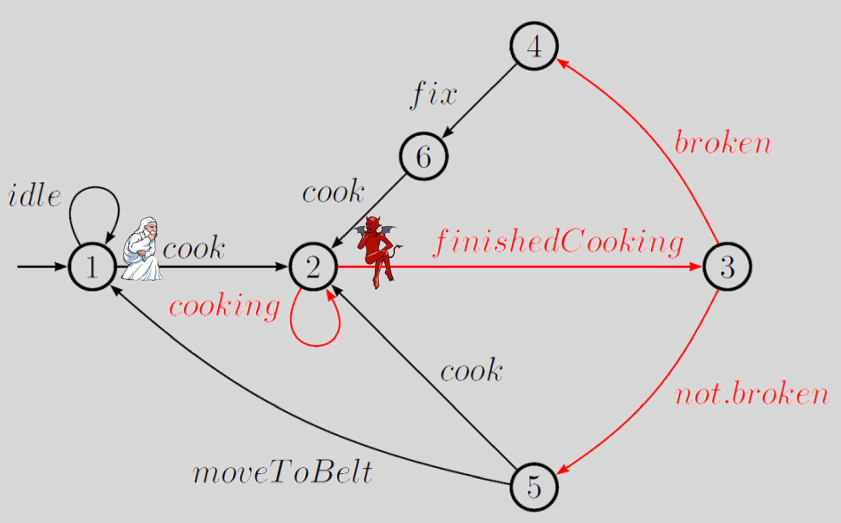
$$\bigwedge_i (\square\Diamond \mathit{cook}_i \Rightarrow \square\Diamond(\mathit{not.broken}_i \wedge (\neg \mathit{broken}_i\, W \neg \mathit{cooking})))$$

+

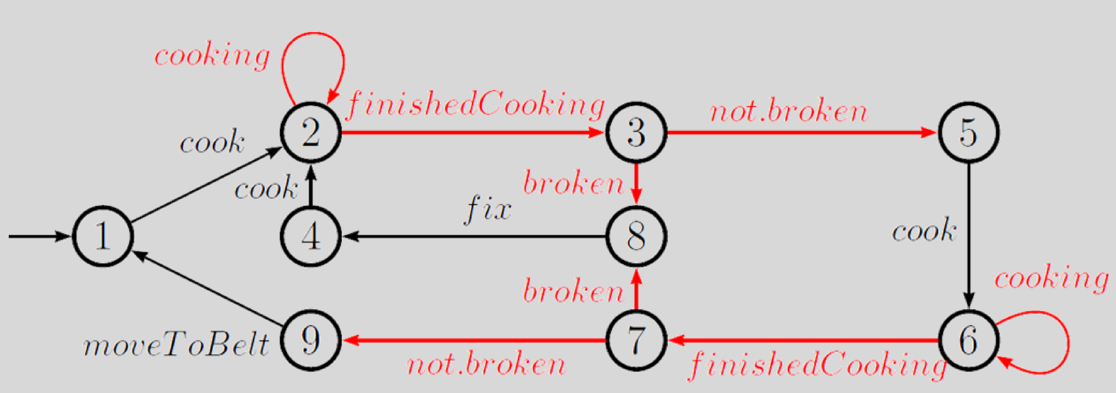
Theorem
If there exists a probabilistic interpretation of failures behaviour, then the probabilistic measure of traces violating SIF is zero.

First Eureka!

Strong Independent Fairness characterises the independence between failures and environment assumptions and allows for discrete modelling



$||$



Strong Independent Fairness (SIF)

$$\models \square\Diamond\neg \mathit{cooking} \wedge \mathit{SIF} \Rightarrow \square\Diamond \mathit{moveToBelt}$$

Theorem
SIF is solvable iff FMF is solvable

Second Eureka!

$$\models \Diamond\square\neg \mathit{broken} \Rightarrow (\square\Diamond\neg \mathit{cooking} \Rightarrow \square\Diamond \mathit{moveToBelt})$$

Finitely Many Failures (FMF)

Theorem
FMF is equivalent to SGR(1)