Homework 1

Alejandro Diaz

adiaz77@gatech.edu

1 QUESTION 1

It is possible to represent the Star Wars problem as a semantic net. Each node of the net represents a state in the problem space. For the Star Wars problem, each node, at a minimum, should provide a way to store who is planet-side and where the ship's position (we do not have to store both sides because we can use one side to deduce the other so long as we know the total number of passengers in the problem). The operator between states will be the transition of the shuttle and its passenger choice. Figure 1 illustrates the semantic network created by abstracting the problem.

With the blueprint of the node, we can use it to design a generate and test method. The generator should use the operator (move 1 or 0 passengers) to generate each possible state. Hence, the generator will generate $j + 1$ cases, where j is the number of people on the same side as the ship. The extra value in possibilities accommodates the case that no passenger is moved.

In turn, the tester should check each generated state for validity using the conditions listed. A failure in any condition pruning any invalid state:

· Checking against the rules of the problem (e.g., Is Rey and Kylo alone without the ship? Is Rey and Snoke together without the ship?)
· Checking if the state is a solution by comparing against the goal state (i.e., Is everyone is space side?)
· Checking to see if the state has been generated before along the path (i.e., Does the state have a connection to an identical state?)
· Merging any identical states on the same level to reduce branching (i.e., Is there another state at this branch level that is identical?)
· The tester should navigate these states in a breadth first search (BFS) to identify the optimal path to the solution state. Worst case time and space efficiency of $O(b^d)$, where b is the branching factor and d is the depth (Korf, 1999)

The full semantic network to this problem is illustrated in Figure 2.

2 QUESTION 2

The General Data Protection Regulation (GDPR) outlines the principles by which companies must treat personal data. The regulation says that personally identifiable data must be consented for, processed fairly and transparently, collected with explicit consent, adequately (i.e., no blanket data-collection), accurately and limited to what is necessary (i.e., data minimization), handled, and stored to meet expectations outlined by the policy (Parliament and European union, 2016)(Davies, 2018).

The regulation outlines how personal data may be used to personalize individual user experiences online. It makes the blanket data collection method illegal (Ch.2 Article V). Service providers can no longer collect personal data on implicit agreements; instead, GDPR requires explicit consent (Ch.2 Article VII). Data must now be opt-in and not opt-out. Services can no longer have a "take it or leave it" approach to their services. Any personal data collectors must offer users the ability to opt-out of personal data collection. Furthermore, GDPR outlines that any personal data that they store should be pseudonymization (Ch.4 Article XXVII). GDPR also allows users to choose to object to certain data processing and request that companies not process their data in such a way (Ch. 3 Article XXI).

Each of these personal data gathering policies has the potential to hinder AI and machine learning algorithms that offer user personalization. In cases where data must be anonymize or users otherwise withdraw consent to data collection or processing, the AI algorithm is working without data for its production model. In such cases, the agent will only be able to work with generic, non-personalized data such as geography, language, and otherwise aggregate data. The agent could use a matching algorithm to find similar personalized data profiles to apply to the anonymized user, but this goes against the spirit of the law. In short, data collectors (including for AI purposes) must ask for informed, categorical consent from users to collect relevant data.

The night that the regulation went into effect, Google was sued for data collection concerns and lost the lawsuit (Satariano, 2019). Google's products, such as their web search, have succeeded more so than any traditional advertisement because of their ability to build an advertising profile on their users.

There were concerns that Google's personalized advertising would be hampered by the GDPR and the fallout of privacy court cases (Barry, 2019) Others argued that AI profiling could replace personal data with contextualization and solve Google's data problems (Davies, 2018). Is there a world where these personalized advertising profiles can coexist with the GDPR?

There is room for google to adapt. If the interface provides transparency into what data is collected and for what purpose, users can agree to consent to allow Google to store a profile on them. Google should process their data transparently and inform users what the data is being used for and for how long. If Google can maintain personalization in their products but lose it in their advertisement, they will still survive. Their products will maintain large user bases that they can advertise too with or without personalization. AI and other personalizing tools are still possible in the EU. Google has other sources of data to draw from that does not violate personal user data. Google would be able to make highly personalized data best on aggregate trends and applying those trends to user groups.

3 REFERENCES

[1] Barry, Stephanie (July 28, 2019). *GDPR and Advertising – the Impact So Far - AdWorld.ie*. adworld.ie. URL: https://www.adworld.ie/2019/07/18/gdpr-and-advertising-the-impact-so-far/ (visited on 02/05/2021).

[2] Davies, Jessice (June 7, 2018). *'Personalization diminished': In the GDPR era, contextual targeting is making a comeback - Digiday*. Digiday. URL: https://digiday.com/media/personalization-diminished-gdpr-era-contextual-targeting-making-comeback/ (visited on 02/05/2021).

[3] Korf, Richard (1999). "Artificial intelligence search algorithms". In: *Citeseer*.

[4] Parliament, European and European union, Council of the (May 4, 2016). "General Data Protection Regulation (GDPR)". In: *Official Journal of the European Union* 59.119, pp. 89, 132. ISSN: 1977-0677. URL: https://gdpr-info.eu/ (visited on 02/05/2021).

[5] Satariano, Adam (Jan. 21, 2019). "Google Is Fined $57 Million Under Europe's Data Privacy Law - The New York Times". In: *New York Times*. URL: https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html (visited on 02/05/2021).