Teaching Automated Strategic Reasoning Using Capstone Tournaments

Oscar Veliz, Marcus Gutierrez, and **Christopher Kiekintveld**
University of Texas at El Paso
El Paso, TX 79968
osveliz@miners.utep.edu mgutierrez22@miners.utep.edu cdkiekintveld@utep.edu

Abstract

Courses in artificial intelligence and related topics often cover methods for reasoning under uncertainty, decision theory, and game theory. However, these methods can seem very abstract when students first encounter them, and they are often taught using simple toy problems. Our goal is to help students to operationalize this knowledge by designing sophisticated autonomous agents that must make complex decisions in games that capture their interest. We describe a tournament-based pedagogy that we have used in two different courses with two different games based on current research topics in artificial intelligence to engage students in designing agents that use strategic reasoning. Many students find this structure very engaging, and we find that students develop a deeper understanding of the abstract strategic reasoning concepts introduced in the courses.

Introduction

One of the central goals of artificial intelligence is to be able to design and implement autonomous agents that make effective decisions in complex domains. We describe a tournament-based pedagogy that we have used in two different courses with two different games to engage students in strategic reasoning. One course is a general introduction to Artificial Intelligence and the other focuses on applications of automated strategic reasoning in computer network security. There are many examples of successful uses of games in teaching AI including Pac-Man (DeNero and Klein 2010) and Mario (Taylor 2011). Our pedagogy is to use capstone projects in these AI courses where students must analyze a game, determine the strategic issues, and integrate multiple course methods to design an agent that will perform well against their peers' agents. Our approach is similar to previous work, but we emphasize using multiple AI topics, open ended agent design, and games based on current research.

Tournaments

We use tournaments to challenge students to develop automated agents that use strategic reasoning to make decisions in multi-player games, incorporating the knowledge and techniques they have learned throughout the course. At a high level, the tournaments have a round-robin structure [1] that matches up every agent against every other agent in many different game instances.

Network Security Game

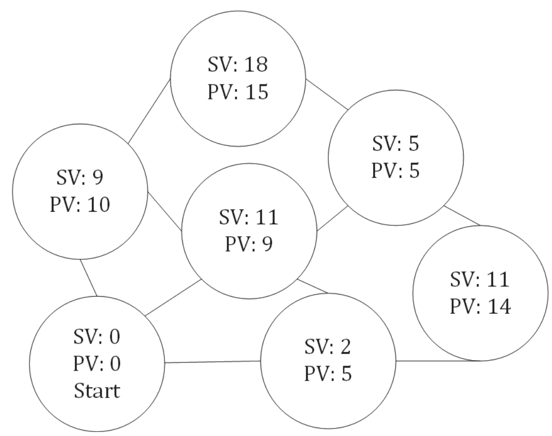

Figure 1: Example network security game where each node represents a computer on a network. Each node has a Security Value (SV) and Point Value (PV).

The first time we implemented a capstone assignment based on this structure was for a course called "Computational Decision Making and Risk Analysis" which focuses on applications of game theory, decision theory, and machine learning to computer network security. The game scenario we developed for this course shown in Figure 1 is inspired by current research in applications of game theory for security, including problems in computer network security (Kiekintveld, Lisý, and Píbil 2015). The game models an attacker/defender interaction, where computer networks are represented as graphs. Attacker agents probe the network looking for weaknesses and ways to attack the network. Defender agents try to harden the network, create firewall rules, and deploy honeypots.

[1] In practice round robin tournaments cannot be used with large numbers of agents requiring adoption of alternative structures.

We also observed significant variation in the types of strategies developed by the different groups of students, particularly for the attacker agents. Some agents would probe as much as they could to acquire maximal information before attacking, while others would would attack blindly and would use the resulting information to act as an informal and imprecise probe action. Some agents spent resources carefully avoiding honeypots, while other agents never probed for honeypots. A few agents even balanced their risk versus reward, by probing the security value versus probing the point value with a certain amount of probability.

The defender agents were, on the whole, somewhat less sophisticated. For example, very few agents used firewalls to strategically close off paths in the graph. Instead, most agents relied on heuristics to strengthen nodes with low security values that they deemed unsecured.

3 Card Pickup

We designed a new game to capstone our AI course drawing inspiration from Poker, which is used for benchmarking in AI research (Bowling et al. 2015). In designing the game we reused much of the generic code for running tournaments from the security game, and also incorporated open source code from PokerApp by Dan Puperi (Puperi 2014). Each player is dealt 2 private cards from a standard 52-card deck. Players take turns traversing a connected graph where the nodes contain sets of possible cards. Players take turns moving to neighboring nodes and at each turn can decide to pick up the card at that node. The real card is only revealed after the agent decides to pick up the card. The agents must pick up exactly 3 cards by the end or otherwise lose the game.

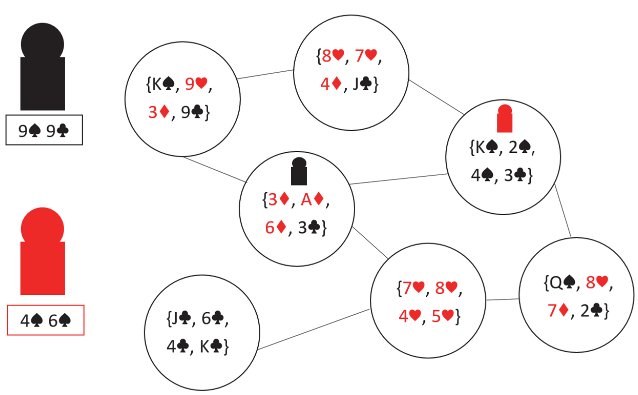

Figure 2: Example 3-Card Pickup Game

Figure 2 shows an example game where the number of fake cards was set to 3. Agents have their own private information so Black could deduce that the 9 of Clubs can not be in the top left node because it is already in its hand. Red also can infer that 4 of Spades is in its hand and therefore is not in the current node leaving it with just three possibilities instead of four. All players know that the card in the bottom middle must be a Heart because the suits match.

Most groups realized that picking up a card without looking at what was in their hand was foolhardy. Many agents used a matching strategy first noting the cards in their hands and then looking for similarly ranked cards among the nodes in the graph. These kinds of strategies would prioritize hands such as Pair, 2 Pair, 3-of-a-Kind, Full House, and 4-of-a-Kind. Many students also noticed that they could update their beliefs about the cards in the graph based on information received during the game as cards were picked up.

Concluding Discussion

We have presented our approach to a capstone tournament pedagogy for teaching automated strategic reasoning, integrating topics such as reasoning under uncertainty, decision theory, and game theory. Our students were challenged to design sophisticated autonomous agents for playing games based in AI literature which students found engaging, fun, and interesting. We created two novel games for agent design and tested them in real classroom projects; we count both of these as successful trial runs and believe that these games could be used more broadly and inspire new games.

We solicited informal feedback and commentary from the students, which has provided valuable insights into how we can improve the specific games in the future. Studying the agent designs also provided an indication of which concepts students did or did not use when developing their agents. It was possible for students to do well on the assignment without placing at the top of the tournament, but the potential for the best grades (including extra credit for the very top performers) was a strong incentive to put a lot of time and effort into the design. Overall we believe that most students found the structure of the project to be very engaging, and that they developed a deeper understanding of the abstract strategic reasoning concepts taught in the courses to new problems.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. IIS-1253950.

References

Bowling, M.; Burch, N.; Johanson, M.; and Tammelin, O. 2015. Heads-up limit hold em poker is solved. *Science* 347(6218):145–149.

DeNero, J., and Klein, D. 2010. Teaching introductory artificial intelligence with pac-man. In *Proceedings of the Symposium on Educational Advances in Artificial Intelligence*, 1885–1889. Menlo Park, California: The AAAI Press.

Kiekintveld, C.; Lisý, V.; and Píbil, R. 2015. Game-Theoretic Foundations for the Strategic Use of Honeypots in Network Security. In *Cyber Warfare*. Springer International Publishing. chapter 5, 81–101.

Puperi, D. 2014. Pokerapp. http://sourceforge.net/projects/pokerapp/. Accessed: 2015-05-01.

Taylor, M. E. 2011. Teaching Reinforcement Learning with Mario : An Argument and Case Study Games for Teaching. In *Proceedings of the Second Symposium on Educational Advances in Artificial Intelligence*, 1737–1742. Menlo Park, California: The AAAI Press.