Extremal Pruning: Applying Game-Hopping Techniques in Real Life

Alexander W. Dent

Information Security Group

Royal Holloway, University of London

Royal Holloway
University of London

Game-Hopping Proofs

- Game-hopping proofs are an incredibly useful tool in mathematical cryptography.
- Key point: Memoryless games.

- Can this approach be used to analyse real-life situations?

Topic of Investigation

- Is it possible to pick something up with no arms?

Topic of Investigation

- Is it possible to pick something up with no arms?

- Assumptions:
  - Every person is either right-handed (with prob. *p*) or left handed (with prob. 1-*p*)

Topic of Investigation

- Is it possible to pick something up with no arms?

- Assumptions:
  - Every person is either right-handed (with prob. *p*) or left handed (with prob. 1-*p*)
  - Subjects will pick things up with favoured hand.

Topic of Investigation

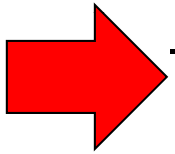
- Is it possible to pick something up with no arms?

- Assumptions:
  - Every person is either right-handed (with prob. *p*) or left handed (with prob. 1-*p*)
  - Subjects will pick things up with favoured hand.
  - Subjects will not pick things up if they can't do it with their favoured hand.

Topic of Investigation

- Is it possible to pick something up with no arms?

- Assumptions:
  - Every person is either right-handed (with prob. *p*) or left handed (with prob. 1-*p*)
  - Subjects will pick things up with favoured hand.
  - Subjects will not pick things up if they can't do it with their favoured hand.



Proof

- Game 1: Normal subject in room asked to pick up a ball on a table.
- Subject “wins” if he picks up the ball.

Proof

- Game 1: Normal subject in room asked to pick up a ball on a table.
- Subject “wins” if he picks up the ball.
- Let W_1 be the event that the subject wins.

Proof

- Game 1: Normal subject in room asked to pick up a ball on a table.
- Subject “wins” if he picks up the ball.
- Let W_1 be the event that the subject wins.

$$\Pr[W_1] = 1$$

➢ Help me!

Proof

- Game 2: Identical to Game 1 except that we hack off one arm of the subject with a rusty machete.

Proof

- Game 2: Identical to Game 1 except that we hack off one arm of the subject with a rusty machete.
- Key point: Arm is chosen uniformly at random from the set of all possible arms.

Proof

- Game 2: Identical to Game 1 except that we hack off one arm of the subject with a rusty machete.
- Key point: Arm is chosen uniformly at random from the set of all possible arms.
- Subject will still be able to pick up ball if we haven't dismembered their *favoured* hand.

Proof

- Game 2: Identical to Game 1 except that we hack off one arm of the subject with a rusty machete.
- Key point: Arm is chosen uniformly at random from the set of all possible arms.
- Subject will still be able to pick up ball if we haven't dismembered their *favoured* hand.

$$\Pr[W_2] = \tfrac{1}{2}\Pr[W_1]$$

- They've trapped me in this bizarre operating theatre.

Proof

- In Game 2, the subject had “lost” one randomly chosen arm.
- Game 3 is identical to Game 2 except we hack off both of the subjects arms with a rusty machete (or dirty scythe).

Proof

- In Game 2, the subject had “lost” one randomly chosen arm.
- Game 3 is identical to Game 2 except we hack off both of the subjects arms with a rusty machete (or dirty scythe).
- If we have already hacked off their favoured hand then Games 2 and 3 are identical.

Proof

- In Game 2, the subject had “lost” one randomly chosen arm.
- Game 3 is identical to Game 2 except we hack off both of the subjects arms with a rusty machete (or dirty scythe).
- If we have already hacked off their favoured hand then Games 2 and 3 are identical.

$$\Pr[W_3] = \tfrac{1}{2}\Pr[W_2]$$

- It’s very dark and I’m scared. I found this laptop on a table.

Conclusion

$$\Pr[W_3] = \tfrac{1}{4} \Pr[W_1] = \tfrac{1}{4}$$

- Even with no arms, you can pick up a ball on a table about one time in four.

➢ There is some rusty farm equipment in the corner.

Results in Practice

$$\Pr[W_3] = \tfrac{1}{4} \Pr[W_1] = \tfrac{1}{4}$$

Results in Practice

$$\Pr[W_3] = \tfrac{1}{4} \Pr[W_1] = \tfrac{1}{4}$$

- How practical is our (rather literal) reduction?
- How tight are our bounds?
  - Our bounds are very tight...

➢ I think I hear someone coming... and they're laughing.

Results in Practice

$$\Pr[W_3] = \tfrac{1}{4} \Pr[W_1] = \tfrac{1}{4}$$

- What about our assumptions?

Results in Practice

$$\Pr[W_3] = \tfrac{1}{4} \Pr[W_1] = \tfrac{1}{4}$$

- What about our assumptions?
- Experimental evidence suggests that subjects don't pick up the ball after their favoured hands have been removed (with a rusty machete, dirty scythe, or soiled scalpel).
  - Mostly they just scream and bleed.

➢ Oh God! No! NO!! Tell my wife I love her...