

Lecture Errata

Distinguishing games.

At one point I write $\Pr[\text{guess } 1 \times 12 \mid f \text{ is } 1 \times 12] - \Pr[\text{guess } 2 \times 6 \mid f \text{ is } 2 \times 6]$.

This is a mistake. The event needs to be the same, with the condition being what changes. So, at about 18:00 I wrote $\Pr[\text{guess } 1 \times 12 \mid f \text{ is } 1 \times 12] - \Pr[\text{guess } 2 \times 6 \mid f \text{ is } 2 \times 6]$ even though I meant $\Pr[\text{guess } 1 \times 12 \mid f \text{ is } 1 \times 12] - \Pr[\text{guess } 1 \times 12 \mid f \text{ is } 2 \times 6]$.