Robin Milner and Mathematics

Glynn Winskel

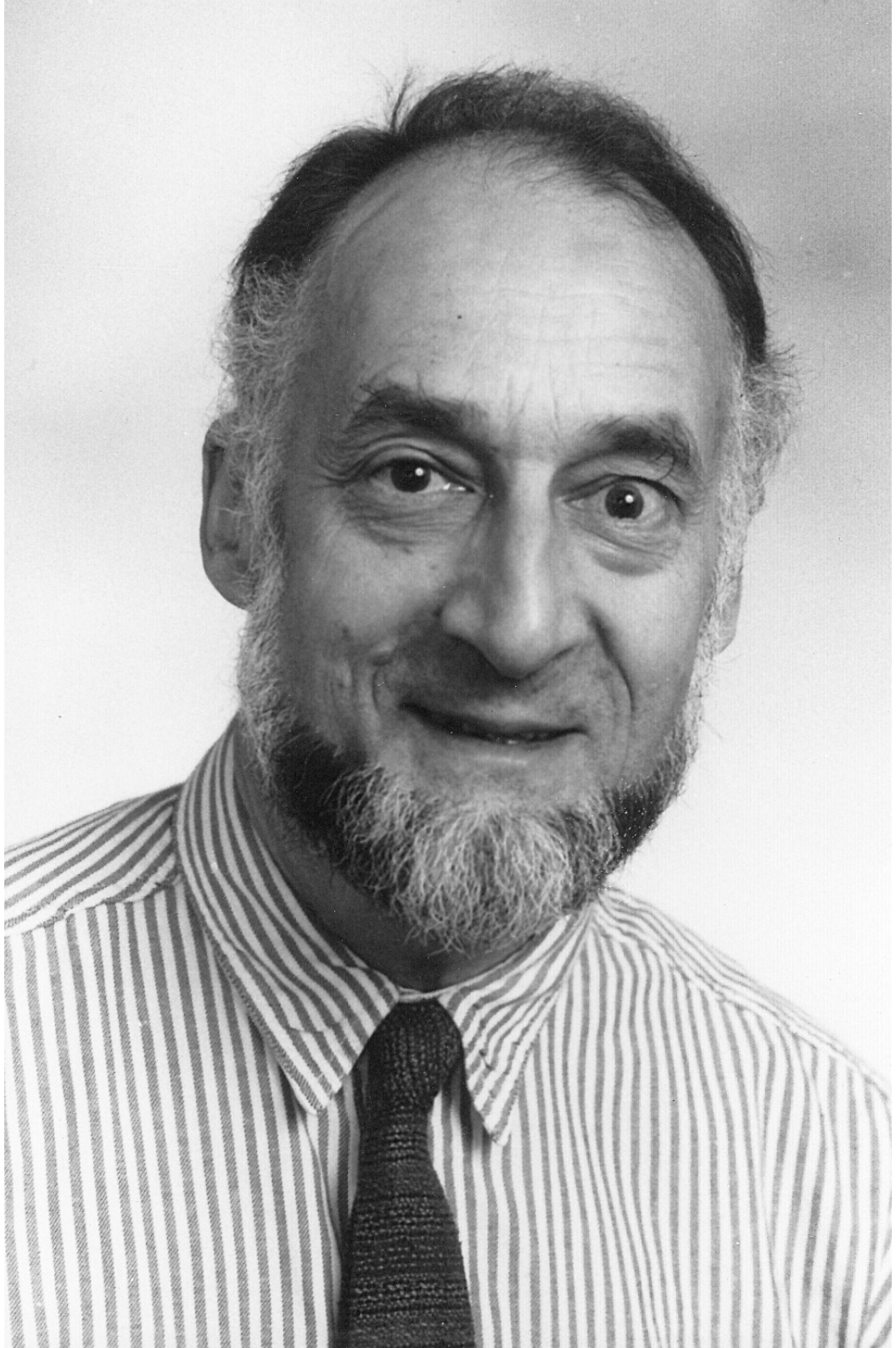
1. Background, Robin's intellectual position(s)
2. Robin's attitude, contributions and potential contributions to Mathematics
3. Robin's ideas and concurrent strategies

Milner Symposium, Edinburgh April 2012

From the speech to Robin Milner on the award of an Honorary Doctorate, Aarhus University, September 1998

While Computer Science leans on Mathematics, Engineering and Physics, its theory, principles and methodology, questions on how to structure and manage the burgeoning world of computation, have to be tackled afresh. The foundational insights of Professor Robin Milner, theory with a keen eye to potential practice, have carved out patterns of research fundamental in Programming Languages and Types, Machine Proof, and Distributed and Mobile Computation. . . .

. . . Robin Milner's research will have a lasting influence on Computer Science. After the fact, the main lines of his work on the foundations of computing share with many great ideas a naturalness and obviousness that belies the hard, detailed and often very specialised work that preceded them. For many in the field it is hard to imagine Computer Science without the fundamental contributions of Robin Milner. What could be a better tribute to a researcher?



Where Robin stood

Operational vs. Denotational semantics: increasingly towards operational semantics and away from denotational semantics

Higher-order: increasingly seen as not fundamental

Extensional vs. intensional: extensional

Equational vs. assertional proof: his own work is almost exclusively equational

Theory vs. practice: theory as a prescriptive tool for practice as it might become

Role of Logic: "Paradise lost" (but modern developments in proof theory? Robin felt a debt to Girard)

Role of Mathematics: mathematics as an *essential tool*


38 moves
FASE
KNIGHTS

Robin Milner and Mathematics

Robin had an early and continuing aptitude for solving problems and Mathematics.

But Mathematics was never the primary goal of his work; his work was CS-motivated, though not always obviously so.
He didn't share the view that: get the Maths right and the rest will follow.
He didn't borrow from deep theories in Mathematics.

Nevertheless,
his ideas are often essentially right and enriching from a mathematical perspective.
His work is likely to have a lasting influence on Mathematics.

Interactive Theorem Proving

LCF $\leadsto$ **ML** and its types to support secure theorem proving

Descendants:

HOL, hardware verification

Isabelle, a meta-prover

Coq, implementing a powerful constructive logic.
$\leadsto$ George Gonthier and Benjamin Werner's Coq proof of the 4-colour conjecture

(Strong) Bisimilarity and Coinduction

$Bisimilarity$ is a ubiquitous intrinsic equivalence, independent of syntax.

On a suggestion of David Park, Robin's original strong bisimilarity $viz.$

$$\bigcap_{n\in\omega} \sim_n$$

via a chain of relations $\sim_n$, was changed to

$$\bigcap_{\alpha\in\mathbf{On}} \sim_\alpha$$

which can be characterised as a greatest post-fixed point. $\rightsquigarrow$ proof technique: to show bisimilarity exhibit a bisimulation.

Bisimulation has inspired a variety of methods of $coinduction.$

Methods of Coinduction

In *coalgebras* homomorphisms are functional bisimulations. To show equality in final coalgebras (*e.g.* streams) suffices to exhibit a bisimulation. (I think this was anticipated in work of Arbib&Manes.)

Freyd's 1990 reformulation of how to solve *recursive domain equations* led to new induction and coinduction principles by uncovering 'bisimulations' for recursive domains [Fiore, Plotkin, Pitts].

Non-wellfounded sets [Aczel, Forti, Honsell].

Coinduction is used recently in defining ∞-*categories* [Lafont, Métayer].

Weak Bisimilarity

Weak bisimilarity is an intrinsic equivalence capturing the invisibility of internal actions. Weak bisimilarity is strong bisimilarity wrt transitions

$$p \stackrel{\tau}{\Rightarrow} q \text{ iff } p(\stackrel{\tau}{\longrightarrow})^* q \quad \text{and} \quad p \stackrel{a}{\Rightarrow} q \text{ iff } \exists r, r'.\ p \stackrel{\tau}{\Rightarrow} r \ \&\ r \stackrel{a}{\longrightarrow} r' \ \&\ r' \stackrel{\tau}{\Rightarrow} q\ .$$

But weak bisimilarity is not a congruence for *e.g.* CCS. $\rightsquigarrow$ *observation congruence*.

In the general open-map development of bisimilarity and weak bisimilarity, the analogue of observation congruence is primary [Cattani-Fiore-W].
Future techniques for weak equivalences?

Names in the Pi-Calculus

In the original development of a name-passing calculus by Mogens Nielsen and Uffe Engberg (based on early joint work of Robin and Mogens) there were $both$ $names$ and $variables$ (over names).

In the fuller and final development of the Pi-Calculus [RM, Parrow and Walker] $variables\ are\ banished$ and names do double-duty also as variables (Occam's razor). A non-traditional deconstruction of the role of variables which has handicapped traditional denotational semantics of the Pi-Calculus.

But in Andy Pitts' $Nominal\ Sets$ there is a similar deconstruction of variables occurs within Fraenkel-Mostowski set theory. The restriction operator of the Pi-Calculus can be seen as derived from a new-name abstraction on Nominal Sets. In recent work Pitts is basing constructions on sets with 'restriction operators.'

Concurrency

• The operations of process algebras, Robin's Calculus of Communicating Systems (CCS 1979) and Tony's CSP, can be expressed in terms of universal constructions for a variety of models, within categories of transition systems, labelled trees, Petri nets, languages, Mazurkiewicz languages, event structures, ...

E.g. Synchronized parallel compositions of event structures are obtained as a restriction (equalizer) of a product in a category of event structures.

• Relations between models via adjunctions.

In Robin's view concurrency brings a fundamental new aspect to computing. Influence on Mathematics, and other areas?

Concurrent strategies

The notion of *deterministic/nondeterministic strategy*
is potentially as fundamental as the notion of *function/relation*.
The notion needs to be developed in sufficient generality.

Two-party concurrent games: Player (a team of players) against Opponent (a team of opponents) subject to constraints of the game.
For *Player/Opponent* read *process/environment, proof/refutation, ally/enemy.*

First: in a general model for concurrency, *event structures*
—*the concurrency analogue of trees.*
Later: a recent more geometrical view
—*games as factorization systems.*

A generalized domain theory:
Functional programming $\rightsquigarrow$ Strategical programming

Event structures

An **event structure** comprises $(E, \leq, \#)$, consisting of a set of *events* E

- partially ordered by $\leq$, the **causal dependency relation**, and

- a binary irreflexive symmetric relation $\#$, the **conflict relation**,

which satisfy $\{e' \mid e' \leq e\}$ is finite and $e \# e' \leq e'' \Rightarrow e \# e''$.

The finite **configurations**, $\mathcal{C}(E)$, of an event structure E consist of those subsets $x \subseteq E$ which are
Consistent: $\forall e, e' \in x.\ \neg(e \# e')$ and *Down-closed:* $\forall e, e'.\ e' \leq e \in x \Rightarrow e' \in x$.

Concurrent games—basics

Games and strategies are represented by **event structures with polarity**, $+/-$ (Player/Opponent).

(Simple) Parallel composition: $A \| B$, by juxtaposition.

Dual, $B^{\perp}$, of an event structure with polarity B is a copy of the event structure B with a reversal of polarities; $\overline{b} \in B^{\perp}$ is complement of $b \in B$, and *vice versa*.

A (nondeterministic) **pre-strategy** in game A is a total map

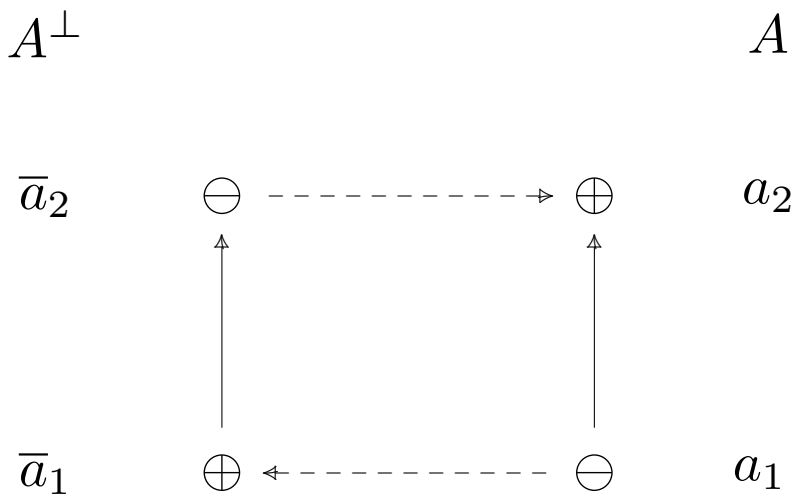
$$\begin{array}{c} S \\ {\scriptstyle \sigma}\downarrow \\ A \end{array}$$

i.e. σ *preserves polarities and*

$$\forall x \in \mathcal{C}(S).\ \sigma x \in \mathcal{C}(A) \ \ \& \ \ \forall s_1, s_2 \in x.\ \sigma(s_1) = \sigma(s_2) \Rightarrow s_1 = s_2.$$

Copy-cat—an example

$$\mathbb{CC}_A$$

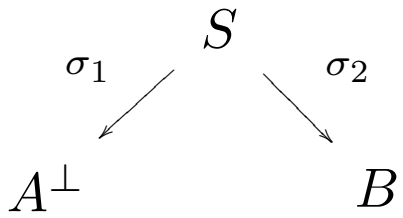


Pre-strategies as arrows

A pre-strategy $\sigma : A \nrightarrow B$, *from* A *to* B, is a strategy *in* $A^{\perp} \parallel B$, *i.e.*

$$\sigma : S \to A^{\perp} \parallel B\,.$$

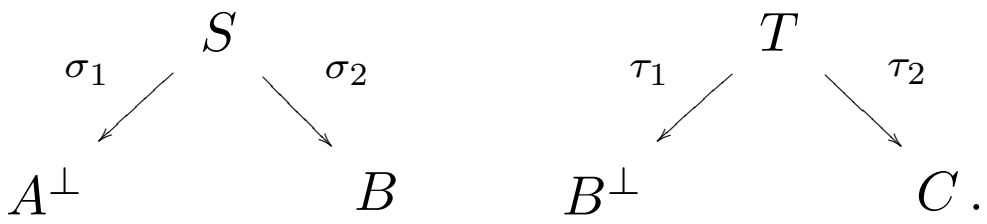
It corresponds to a *span* of event structures with polarity



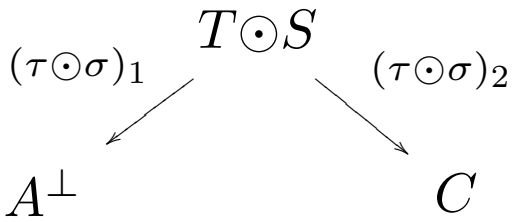
where σ_1, σ_2 are *partial* maps of event structures with polarity; one and only one of σ_1, σ_2 is defined on each event of S.

Composing pre-strategies

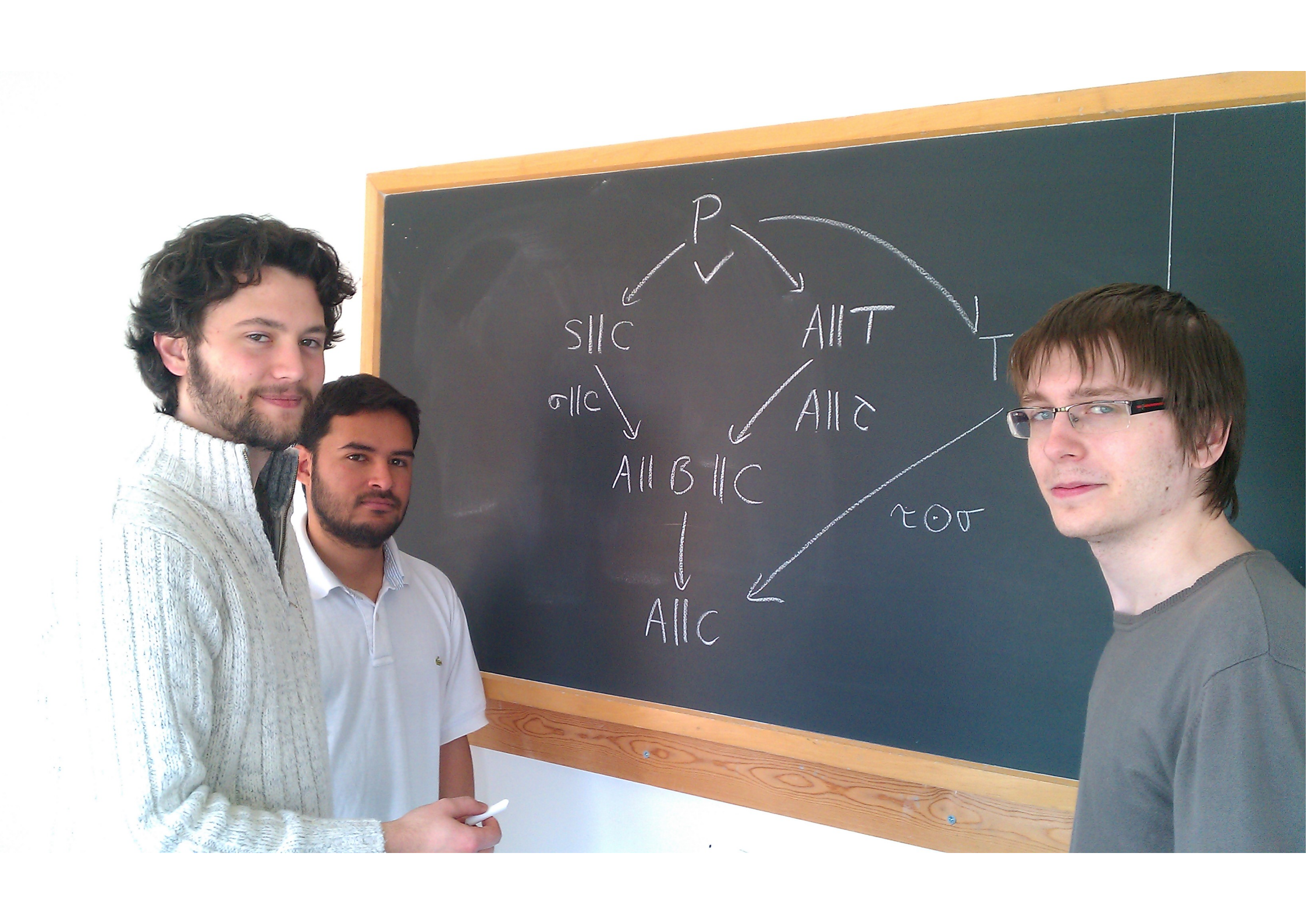
Two pre-strategies $\sigma : A \nrightarrow B$ and $\tau : B \nrightarrow C$ as spans:



Their composition



where $T \odot S =_{\mathrm{def}} (S \times T \restriction \mathbf{Syn}) \downarrow \mathbf{Vis}$ where ...


P
S ∥ C
A ∥ T
T
σ ∥ C
A ∥ C
A ∥ B ∥ C
τ ∘ σ
A ∥ C

Strategies

Copy-cat $\mathbb{CC}_A$ is idempotent:

$$\mathbb{CC}_A \odot \mathbb{CC}_A \cong \mathbb{CC}_A \,.$$

Strategies are defined to be those pre-strategies $\sigma : A \nrightarrow B$ which "compose well" with copy-cat:

$$\mathbb{CC}_B \odot \sigma \odot \mathbb{CC}_A \cong \sigma \,,$$

so those obtained as

$$\mathbb{CC}_B \odot \sigma \odot \mathbb{CC}_A \,,$$

for a pre-strategy $\sigma : A \nrightarrow B$.

$$\rightsquigarrow \quad \textit{a bicategory of concurrent strategies}$$

A characterization of strategies

A strategy in a game A comprises $\sigma : S \to A$, a total map of event structures with polarity, such that

(i) whenever $\sigma x \subseteq^{-} y$ in $\mathcal{C}(A)$ there is a unique $x' \in \mathcal{C}(S)$ so that $x \subseteq x'$ & $\sigma x' = y$, *i.e.*

$$\begin{array}{ccc} x & \subseteq & x' \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ \sigma x & \subseteq^{-} & y\,, \end{array}$$

and

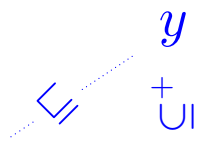
(ii) whenever $y \subseteq^{+} \sigma x$ in $\mathcal{C}(A)$ there is a (necessarily unique) $x' \in \mathcal{C}(S)$ so that $x' \subseteq x$ & $\sigma x' = y$, *i.e.*

$$\begin{array}{ccc} x' & \subseteq & x \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ y & \subseteq^{+} & \sigma x\,. \end{array}$$

Corollary

Defining a partial order — *the Scott order* — on configurations of A

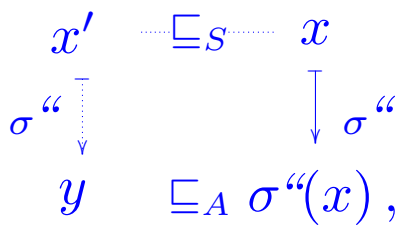
$$x \sqsubseteq_A y \iff_{\text{def}} x \supseteq^- \cdot \subseteq^+ \cdots \supseteq^- \cdot \subseteq^+ y$$



we obtain a factorization system $((\mathcal{C}(A), \sqsubseteq_A), \supseteq^-, \subseteq^+)$, *i.e.* $\exists! z.\ x \supseteq^- z$.

Theorem *Strategies $\sigma : S \to A$ correspond to a discrete fibrations*

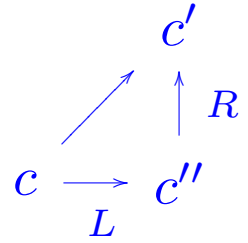
$$\sigma\text{“}: (\mathcal{C}(S), \sqsubseteq_S) \to (\mathcal{C}(A), \sqsubseteq_A), \quad i.e.$$



preserving $\supseteq^-$, $\subseteq^+$ and $\emptyset$.

Games as factorization systems

A **rooted factorization system** $(\mathbb{C}, L, R, 0)$ comprises a small category $\mathbb{C}$ on which there is a factorization system $(\mathbb{C}, L, R)$,

so all maps $c \to c'$ factor uniquely up to iso as 

,

with an object 0 s.t.

$$0 \leftarrow_L \cdot \rightarrow_R \cdots \leftarrow_L \cdot \rightarrow_R c$$

for all objects c in $\mathbb{C}$.

Example $((\mathcal{C}(A), \sqsubseteq_A) \ , \supseteq^-, \subseteq^+, \emptyset)$ for a concurrent game A.

Strategies

A *strategy in* a rooted factorization system $\mathbb{A}$ is a discrete fibration

$$\begin{array}{c} \mathbb{S} \\ {\scriptstyle F}\downarrow \\ \mathbb{A} \end{array}$$

from another rooted factorization system $\mathbb{S}$, which preserves L, R maps and 0.
Example: σ" for a concurrent strategy σ.

A *strategy from* $\mathbb{A}$ *to* $\mathbb{B}$ is a strategy in $\mathbb{A}^{\perp} \| \mathbb{B}$ where

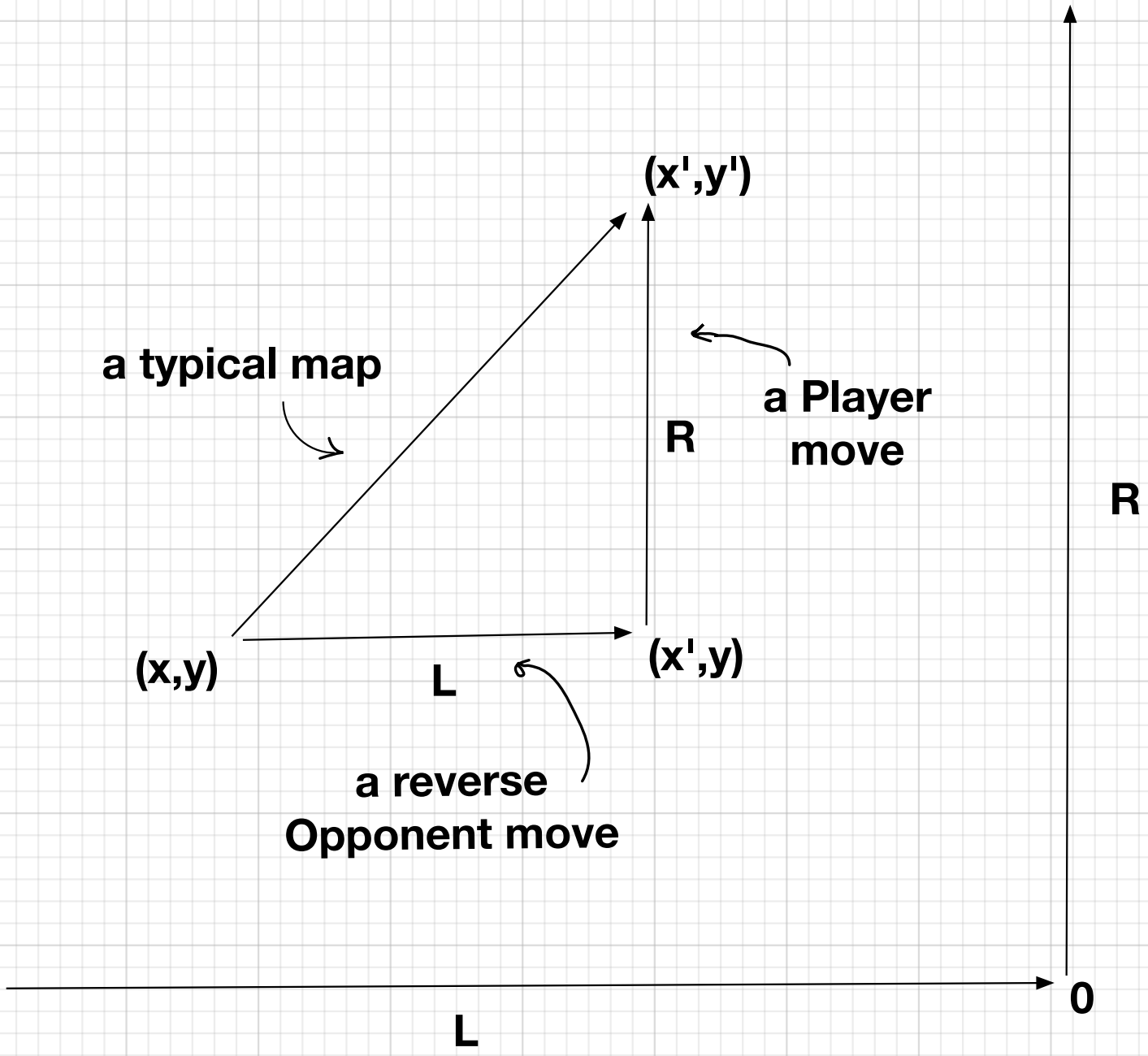
$$(\mathbb{A}, L, R, 0)^{\perp} =_{\text{def}} (\mathbb{A}^{\text{op}}, R^{\text{op}}, L^{\text{op}}, 0)$$

$$(\mathbb{A}, L_A, R_A, 0_A) \| (\mathbb{B}, L_B, R_B, 0_B) =_{\text{def}} (\mathbb{A} \times \mathbb{B}, L_A \times L_B, R_A \times R_B, (0_A, 0_B))$$

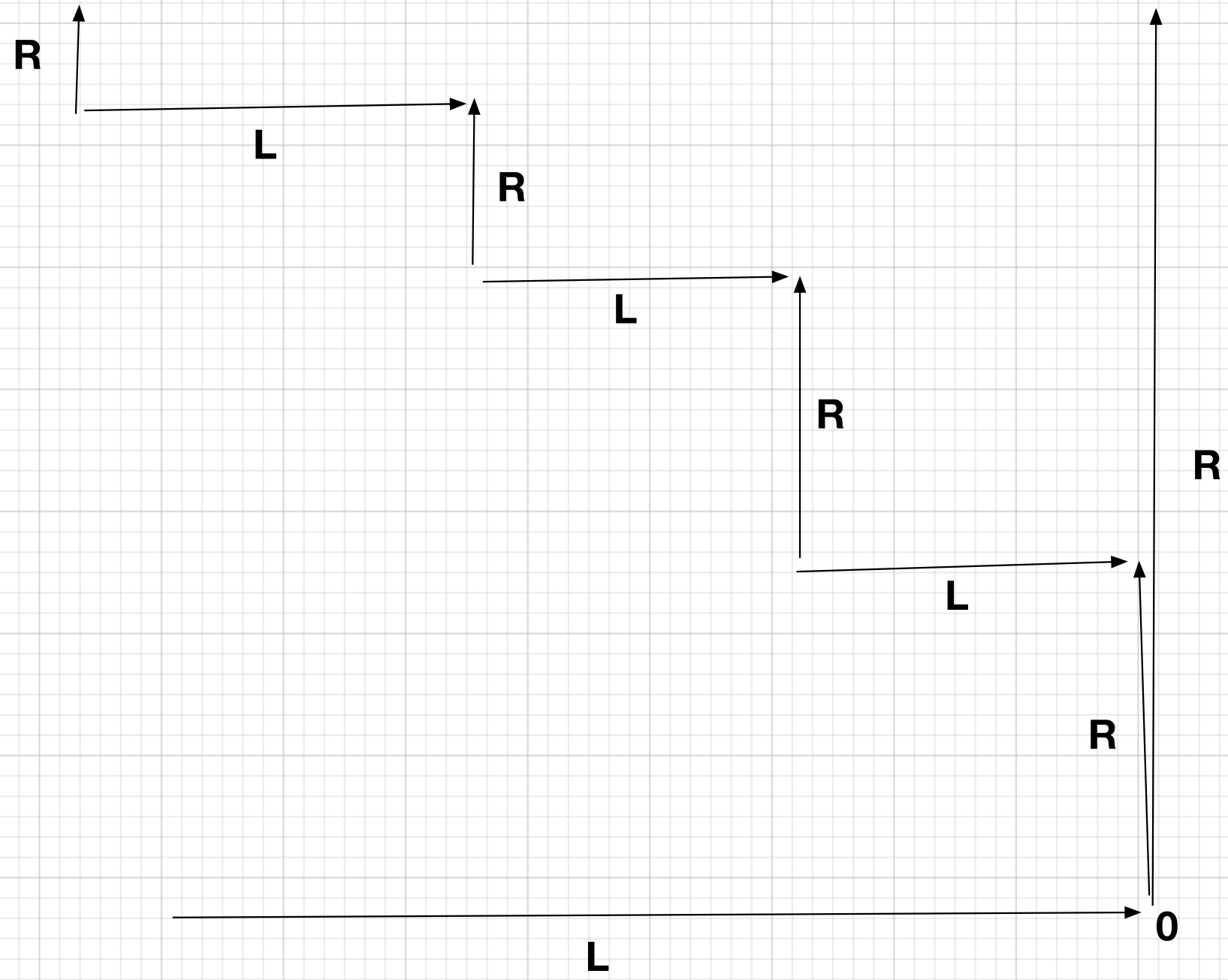
Composition: *reachable part of* profunctor composition.

$\rightsquigarrow$ *'Venn diagrams' for games and strategies.*

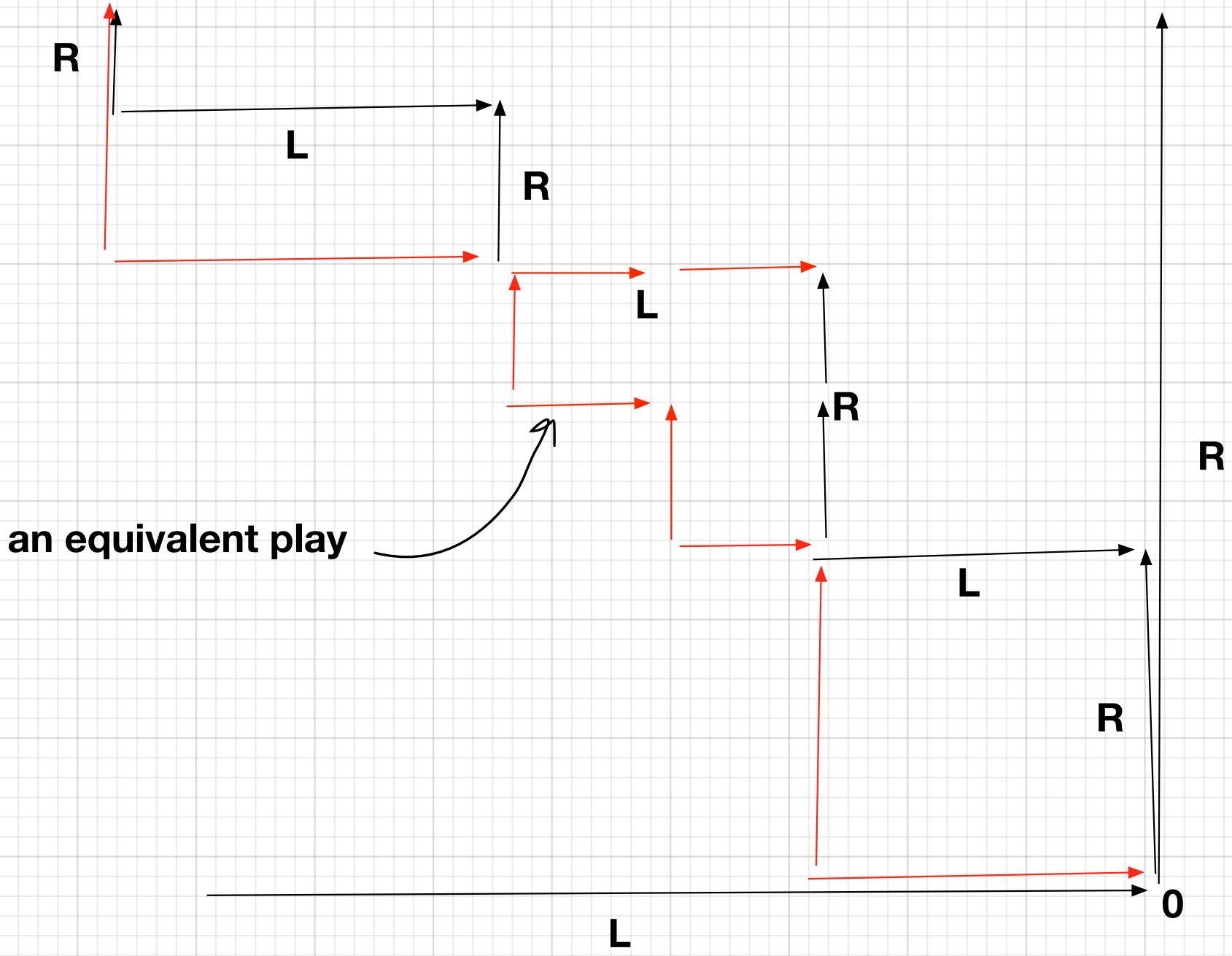
Example: the Euclidean quarter plane



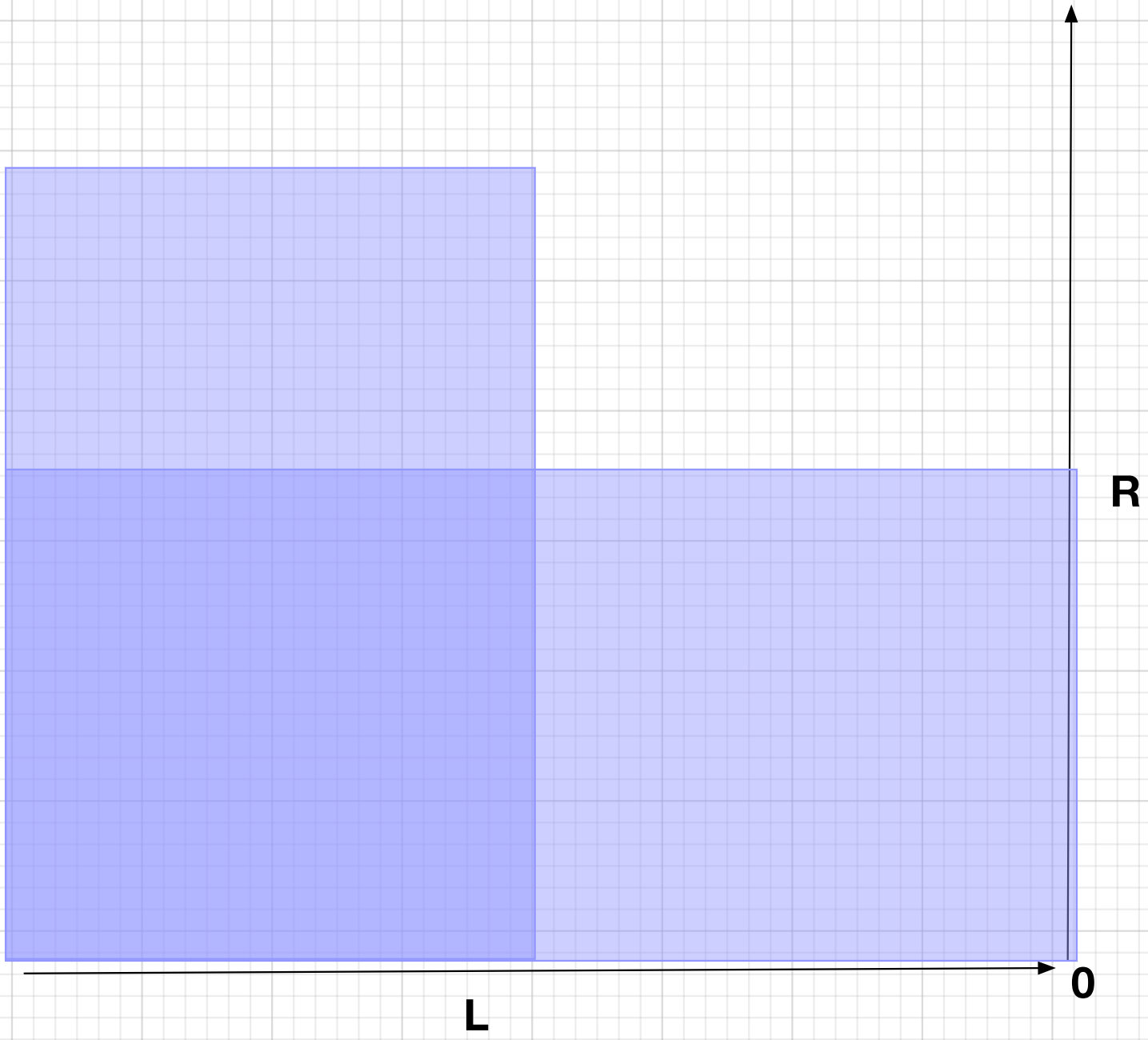
A typical play



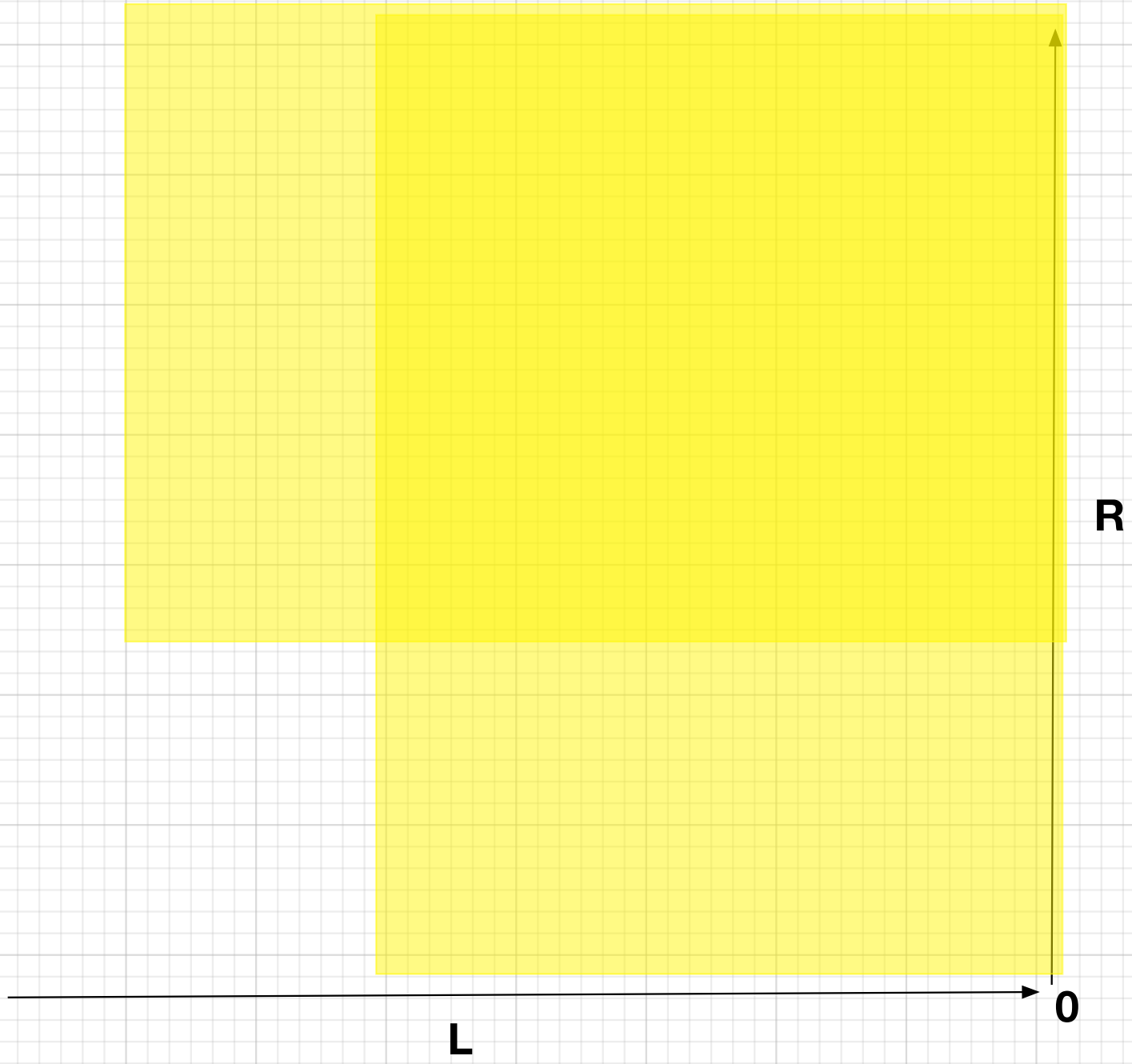
A typical play



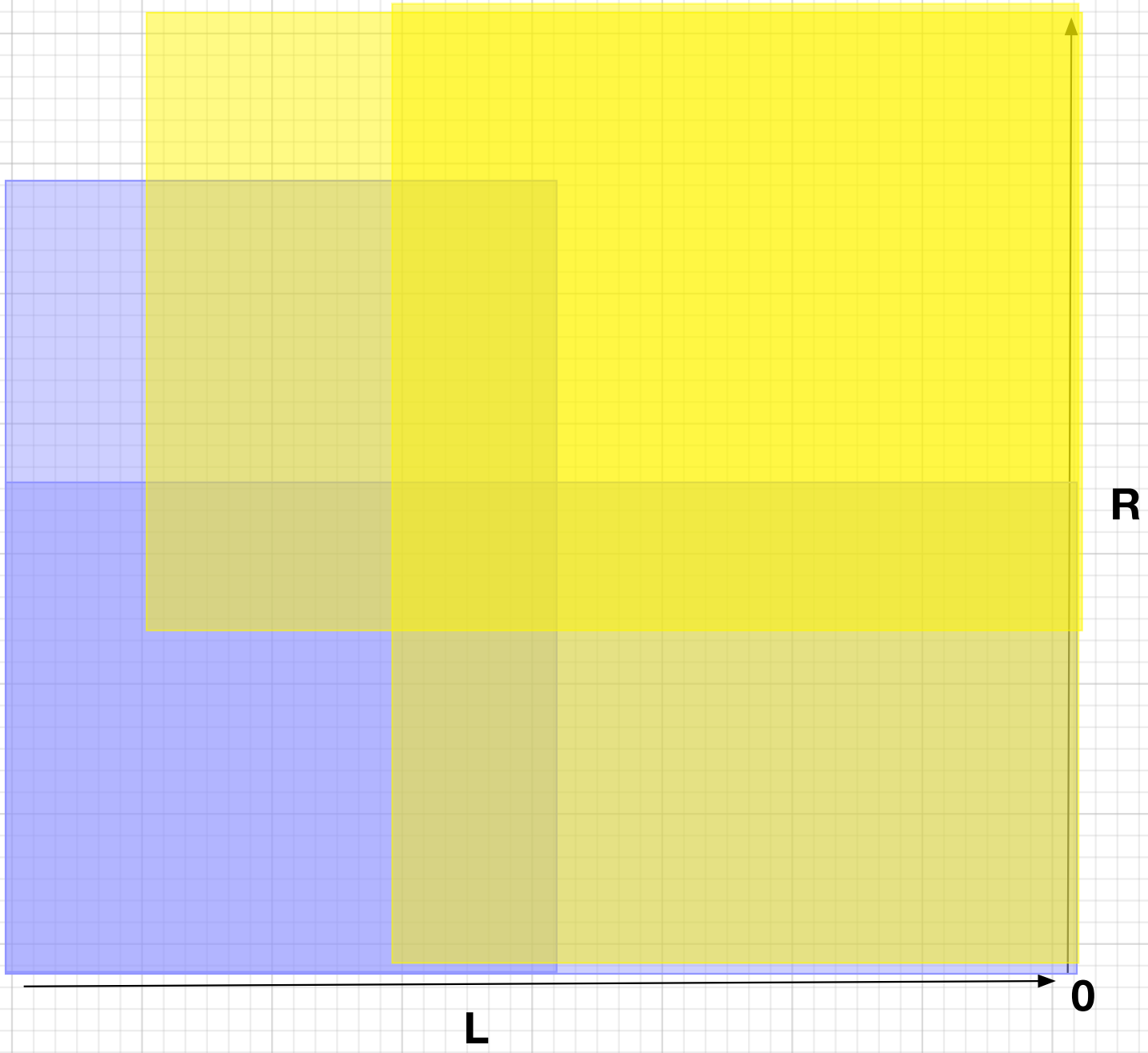
A typical deterministic strategy



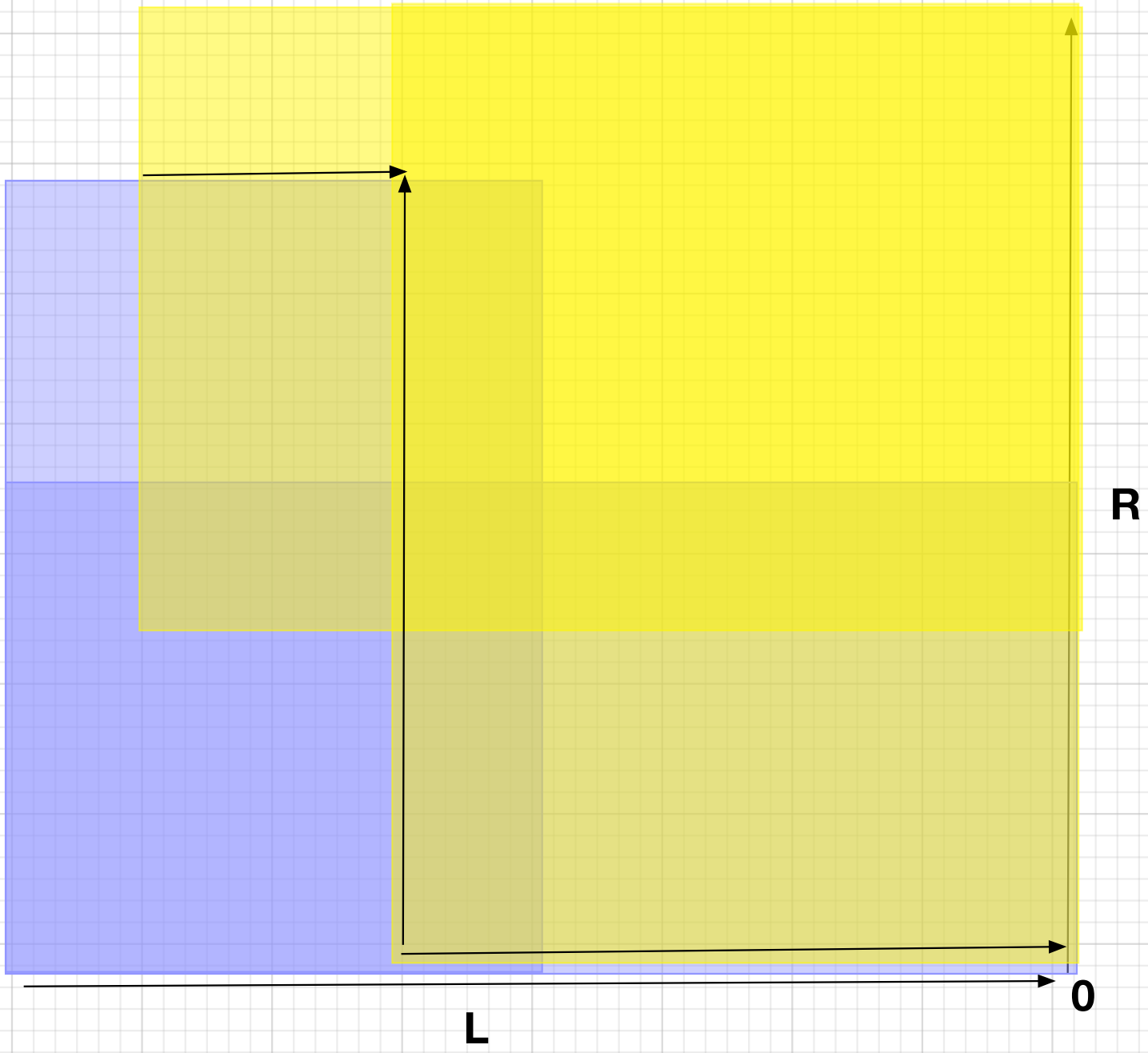
A typical deterministic counter-strategy

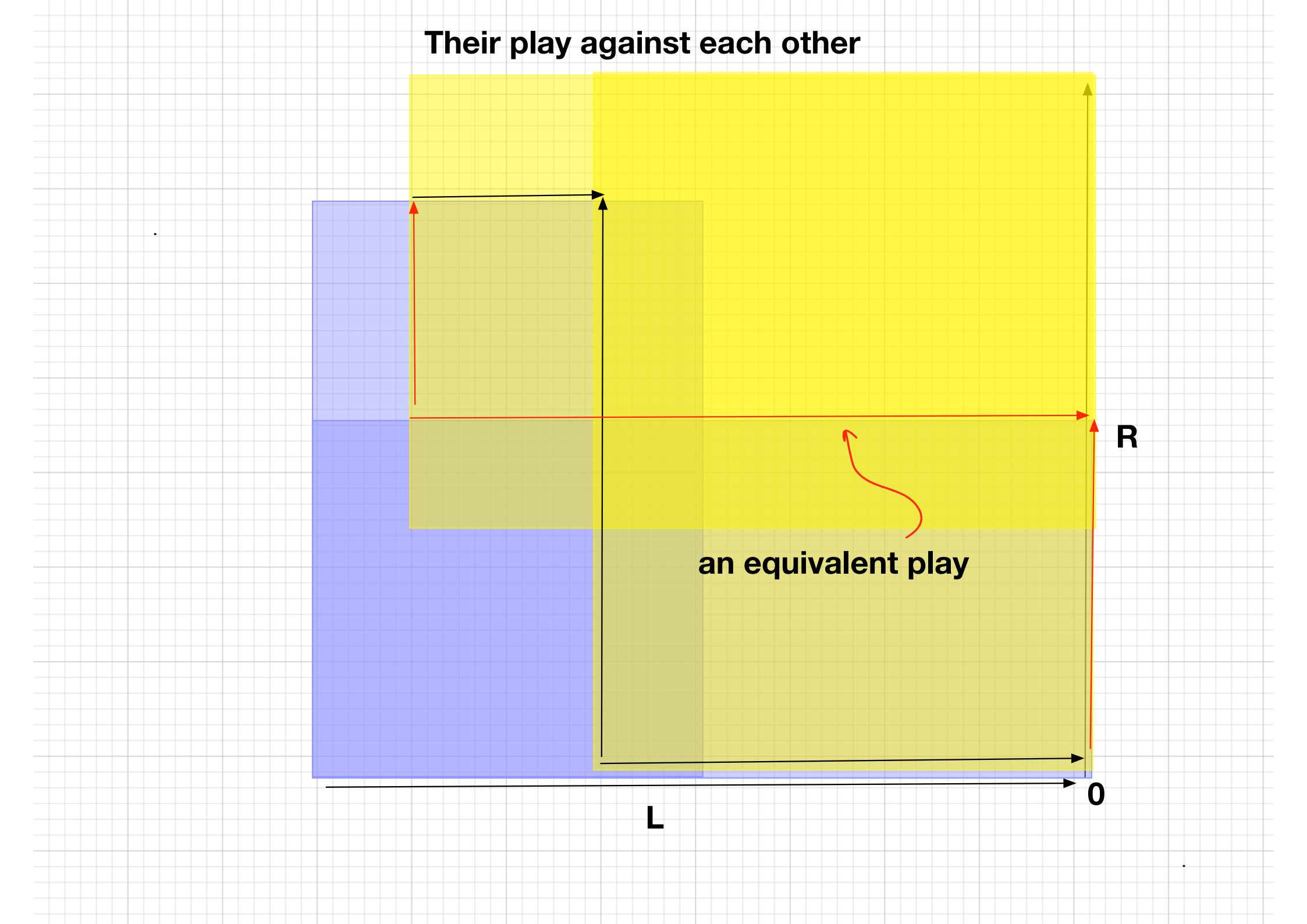


Their play against each other



Their play against each other




Their play against each other
R
an equivalent play
0
L

A similar example: the game of chase

Player: the **Hunter**, velocity vector $\mathbf{h}$; its moves are changes in velocity $\mathbf{\Delta h}$

Opponent: the **Prey**, velocity vector $\mathbf{p}$; its moves are changes in velocity $\mathbf{\Delta p}$

A strategy for Hunter (observed in people): run (towards Prey) so Prey appears to be moving in a fixed straight line (direction vector $\mathbf{d}$) from Hunter's viewpoint, *i.e.* adjust velocity to maintain the winning condition

$$\mathbf{p} - \mathbf{h} = c.\mathbf{d} \quad \text{for some non-negative real } c$$

within a game with objects (states) $(\mathbf{p}, \mathbf{h})$ and arrows
$(\mathbf{p} + \mathbf{\Delta p}, \mathbf{h}) \rightarrow_L (\mathbf{p}, \mathbf{h})$ and $(\mathbf{p}, \mathbf{h} \rightarrow_R (\mathbf{p}, \mathbf{h} + \mathbf{\Delta h}))$.

[*BBC Horizon programme "The Unconscious Mind"*]

Lessons from Robin

develop thoroughness, craftsmanship, and careful exposition

have passion for your work

cultivate cleverness, and grounded confidence, to transcend traditional boundaries

seek challenges, and freshness of thought

make research accessible to students and practitioners, write books