



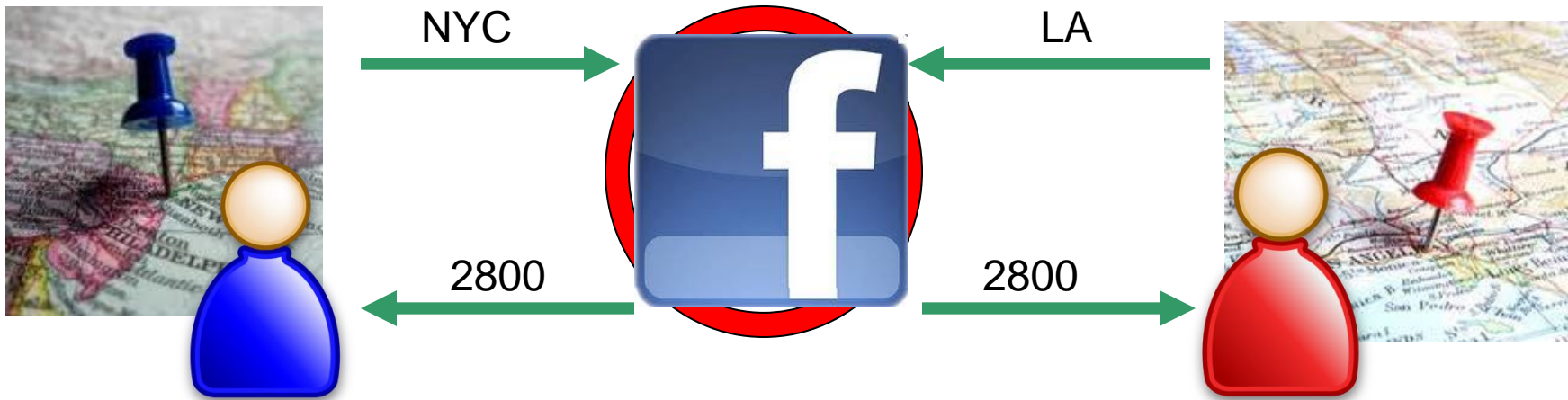
Fair Computation with Rational Players



Adam Groce and Jonathan Katz
University of Maryland

Two-party computation

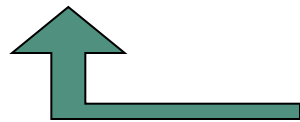
Distance?



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):

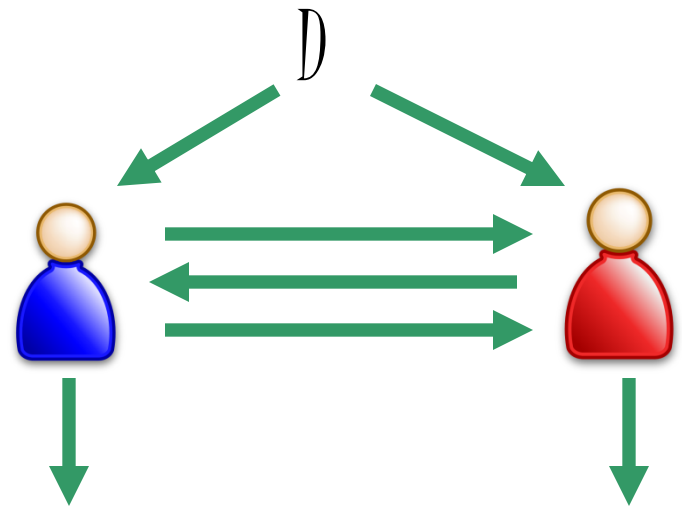
If behaving honestly is a *strict* Nash equil. in the ideal world, then there is a *real-world* protocol that is fair when players are rational

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

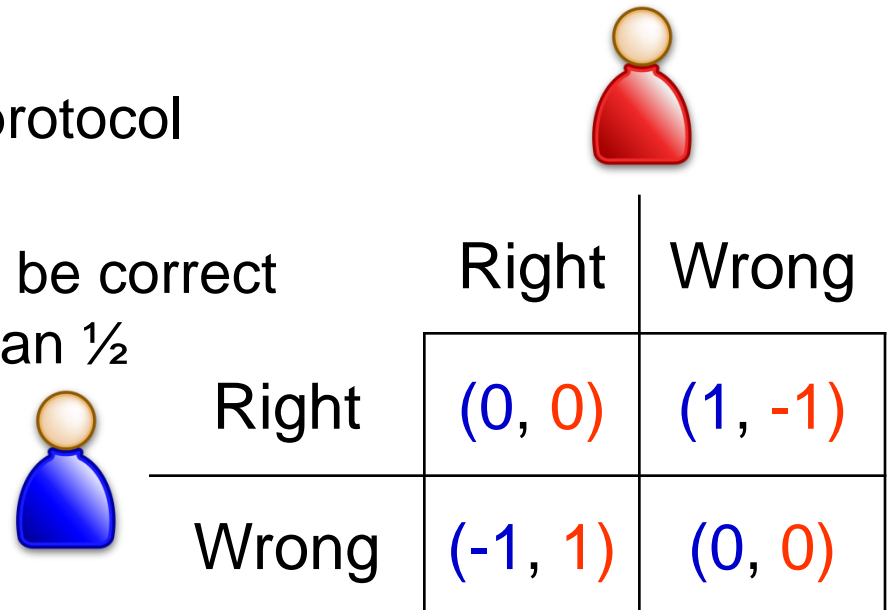
- Design a “rational fair” protocol for f , i.e., such that running the protocol honestly is a *computational* Nash equilibrium
 - That is, no polynomial-time player can gain more than negligible utility by deviating
- Note: stronger equilibrium notions have been considered in other cryptographic contexts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

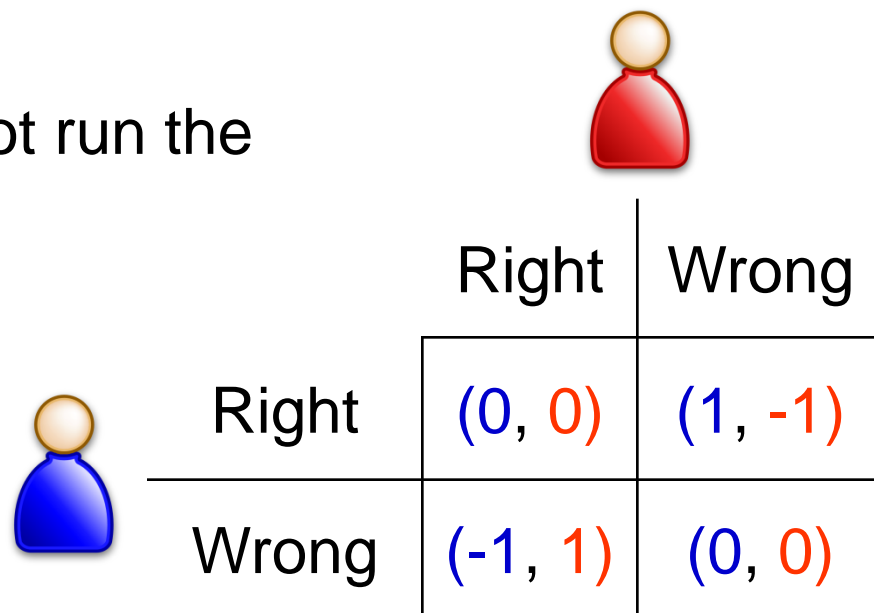
- There exists a rational protocol with correctness $\frac{1}{2}$
- No rational protocol can be correct with probability better than $\frac{1}{2}$

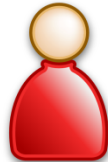
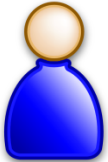


| | |  | |
|---|-------|---|---------|
| | | Right | Wrong |
|  | Right | (0, 0) | (1, -1) |
| | Wrong | (-1, 1) | (0, 0) |

Asharov-Canetti-Hazay (2011)

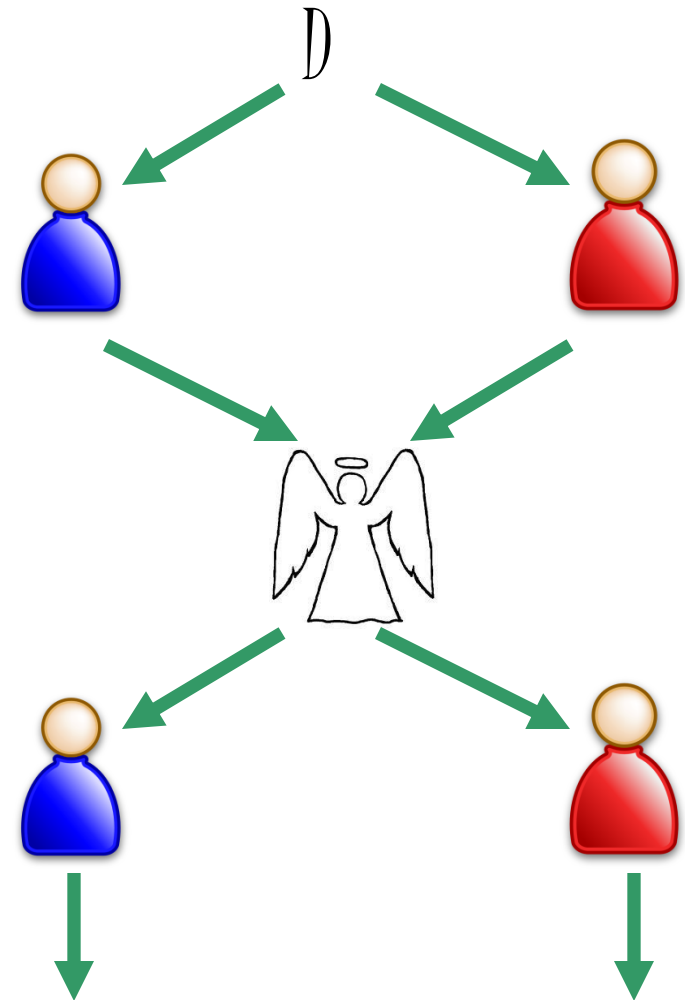
- But wait!
 - Guessing randomly is also an equilibrium...
 - ...and achieves the same payoff as *any possible* protocol (even with a trusted party)
 - Parties may as well not run the protocol at all!



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

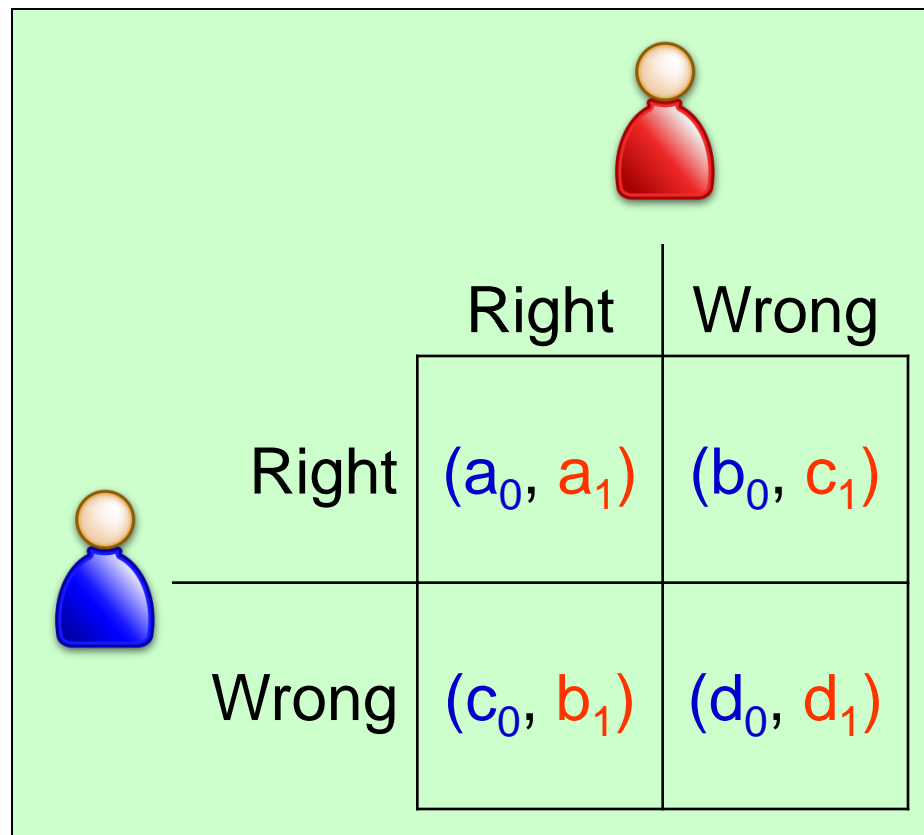
The ideal-world game

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



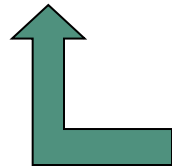
A payoff matrix diagram illustrating a game between two players. The matrix is set against a light green background. At the top center is a red player icon. To the left of the matrix is a blue player icon. The matrix is divided into four quadrants by a horizontal and a vertical line. The columns are labeled 'Right' and 'Wrong' at the top. The rows are labeled 'Right' and 'Wrong' on the left. The payoffs are given as ordered pairs (Player 1, Player 2) in each cell.

| | Right | Wrong |
|-------|--------------|--------------|
| Right | (a_0, a_1) | (b_0, c_1) |
| Wrong | (c_0, b_1) | (d_0, d_1) |

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

Honest strategy of P_0 (ideal world)

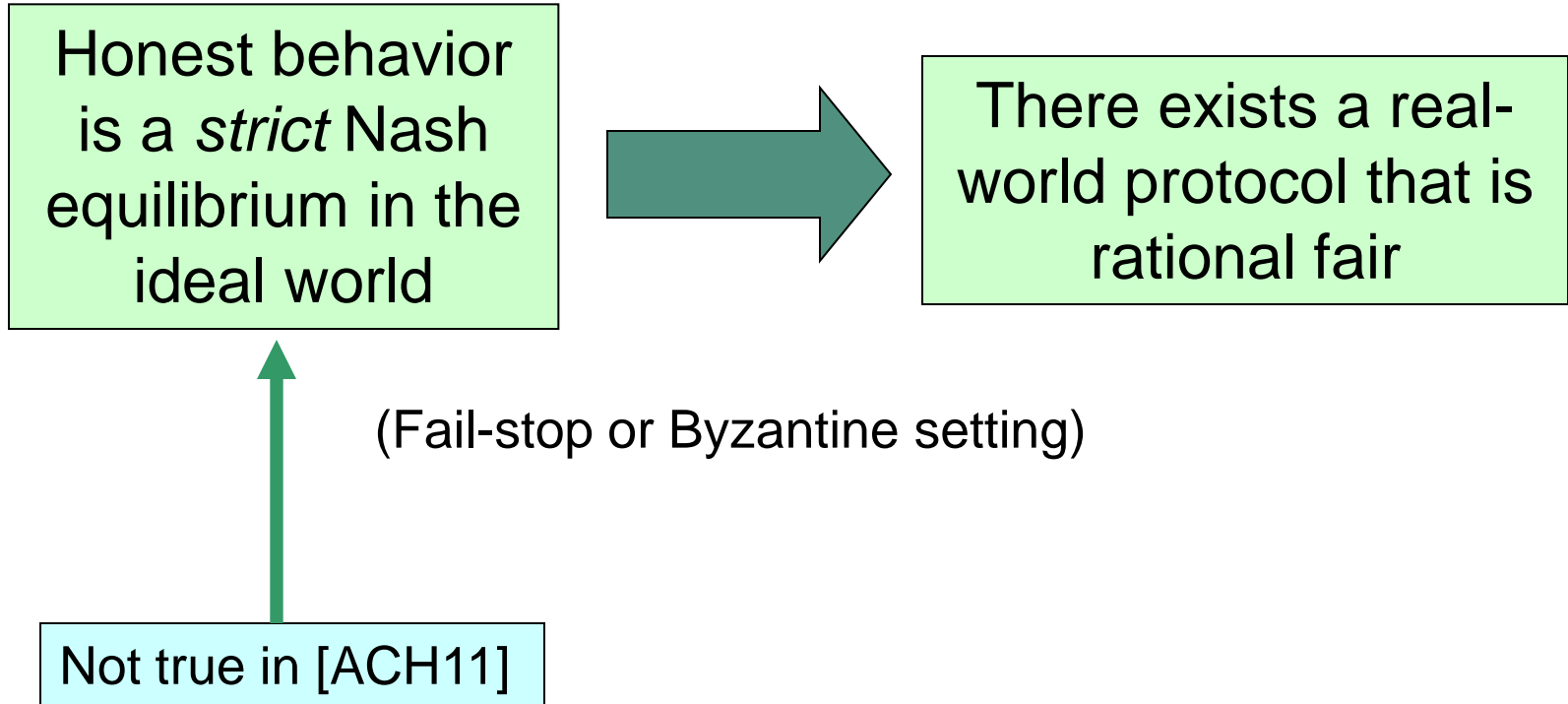
- Send true input x_0 to functionality
- Output the answer given by the functionality
- If functionality gives \perp , generate output according to distribution $W_0(x_0)$



Not used in an honest execution, but must exist.

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

Our result



Our protocol I

Use ideas from [GHKL08, MNS09, GK10]

ShareGen

- Choose i^* from geometric distribution with parameter p
- For each $i \leq n$, create values $r_{i,0}$ and $r_{i,1}$
 - If $i \geq i^*$, $r_{i,0}$ 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 \rightarrow utility a_0

Both correct

If P_0 aborts early....

... in round i^* \rightarrow utility b_0

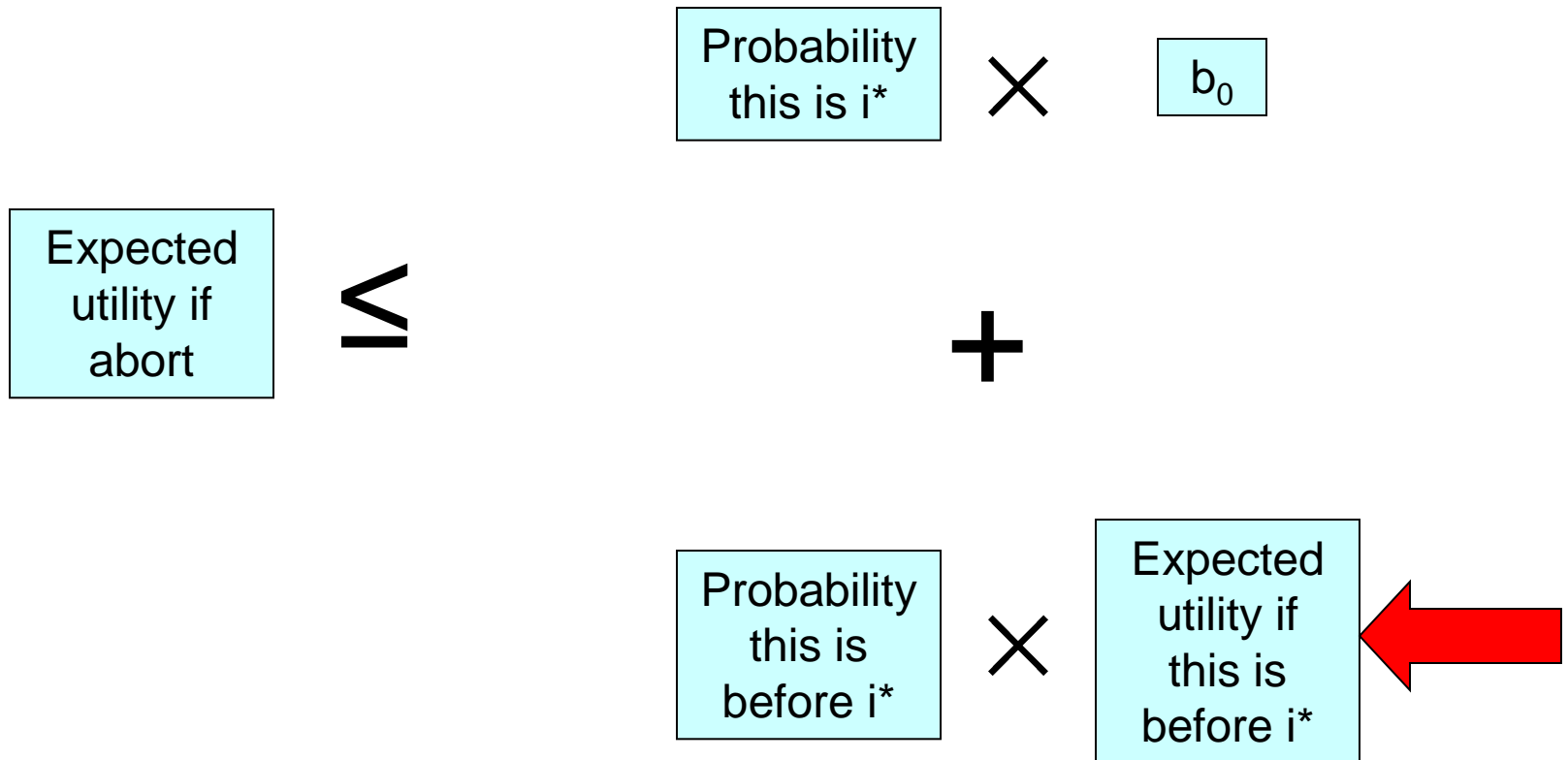
P_0 correct,
 P_1 incorrect

... before round i^* \rightarrow utility strictly less than a_0

From ideal world
equilibrium assumption

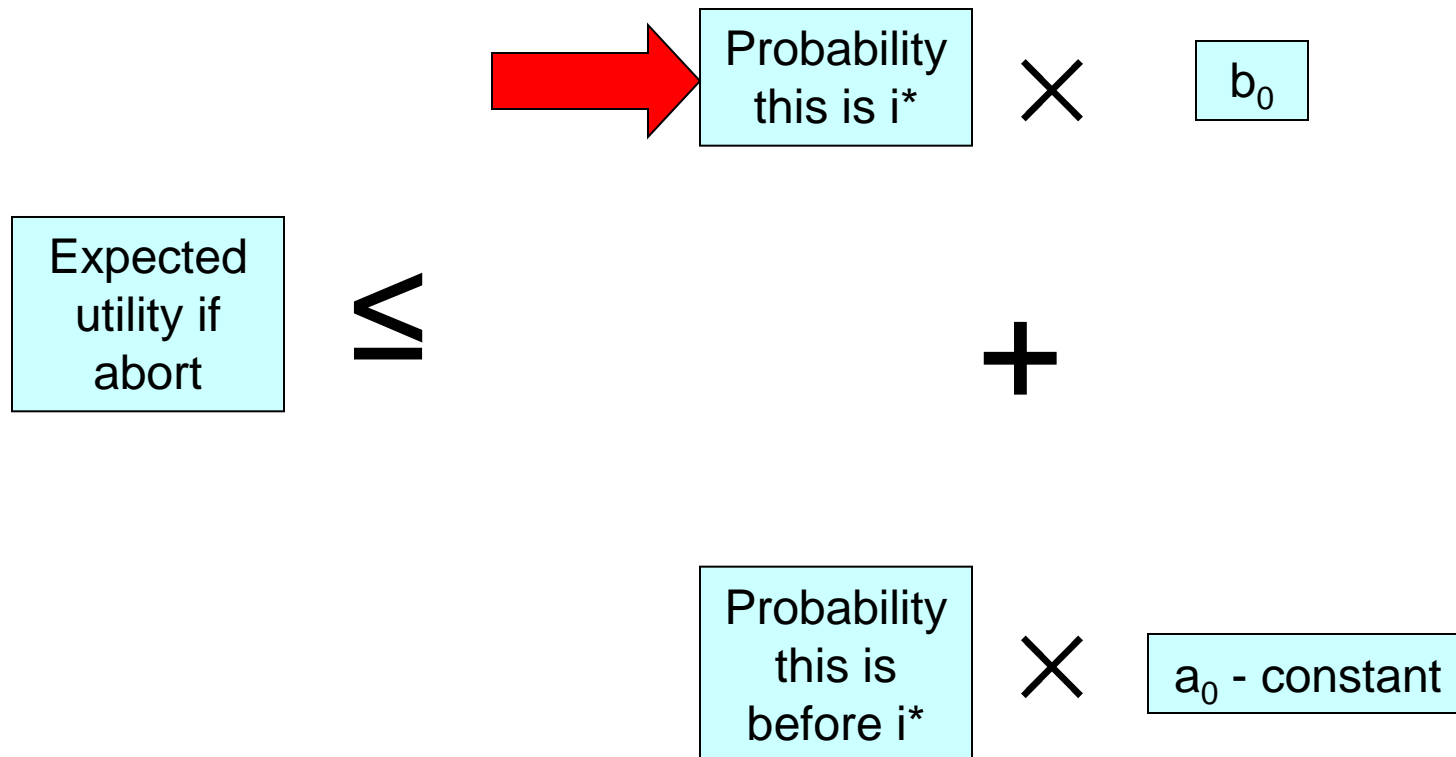
Analysis – Will P_0 abort early?

When P_0 sees output y in round i :



Analysis – Will P_0 abort early?

When P_0 sees output y in round i :



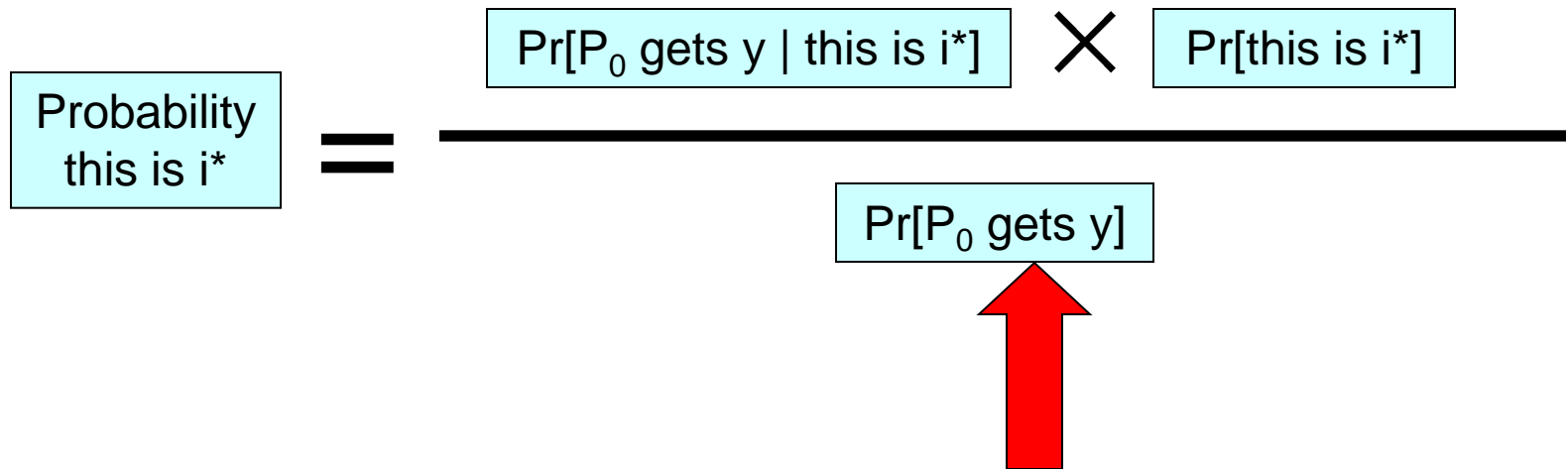
Analysis – Will P_0 abort early?

When P_0 sees output y in round i :

$$\text{Probability this is } i^* = \frac{\Pr[P_0 \text{ gets } y \text{ and this is } i^*]}{\Pr[P_0 \text{ gets } y]}$$

Analysis – Will P_0 abort early?

When P_0 sees output y in round i :

$$\text{Probability this is } i^* = \frac{\text{Pr}[P_0 \text{ gets } y \mid \text{this is } i^*] \times \text{Pr}[\text{this is } i^*]}{\text{Pr}[P_0 \text{ gets } y]}$$


Analysis – Will P_0 abort early?

When P_0 sees output y in round i :

$$\begin{array}{c} \text{Probability} \\ \text{this is } i^* \end{array} = \frac{\text{Pr}[P_0 \text{ gets } y \mid \text{this is } i^*] \times \text{Pr}[\text{this is } i^*]}{\text{Pr}[P_0 \text{ gets } y \mid \text{this isn't } i^*] \text{Pr}[\text{this isn't } i^*] + \text{Pr}[P_0 \text{ gets } y \mid \text{this is } i^*] \text{Pr}[\text{this is } i^*]}$$

The diagram illustrates the total probability of P_0 seeing output y in round i . It is represented as a fraction where the numerator is the product of the conditional probability of seeing y given that the round is i^* and the probability of the round being i^* . The denominator is the sum of two terms: the product of the conditional probability of seeing y given that the round is not i^* and the probability of the round not being i^* , plus the product of the conditional probability of seeing y given that the round is i^* and the probability of the round being i^* . A red arrow points down to the $\text{Pr}[\text{this is } i^*]$ term in the numerator, and another red arrow points up to the $\text{Pr}[\text{this is } i^*]$ term in the denominator.

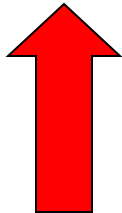
Analysis – Will P_0 abort early?

When P_0 sees output y in round i :

$$\begin{aligned} \text{Probability this is } i^* &= \frac{\Pr[P_0 \text{ gets } y \mid \text{this is } i^*] \times p}{\Pr[P_0 \text{ gets } y \mid \text{this isn't } i^*] \Pr[\text{this isn't } i^*] + \Pr[P_0 \text{ gets } y \mid \text{this is } i^*] p} \end{aligned}$$

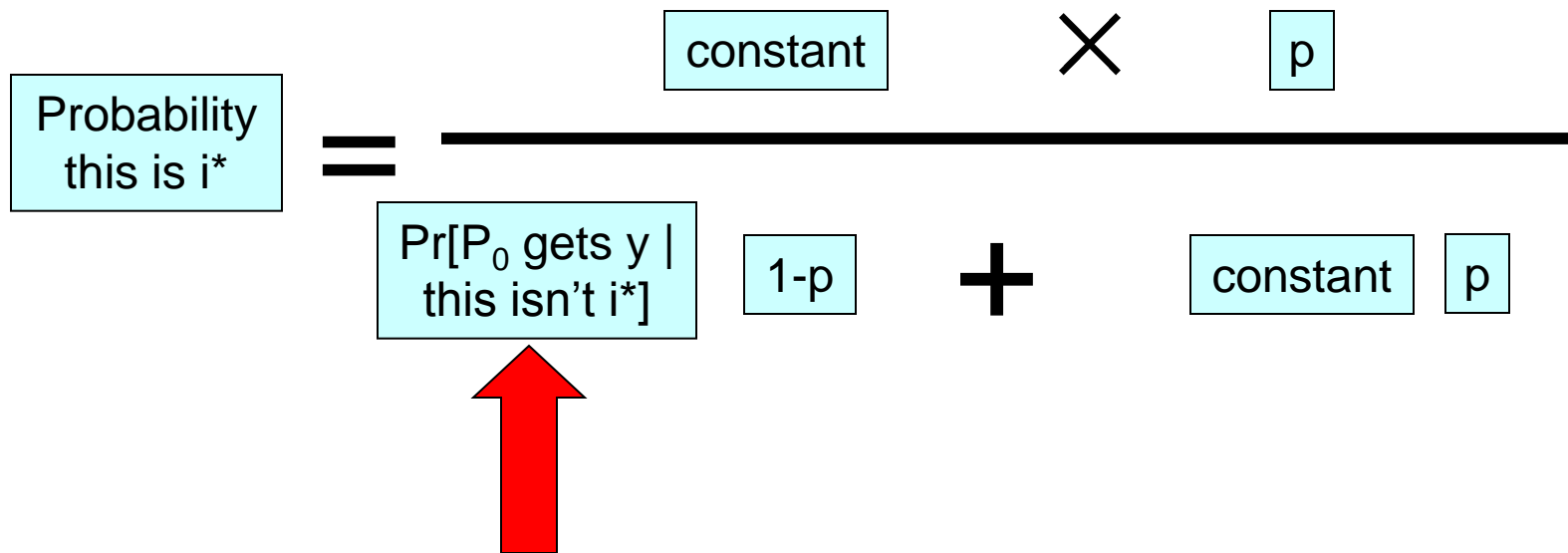
Analysis – Will P_0 abort early?

When P_0 sees output y in round i :

$$\begin{array}{c} \text{Probability} \\ \text{this is } i^* \end{array} = \frac{\text{constant} \times p}{\text{Pr}[P_0 \text{ gets } y \mid \text{this isn't } i^*] + \text{Pr}[\text{this isn't } i^*] + \text{constant} \times p}$$


Analysis – Will P_0 abort early?

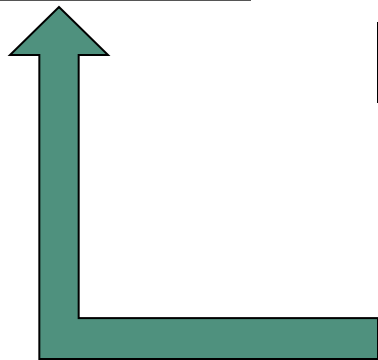
When P_0 sees output y in round i :

$$\begin{array}{c} \text{Probability} \\ \text{this is } i^* \end{array} = \frac{\text{constant} \times p}{\text{Pr}[P_0 \text{ gets } y \mid \text{this isn't } i^*] \cdot (1-p) + \text{constant} \cdot p}$$


Analysis – Will P_0 abort early?

When P_0 sees output y in round i :

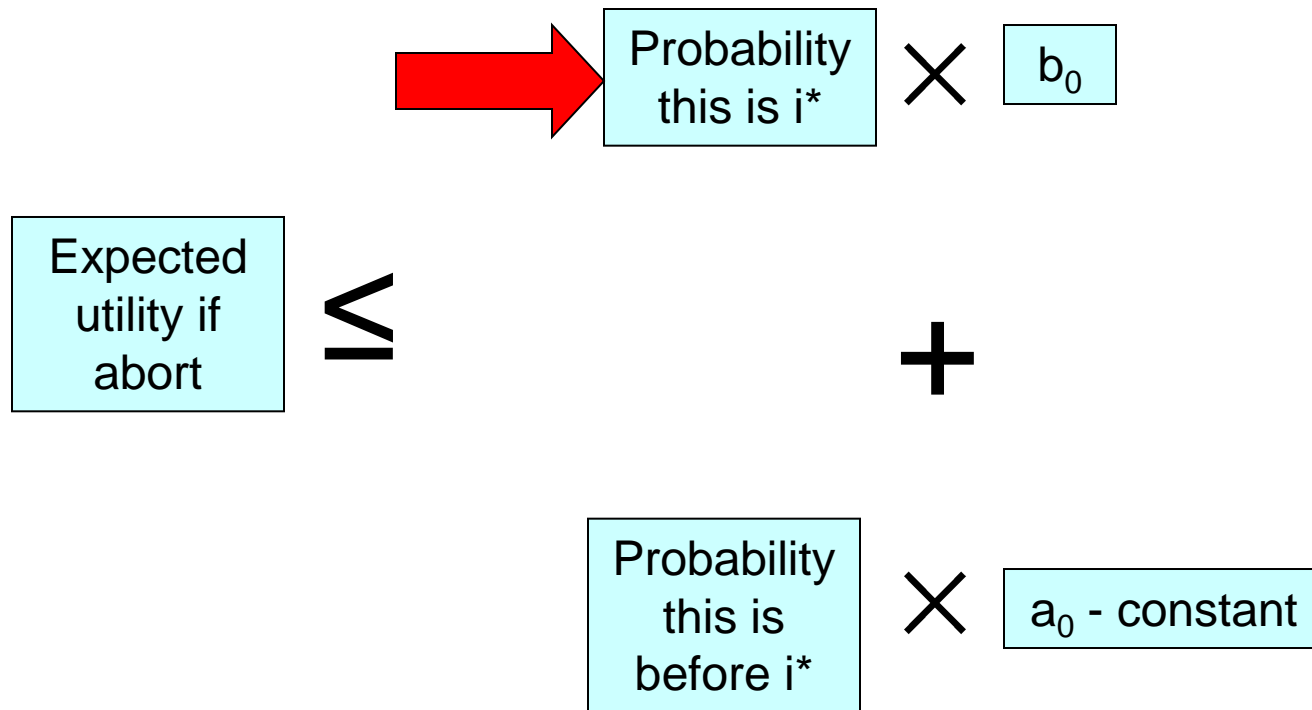
$$\text{Probability this is } i^* = \frac{\text{constant} \times p}{\text{constant} > 0 \cdot (1-p) + \text{constant} \cdot p}$$



Can make arbitrarily low by choice of p

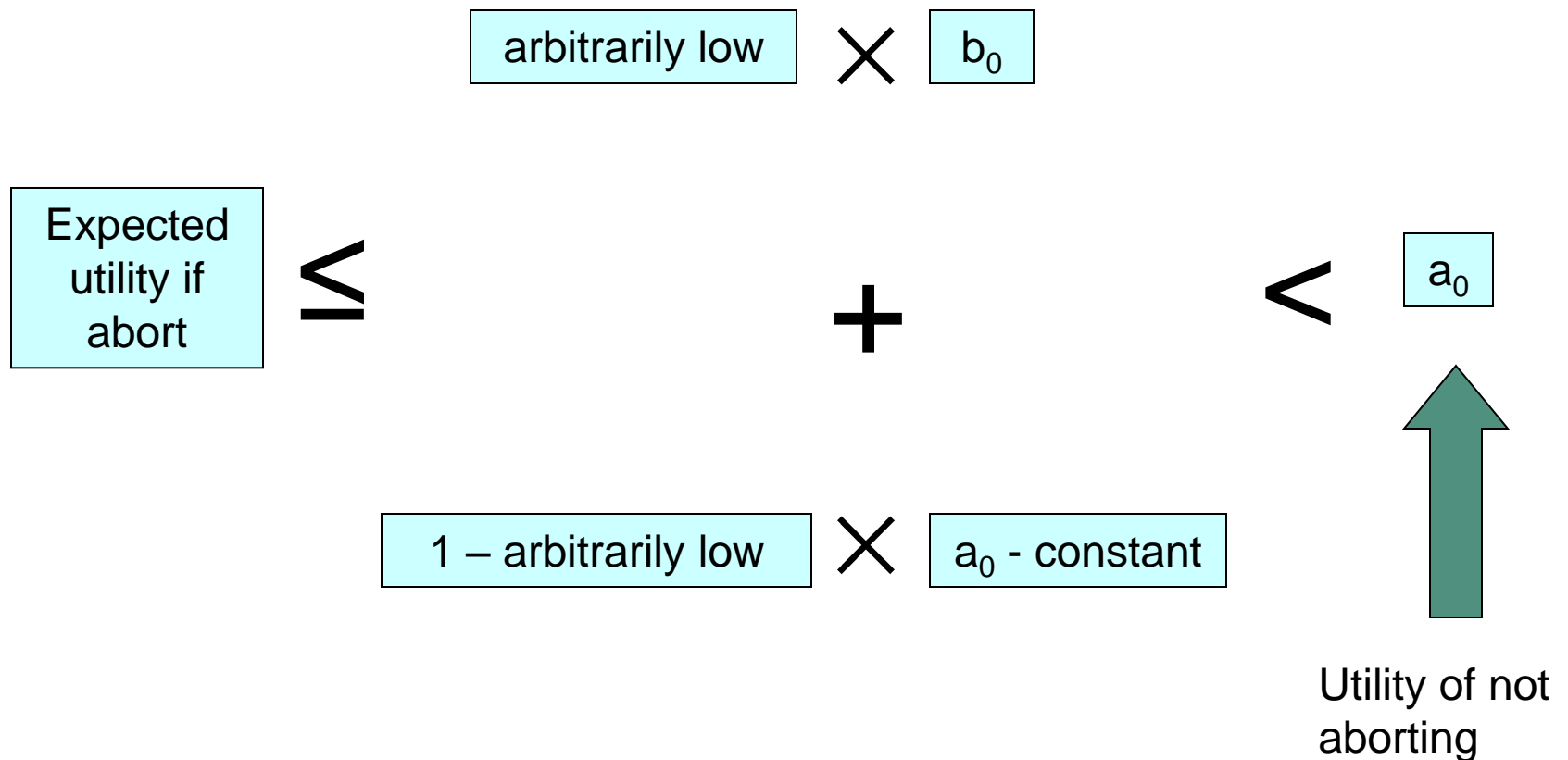
Analysis – Will P_0 abort early?

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