Fairness constraints in modelling.

used to describe some form of non-det. sequences.

When a non-det. choice occurs, we often assume it to be **fair**: it does not consistently omit one option.

e.g. in the ABP messages can be lost (forgotten) but we don't want it to happen systematically)

Fairness property

expresses that, under certain condition, an event will occur (or will fail to occur) inf. often

if access to a critical section is inf. often requested, then access will be granted inf. often

CTL can express

$A\overset{\infty}{F}p$ by $AGAFp$

$E\overset{\infty}{F}p$ is not expressible

Model Checking With Fairness

Note: For LTL, fairness constraints are not needed.

Why? Can always write

$$\underbrace{GF\varphi}_{\text{inf. often } \varphi} \rightarrow \psi \qquad \text{LTL}$$

Compare: adding As or Es to obtain a CTL formula won't work:

$$\underbrace{AGAF\varphi}_{\text{inf. often } \varphi} \rightarrow \psi \qquad \text{CTL}$$

CTL formula says:

"if all paths are fair, then Ψ holds"

LTL formula restricts our attention to the paths which are fair (don't care about the other ones)

Idea for CTL:

restrict the range of connectives A and E in all CTL specifications

(done by adding FAIRNESS in SMV)

Can define "CTL + fairness"

the CTL algorithms can be adopted, but the complexity of MC increases to $\mathcal{O}(|A| \times |\varphi|^2)$.

many tools (like SMV) suggest to use fairness hypotheses (fairness constraints) as part of the model rather than to use CTL + fairness

Note: In SMV, we allow simple fairness constraints only, e.g. "!st=c inf. often"

Do not allow other types of constraints, e.g.

$\boxed{\text{If } \varphi \text{ inf. often then } \psi \text{ inf. often.}}$

How to implement?

Let $C \stackrel{\text{def}}{=} \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$

be a set of n fairness constraints

<u>Def</u> A computational path

$s_0 \to s_1 \to \ldots$

<u>is fair</u> with respect to C

if for each i there are infinitely many j's such that $s_j \models \varphi_i$, i.e., <u>each φ_i occurs inf. often along the path</u>.

Notation: A_C, E_C mean

A and E restricted to fair paths (~~those~~ w.r.t. set C)

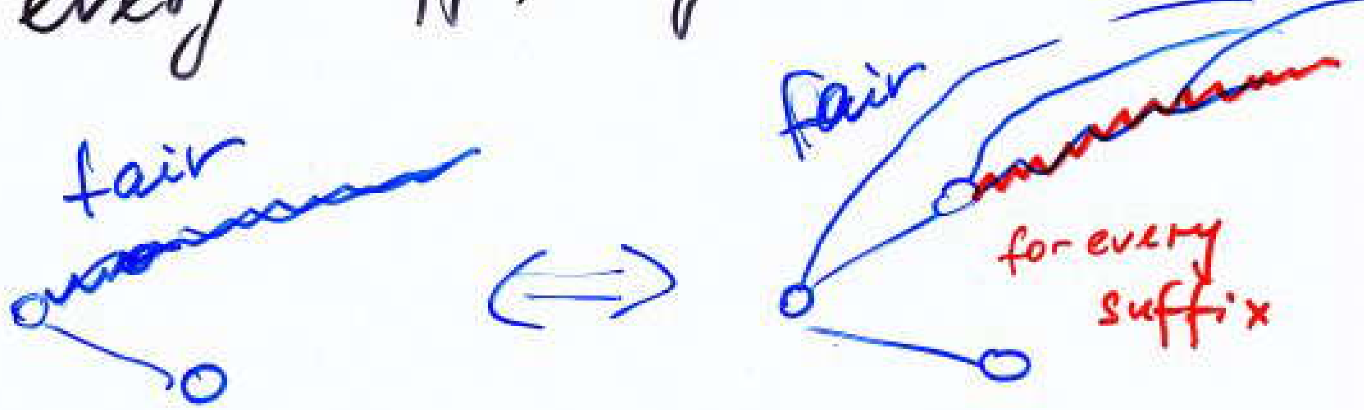
Ex. $M, s_0 \models A_C G \varphi$

iff φ is true in every state along all fair paths

(w.r.t. C)

Note: a) $\{E_C U, E_C G, E_C X\}$ is an adequate set of fair temporal connectives.

b) a path is fair iff every suffix of it is fair



Thus:

$$E_C X \varphi \equiv EX(\varphi \wedge \underbrace{E_C G T}_{\text{some path from the current state is fair}})$$

EX restricted to the fair paths

$E_C G T$ means "there is a path which satisfies the fairness constraints C and formula T is true in every state of it"

trivially true

Also,

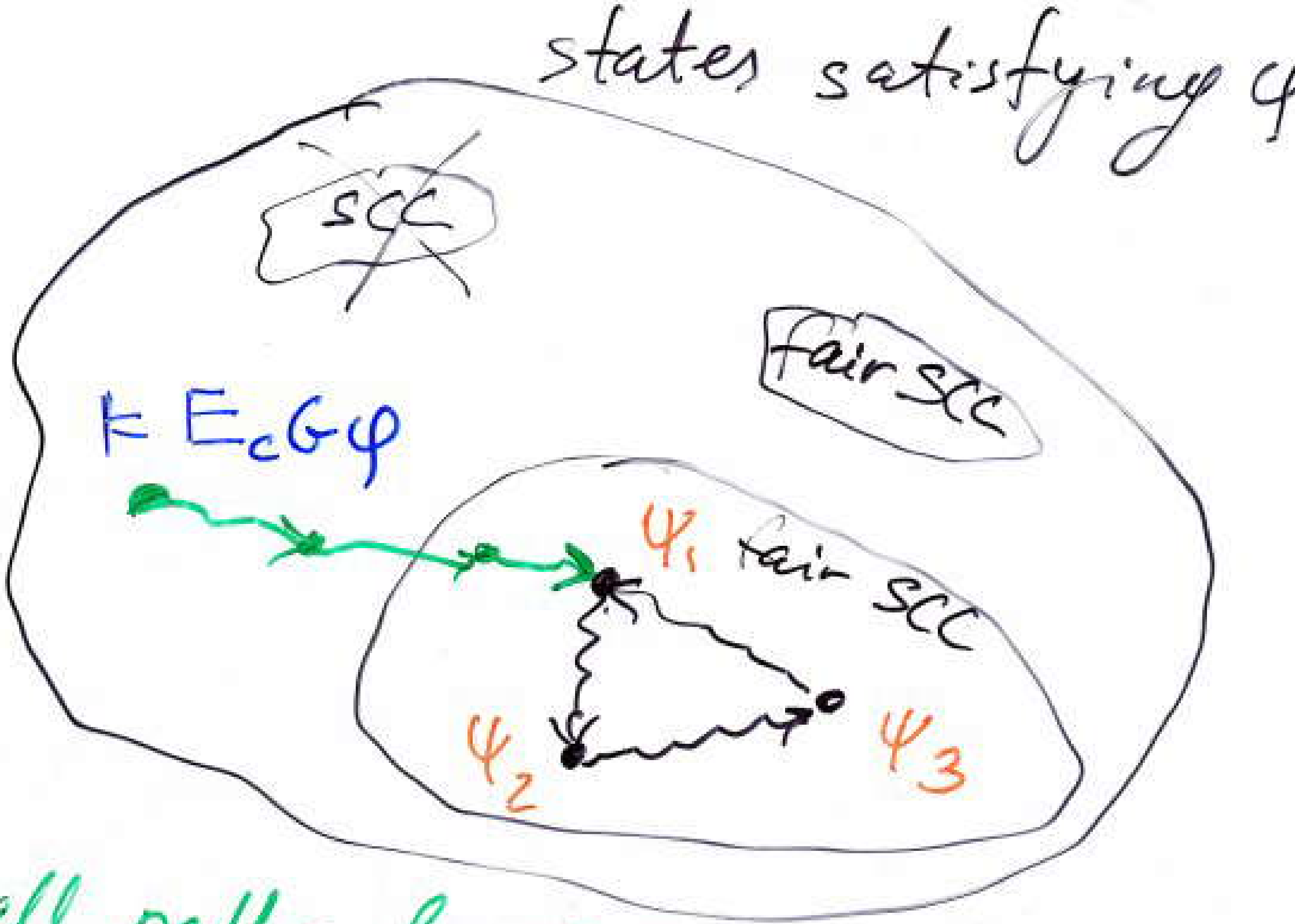
$$E_c[\varphi \, U \, \psi] \equiv E[\varphi \, U \, (\psi \wedge \underline{E_c G T})]$$

$\Rightarrow$ an algorithm for $E_c G$ is sufficient to deal with fairness constraints

Algorithm for $E_C G \varphi$ where $C = \{\psi_1, .., \psi_n\}$

fairness constraints.

- Restrict the graph to states satisfying φ
- Find the maximal SCCs of the restricted graph
- For every SCC, check whether, for each $\psi_i \in C$, the SCC contains a state where ψ_i is true, otherwise, remove this SCC (since it's not fair)



all paths leading to the remaining SCC are fair

$C = \{\psi_1, \psi_2, \psi_3\}$

Use Breadth-first-search to find the states of the restricted graph that can reach a fair SCC.

$O(n \cdot f \cdot (V+E))$