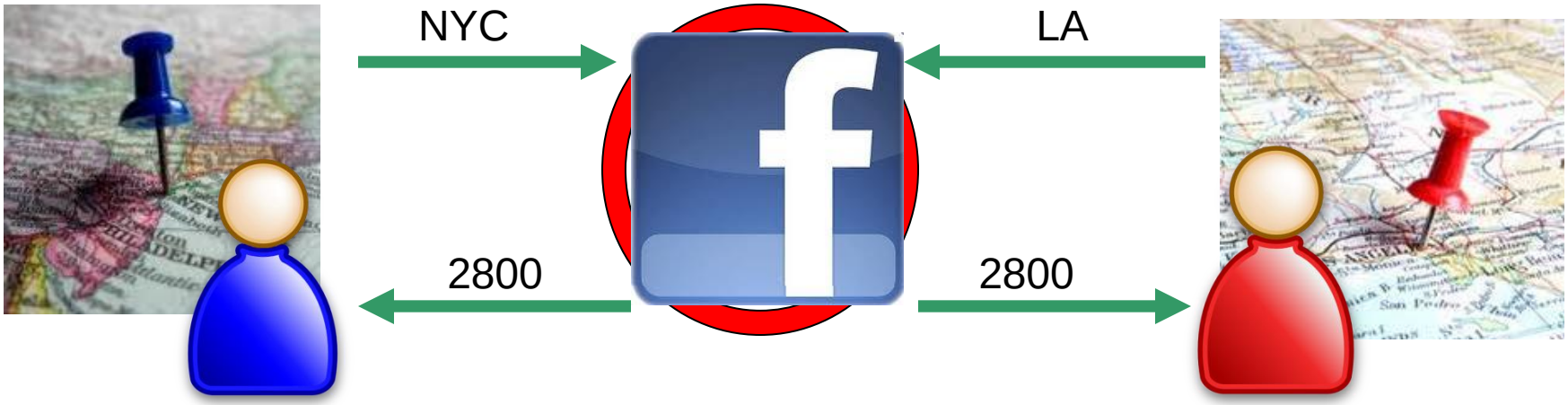
Fair Computation with Rational Players

Adam Groce and Jonathan Katz

University of Maryland

Two-party computation

Distance?



Two-party computation

Fairness: If either player learns the output, then the other player does also.

Impossible in general [Cleve86]

Dealing with this impossibility

- Fairness for specific functions [GHKL08]
- *Partial* fairness [BG89, GL90, GMPY06, MNS09, GK10], …
- Physical assumptions [LMPS04, LMS05, IML05]

- Here: assume **rational** behavior
  - Generalizing prior work on rational secret sharing [HT04, GK06, LT06, ADGH06, KN08, FKN10], …

Our results (high level)

- Consider an *ideal-world* evaluation of the function (using a trusted third party)
  - Look for a game-theoretic equilibrium in that setting

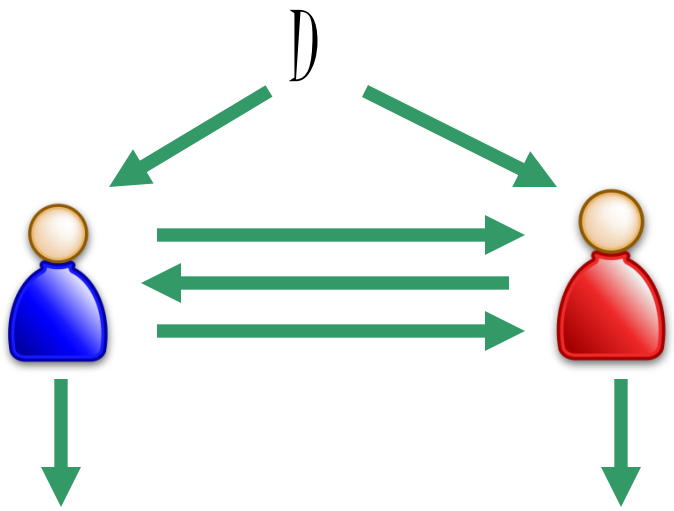
- Theorem (informal):
  If behaving honestly is a *strict* Nash equil. in the ideal world, then there is a *real-world* protocol that is fair when players are rational

Putting our result in context

- Much recent interest in combining game theory and cryptography
  - Applying game theory to cryptographic tasks (bypass impossibility, increase efficiency, …)
  - Using cryptography to remove a mediator [CS82, Forges90, Barany92, DHR00, …]
  - Defining cryptographic goals in game-theoretic terms [ACH11]
    - Had appeared to give a negative answer regarding fairness

The real-world game

1. Parties running a protocol to compute some function f
2. Receive inputs x_0, x_1 from known distribution
3. Run the protocol…
4. Output an answer
5. Utilities depend on both outputs, and the true answer $f(x_0, x_1)$

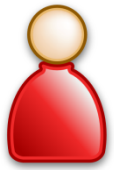


Goal

- Design a “rational fair” protocol for *f,* i.e., such that running the protocol honestly is a *computational* Nash equilibrium
  - That is, no polynomial-time player can gain more than negligible utility by deviating
- Note: stronger equilibrium notions have been considered in other cryptographic contexts
  - We leave these for future work

Asharov-Canetti-Hazay (2011)

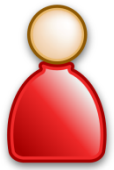
- They consider a special case of our real-world game (with different motivation):
  - Uniform, independent binary inputs x_0 and x_1
  - Computing XOR
  - Utilities given by:
- Results:
  - There exists a rational protocol with correctness ½
  - No rational protocol can be correct with probability better than ½



	Right	Wrong
Right	(0, 0)	(1, -1)
Wrong	(-1, 1)	(0, 0)

Asharov-Canetti-Hazay (2011)

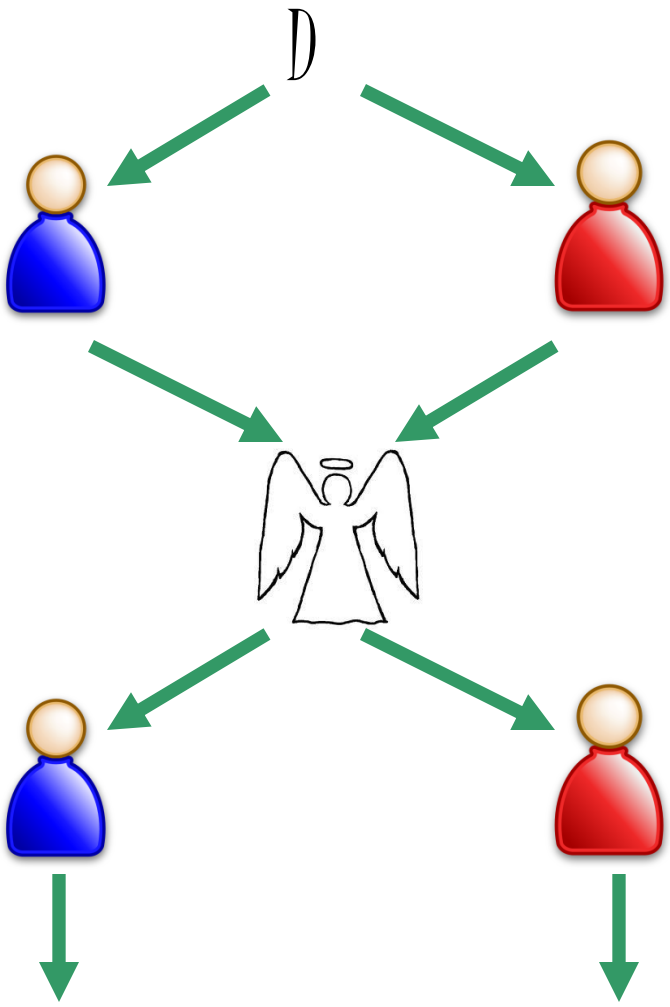
- But wait!
  - Guessing randomly is also an equilibrium…
  - …and achieves the same payoff as *any possible* protocol (even with a trusted party)
  - Parties may as well not run the protocol at all!



	Right	Wrong
Right	(0, 0)	(1, -1)
Wrong	(-1, 1)	(0, 0)

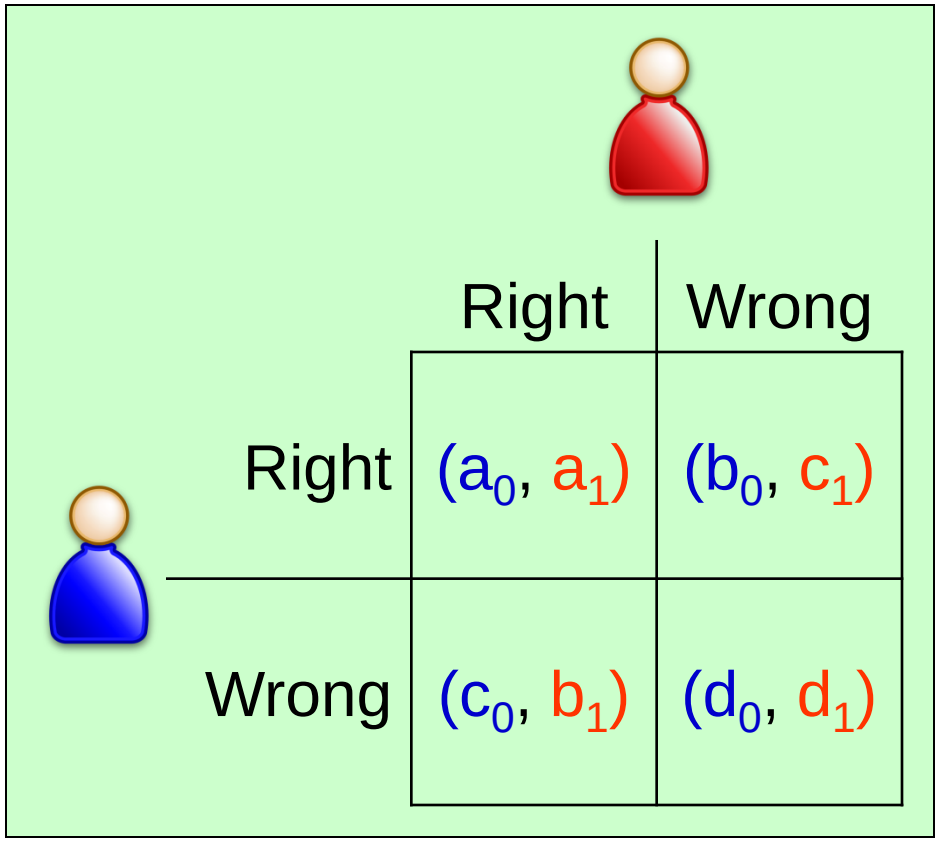
The ideal-world game

1. Receive inputs x_0, x_1 from known distribution
2. Send an input (or $\perp$) to the ideal functionality
3. Receive an output (or $\perp$) from the functionality
4. Output an answer
5. Utilities depend on both outputs, and the true answer $f(x_0, x_1)$



Utilities

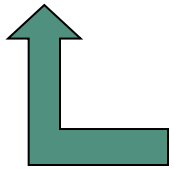
Payoff Matrix



(Assume $b > a \geq d \geq c$)

Honest strategy of P_0 (ideal world)

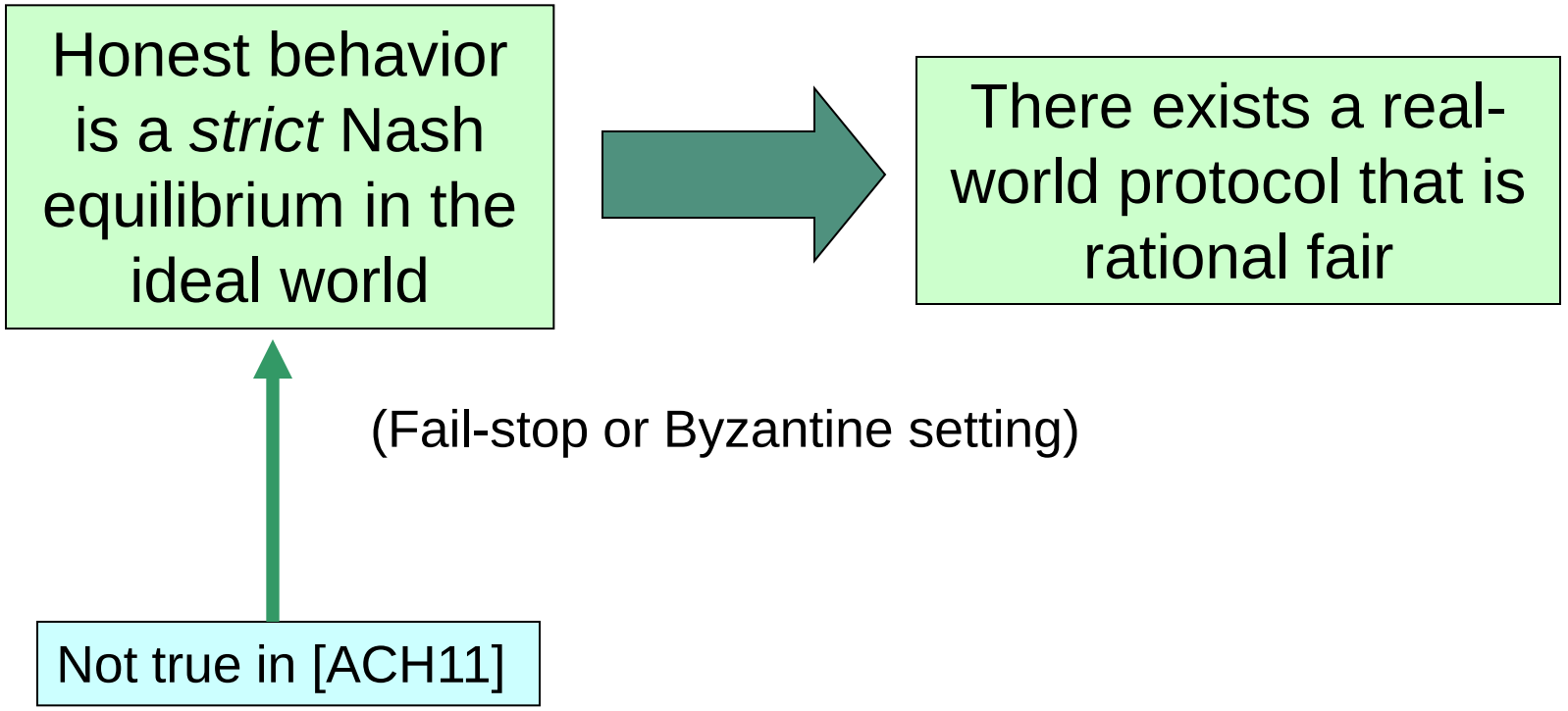
- Send true input x_0 to functionality
- Output the answer given by the functionality
- If functionality gives $\perp$, generate output according to distribution $W_0(x_0)$



Not used in an honest execution, but must exist.

We can assume $W_0(x_0)$ has full support.

Our result


Honest behavior is a *strict* Nash equilibrium in the ideal world
There exists a real-world protocol that is rational fair
(Fail-stop or Byzantine setting)
Not true in [ACH11]

Our protocol I

Use ideas from [GHKL08, MNS09, GK10]

ShareGen

- Choose i* from geometric distribution with parameter p
- For each i ≤ n, create values $r_{i,0}$ and $r_{i,1}$
  - If i ≥ i*, $r_{i,0}$ and $r_{i,1}$ are the desired outputs
  - If i < i*, $r_{i,0}$ and $r_{i,1}$ are chosen according to distributions $W_0(x_0)$ and $W_1(x_1)$
- Secret-share each $r_{i,j}$ value; give one share to P_0 and the other to P_1

Our protocol II

- Compute ShareGen (unfairly)
- In round i, parties exchange shares
  - P_0 learns $r_{i,0}$ and P_1 learns $r_{i,1}$
- If the other player aborts early, output the last value learned
- If the protocol finishes, output $r_{n,0}$ and $r_{n,1}$

Analysis – will P_0 abort early?

Assume P_0 is notified once i* has passed

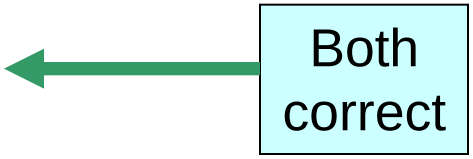
Aborting after this point cannot help

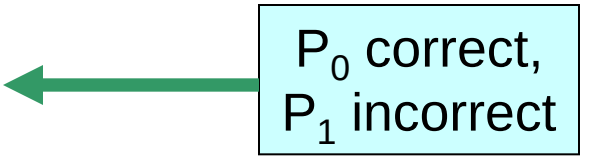
If P_0 doesn't abort early → utility a_0

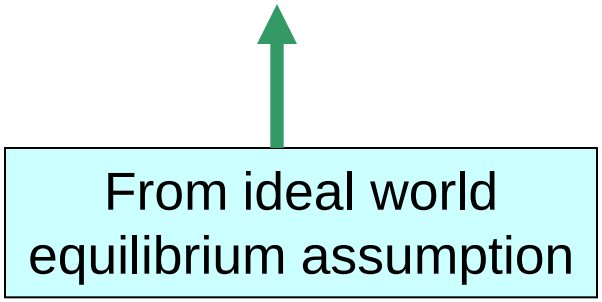
If P_0 aborts early….

… in round i* → utility b_0

… before round i* → utility strictly less than a_0

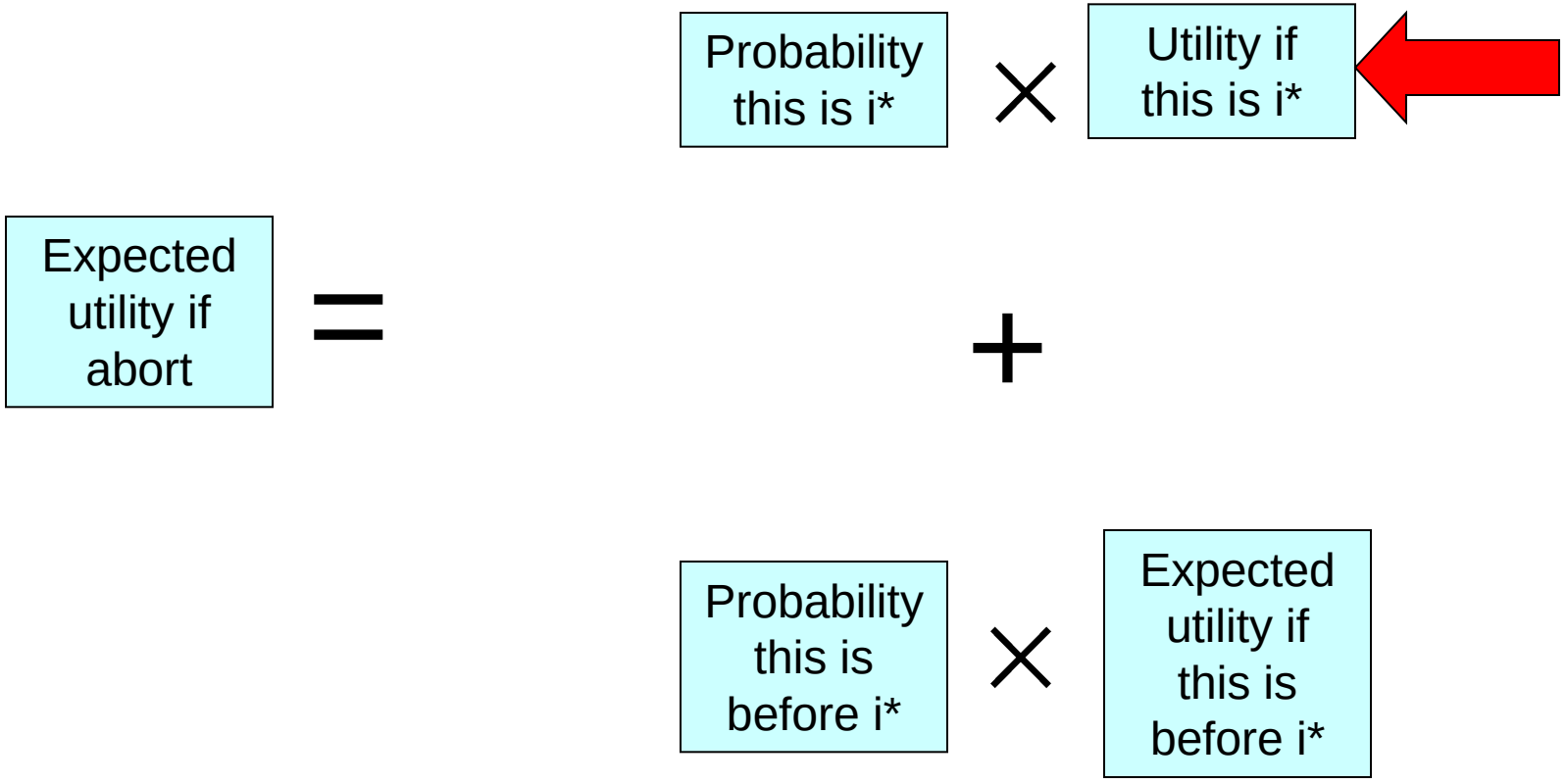






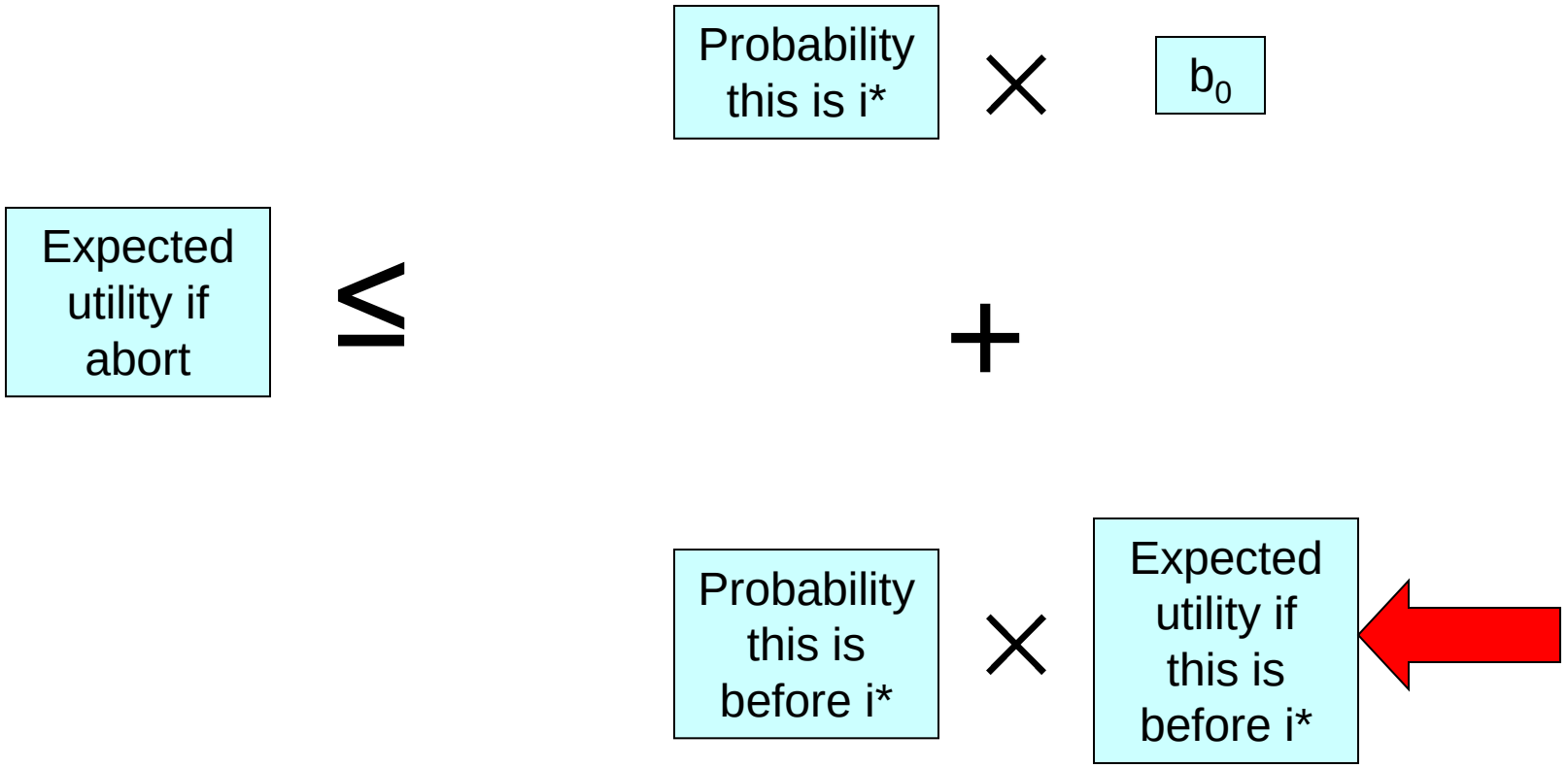
Analysis – will P_0 abort early?

When P_0 sees output y in round i:



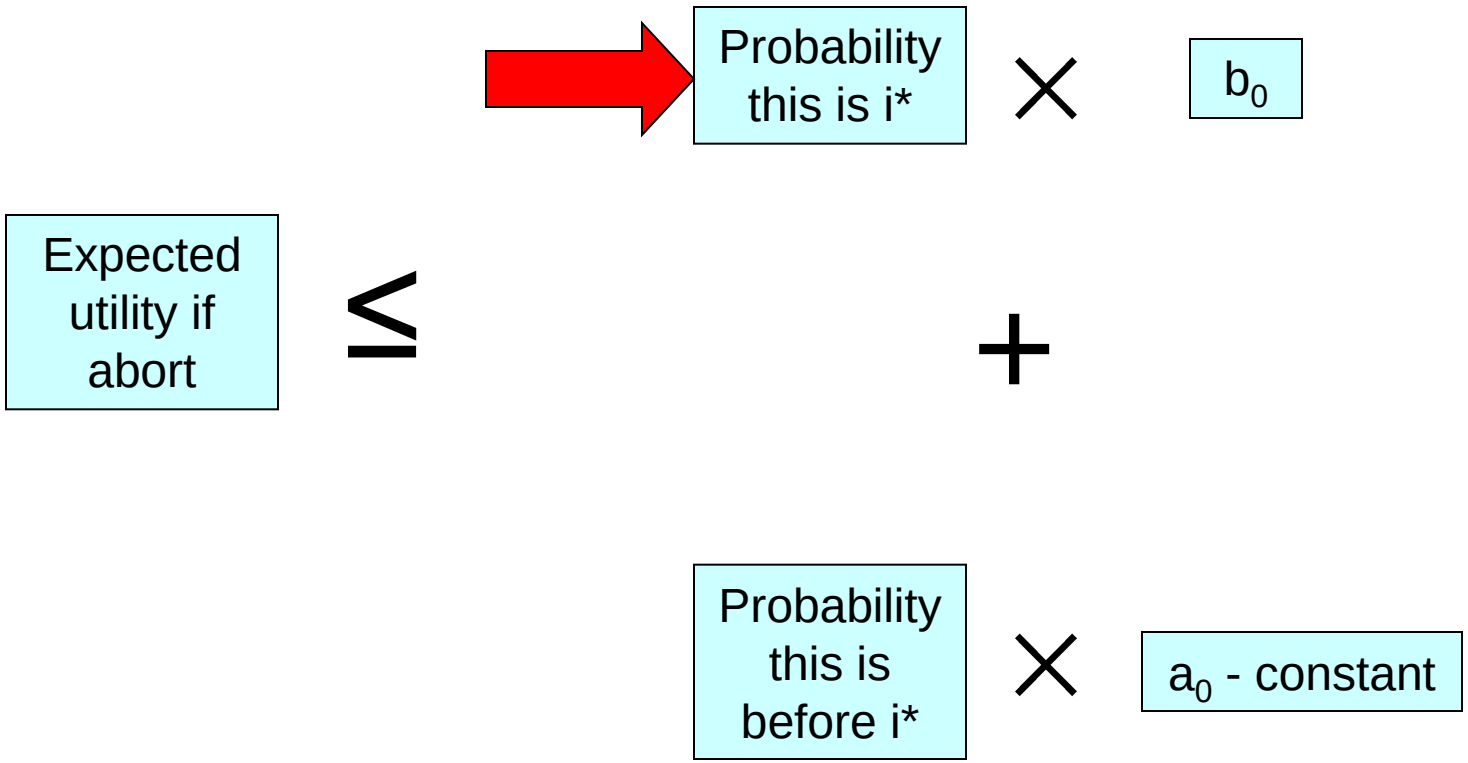
Analysis – Will P_0 abort early?

When P_0 sees output y in round i:



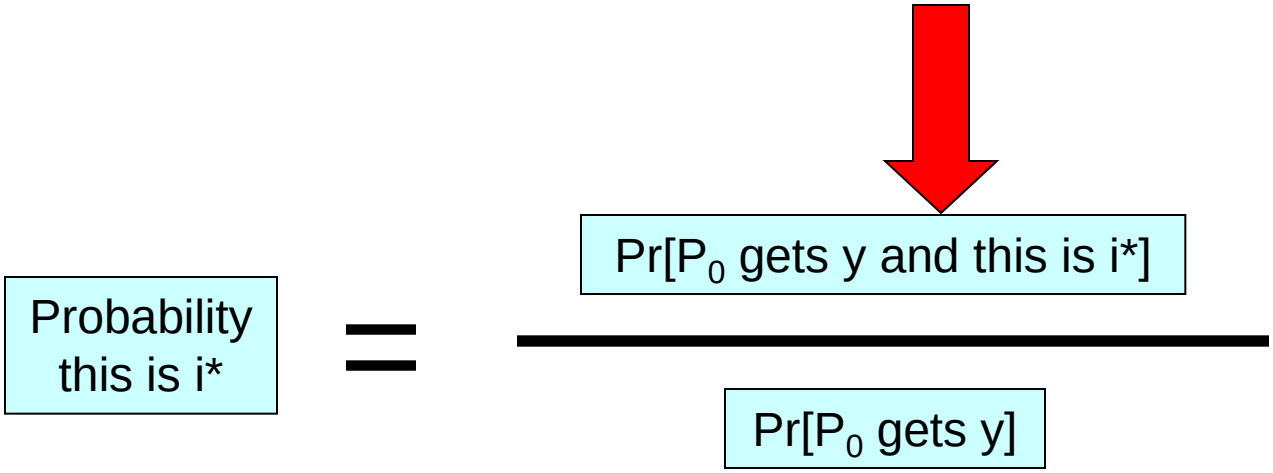
Analysis – Will P_0 abort early?

When P_0 sees output y in round i:



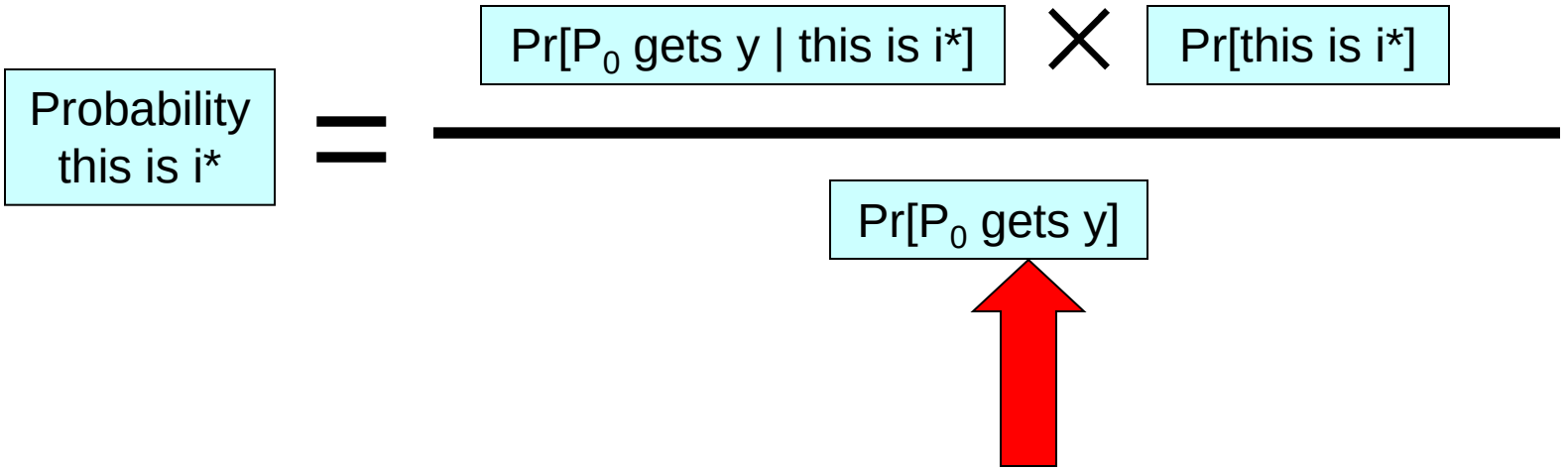
Analysis – Will P_0 abort early?

When P_0 sees output y in round i:



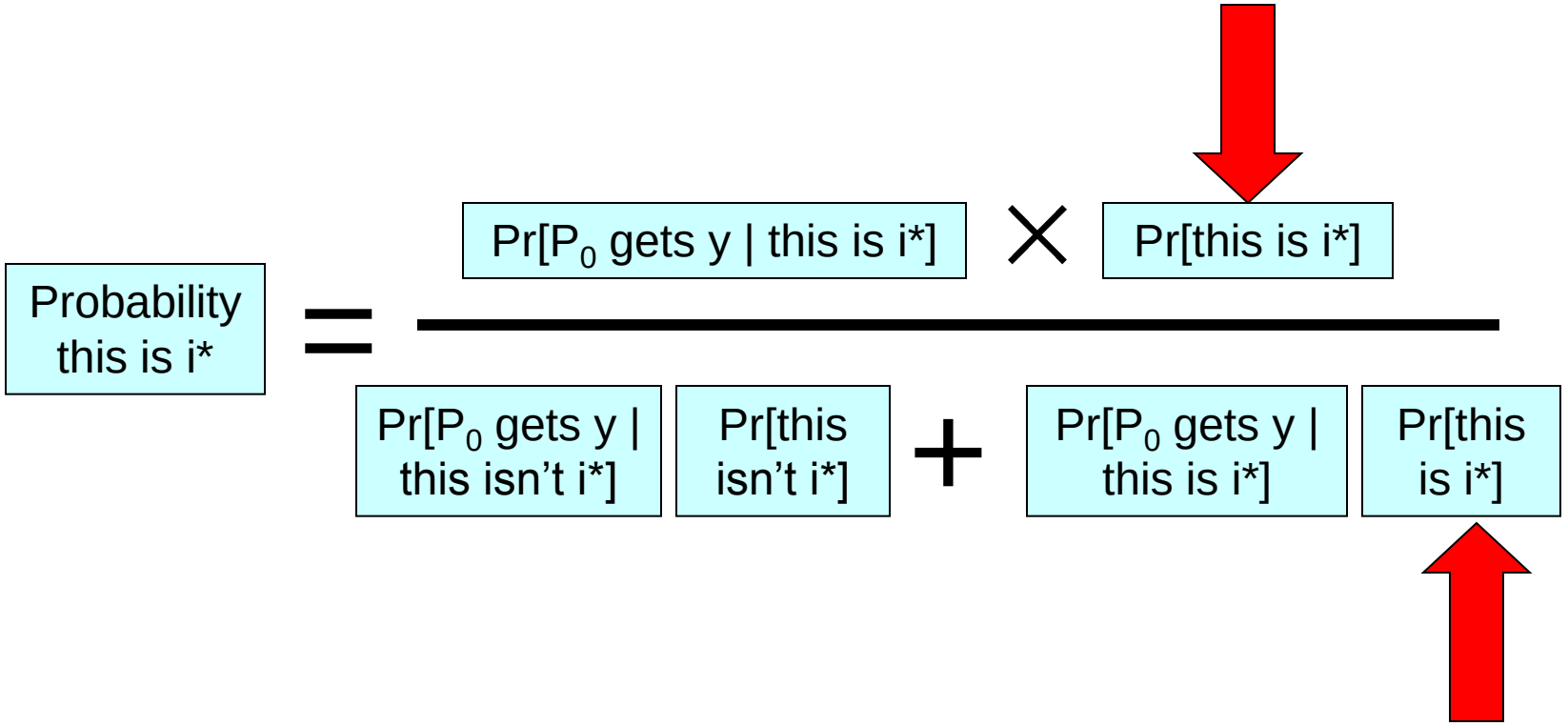
Analysis – Will P_0 abort early?

When P_0 sees output y in round i:



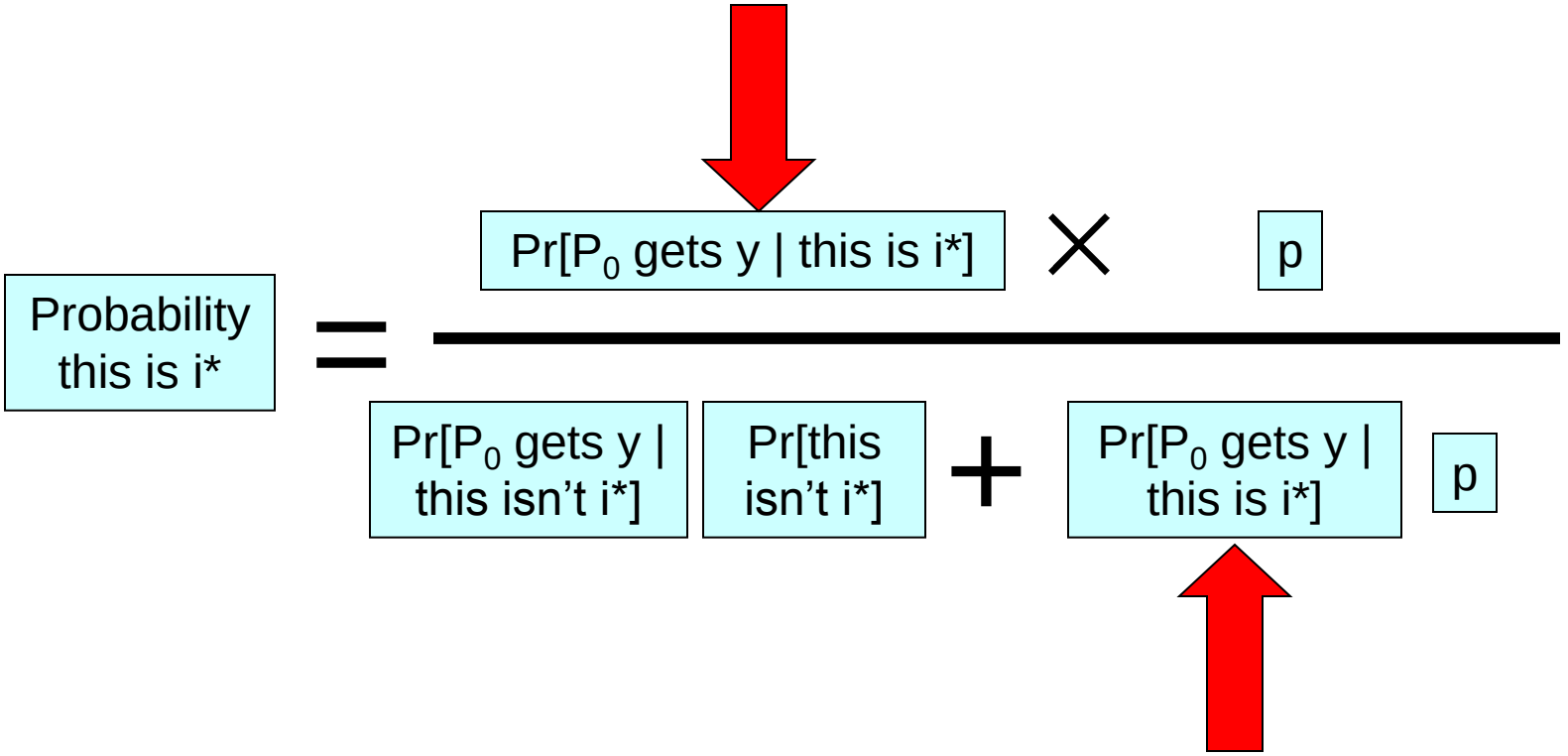
Analysis – Will P_0 abort early?

When P_0 sees output y in round i:



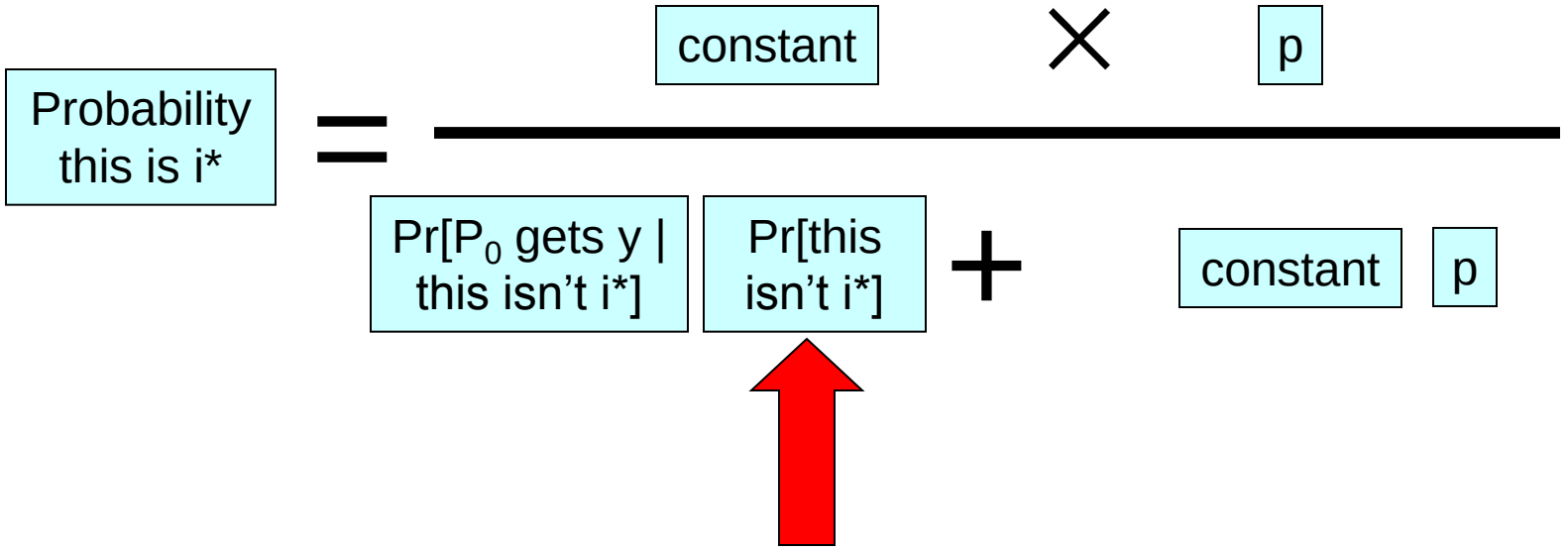
Analysis – Will P_0 abort early?

When P_0 sees output y in round i:



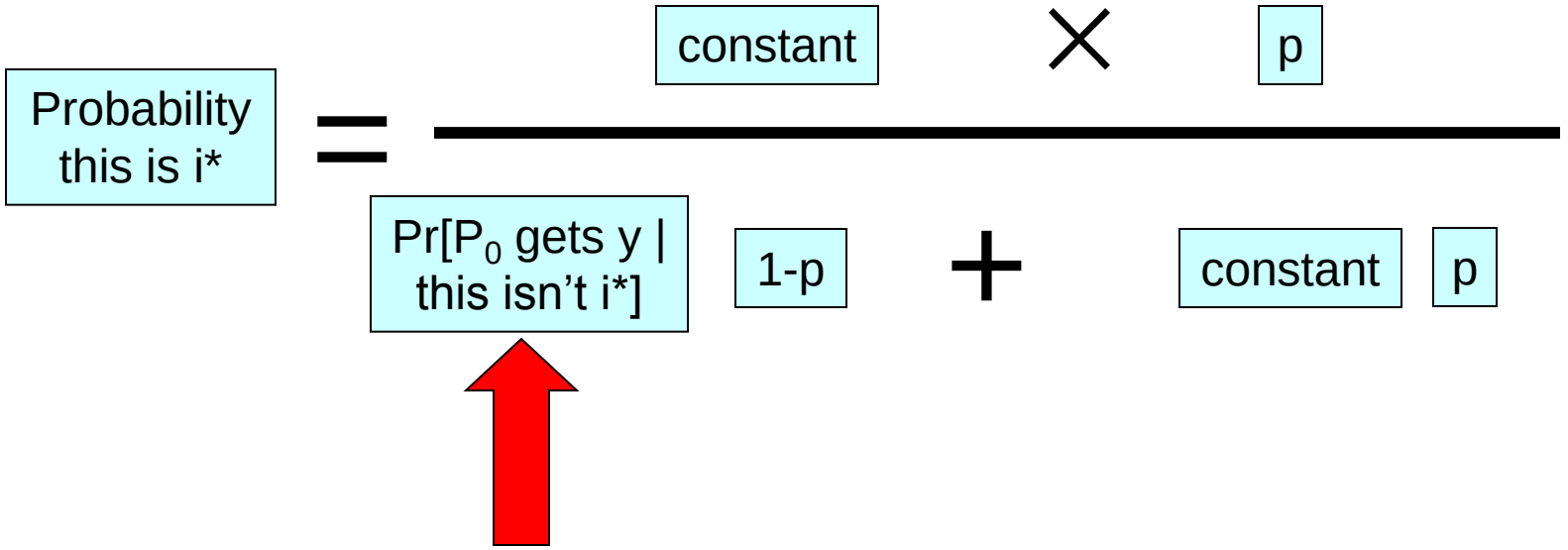
Analysis – Will P_0 abort early?

When P_0 sees output y in round i:



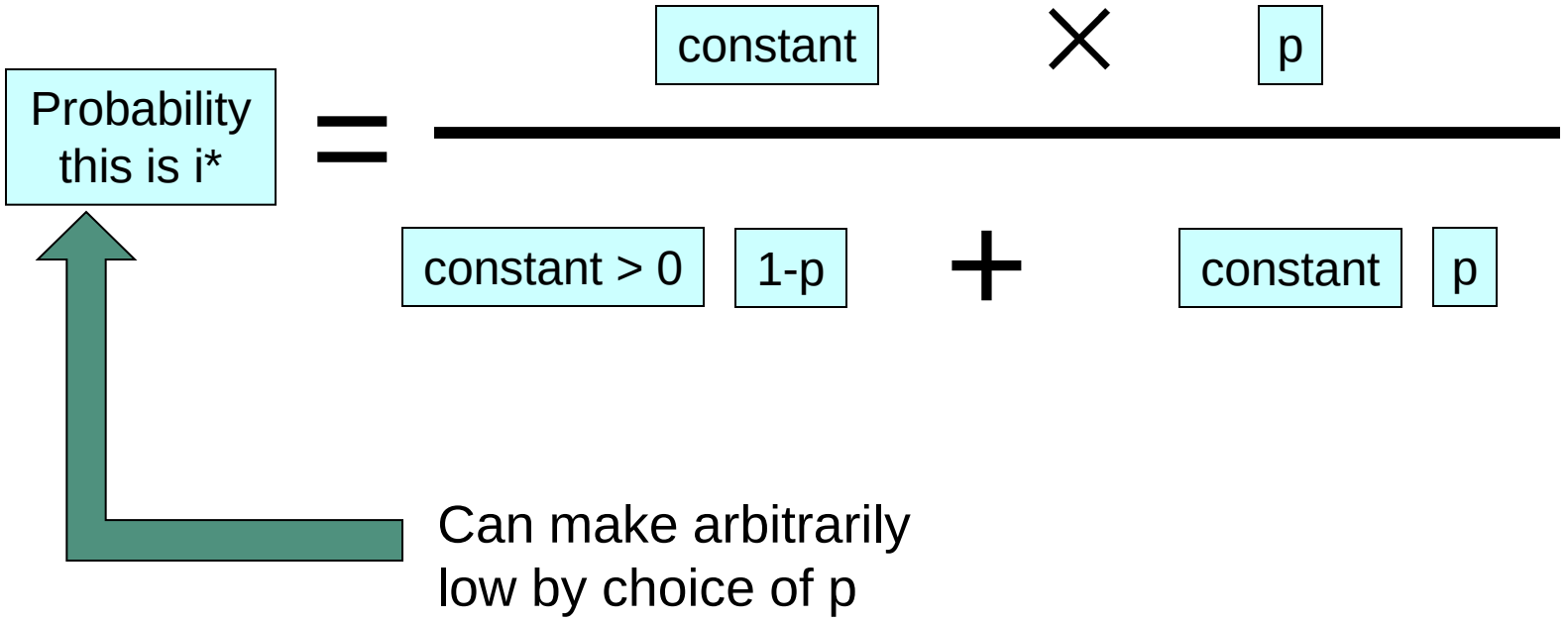
Analysis – Will P_0 abort early?

When P_0 sees output y in round i:



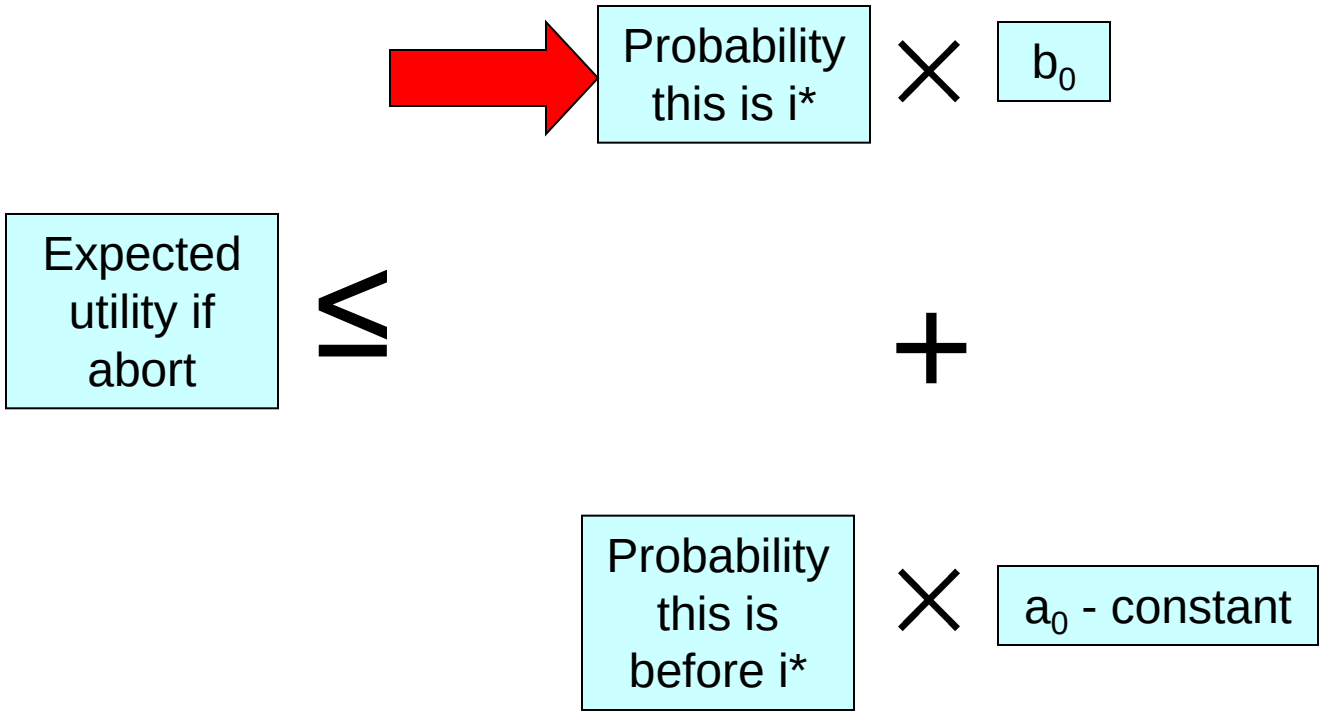
Analysis – Will P_0 abort early?

When P_0 sees output y in round i:



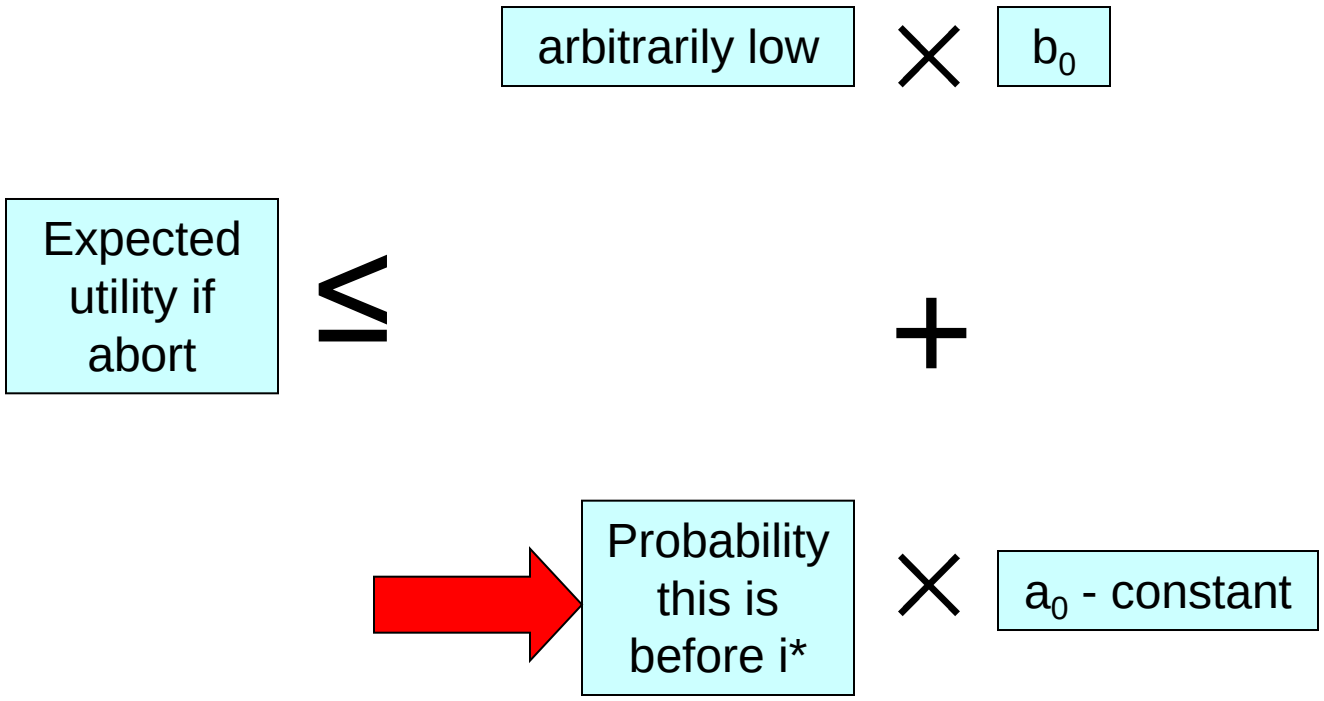
Analysis – Will P_0 abort early?

When P_0 sees output y in round i:



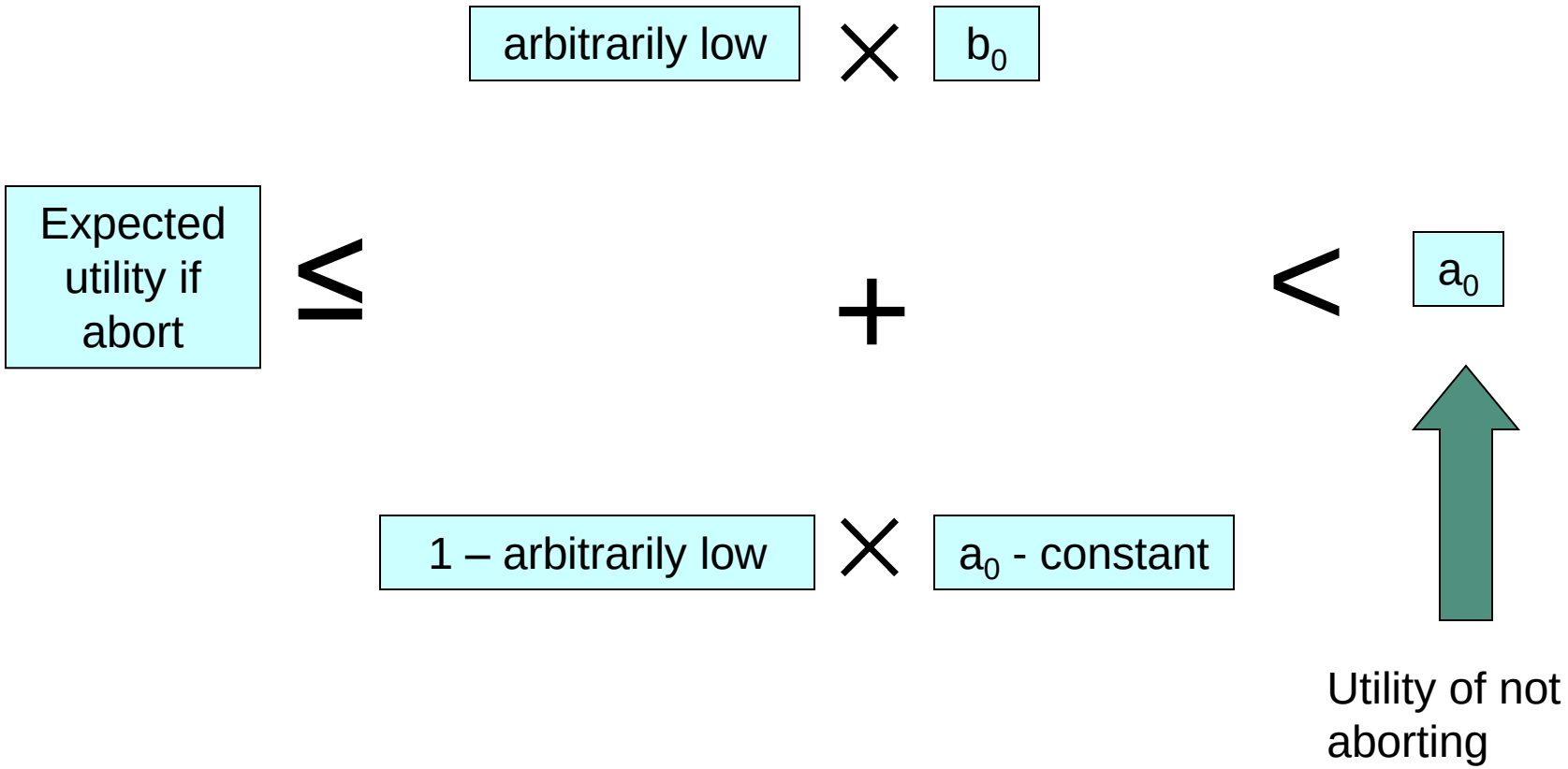
Analysis – Will P_0 abort early?

When P_0 sees output y in round i:



Analysis – Will P_0 abort early?

When P_0 sees output y in round i:



Conclusion

- Rational fairness is possible!
  - As long as there is a strict preference for fairness in the ideal world (by at least one of the parties)
- The more pronounced parties' preferences are, the more round-efficient the real-world protocol is

Extensions and open problems

- Multi-party case, more general utilities
  - Recent work with Amos Beimel and Ilan Orlov
- Open:
  - Prove a (partial?) converse of our result
  - Consider stronger notions of equilibrium in the real world
  - Address other concerns besides fairness?

Thank you