Homework 1

Xinghao Chen
xchen785@gatech.edu

1 PROBLEM 1

1.1 The Semantic Network

See Figure 1. A red cross means a state is invalid because of the constraints; a yellow cross means that the state is unproductive because it has apppeared in earlier steps.

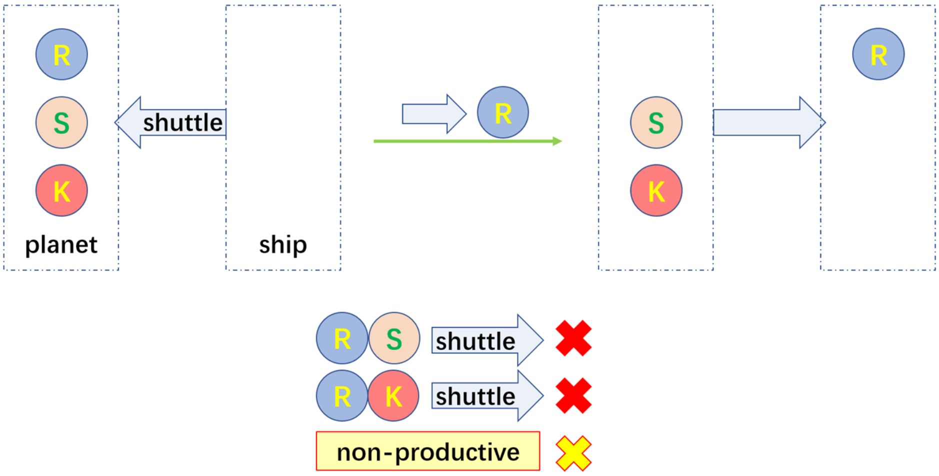

Figure 1— The semantic network showing the states and transitions.

1.2 The solution

See Figure 2. Note that **it is omitted in the initial transitions to move the shuttle without a passenger**, because this is not productive.

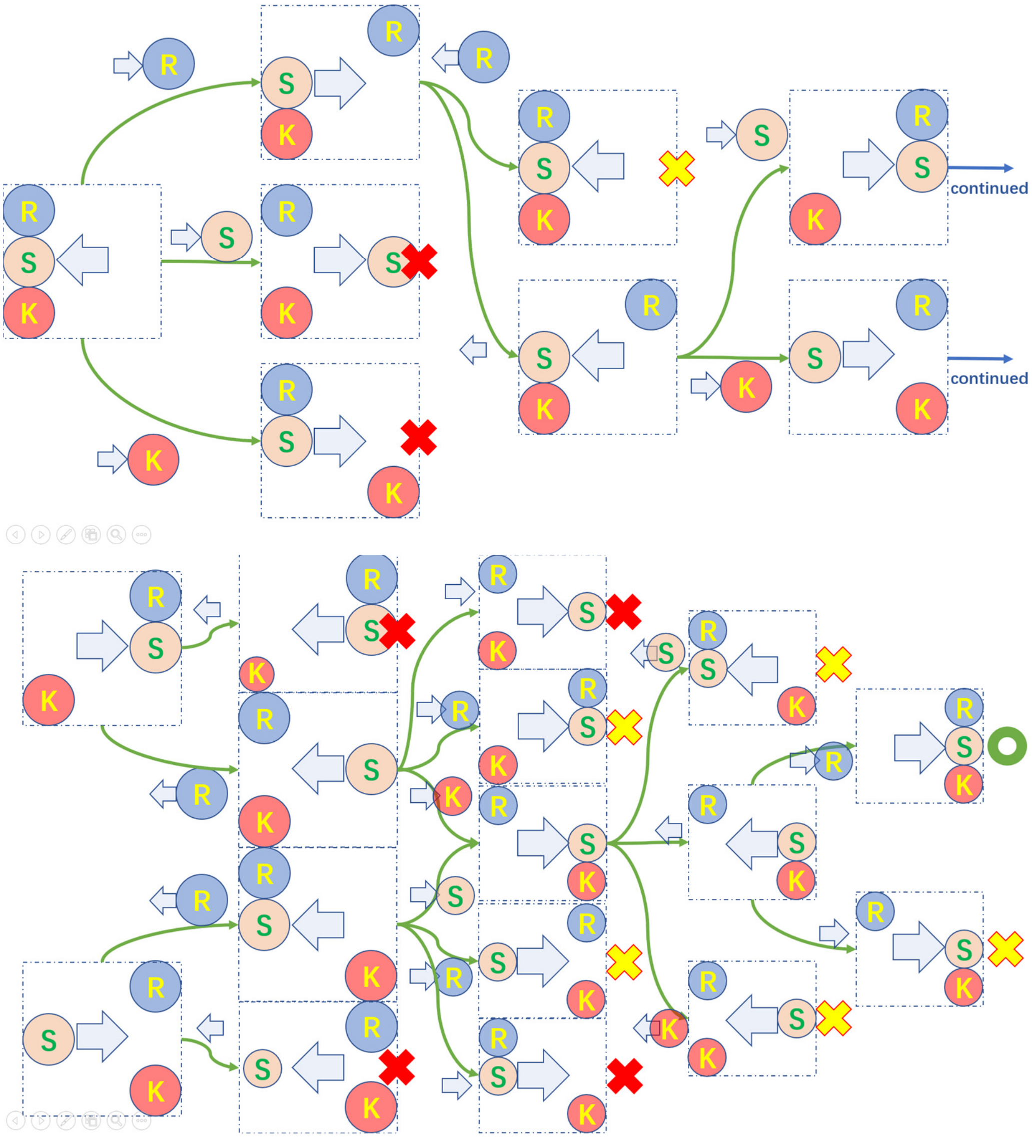

Figure 2 — The solution via generate & test

2 PROBLEM 2

2.1 The content of *General Data Protection Regulation* about the usage of personal data

Regulations about the usage of personal data are majorly documented in the 2nd chapter. The collecting and processing of personal data shall be lawful, fair and transparent, be at a minimal scale, and is strictly limited for only specified, explicit and legitimate purposes. Inaccurate data shall be erased or rectified without delay. Data shall be kept for no longer than is necessary for the specific purposes. The processing of data shall follow an appropriate manner for integrity and confidentiality.

Besides, the data subject has the right to access, rectificate, erase, or restrict the use of his or her personal data.

2.2 How the regulation might apply to the use of artificial intelligence to create personalized experiences?

The regulation, enforcing extra restrictions on data management, requires a more complex architecture of data warehouse. Consequently, the data holders must be able to flexibly handle the ever-changing data. However, not only do we need to enhance the exorbitant data infrastructures for refined management and timely rectification and deletion, we would also encounter the problem of deleting latent data from a trained AI model.

2.2.1 *It is hard to withdraw data from an AI agent*

Current AI technologies rarely consider the demand of retreating some data from a trained model. However, this demand has risen abruptly as researchers point out the privacy risks from big data. Sometimes we can even let the AI repeat some raw, sensitive personal privacy it had seen in training. (Carlini N., Tramer F., Wallace E., Jagielski M., Herbert-Voss A., Lee K., Roberts A., et al., 2020, arXiv, arXiv:2012.07805). What if some data has been used for training an AI, but the data subject then requires that his or her data must be deleted and shall not be used for such an AI agent? For now, the legal answer seems only to be abandoning the previous model and training it again. However, the cost of training heavy models frequently is not always affordable to enterprises. This problem would become a serious concern for any business organization to train an AI agent using big personal data.

2.2.2 *Forecasting the future: advance of technologies and law*

Retreating data can be hard. But in the foreseeable future, we can still prevent data leaking and misusing.

With strict regulations, new technologies may emerge to protect the data subject without significantly weaken the efficiency of AI development. Current simple techniques, such as adding noise into raw data, has taken its effect to some extent. Perhaps, in the future, federated learning, which can be equipped with advanced cryptography techniques for data privacy, would play an important role to broaden the utility of data by ensuring that the data can be used without being read in its raw status.

Also, further laws may be issued to specify the details between the monopolism of data and every individual's privacy. To relieve the risk of large-scale data misusing, we may tax any single organization that stores overly large data. We can even set up third-party data warehouses which are designated to preserve unfailingly lawful data.

2.3 An example industry deeply embedded in personalization

Medical AI agents, though serving as a great savior of both doctors and patients, unfortunately records each one's most personalized data. State-of-the-art medical AI agents, based on big medical data including images and clinical reports, are good at diagnosis. But the data taken from large numbers of individual patients would certainly face the GDPR restrictions. Awkwardly, it is almost impossible not to collect these medical data. Otherwise, doctors may have little means of treatment.

2.4 The possible adaption of medical data management to the GDPR regulations

Although ideally described in GDPR, not all the clauses can be easily achieved in medical practice. There have to be detailed legal instruments and more advanced technologies to strike a better balance.

2.4.1 *From the perspective of AI to advance*

First of all, due to the technical difficulty to retreat data from an AI agent, it would be better if patients must waive their right to delete latent data in an agent, once they consent that their data can be used for training AI. If GDPR insists on protecting individuals' right to withdraw data from AI, there would be virtually no chance for researchers to train any AI agent.

Secondly, medical purposes should be explicitly listed as a field of public interest. With such a guarantee, we can follow the clause 1(b) of Article 5 of GDPR to let medical AI agents advance more efficiently. Laws should be refined to ensure the development of key technologies.

Finally, new technologies, as have been described in 2.2.2, may emerge to serve a more efficient balance between privacy and technology development. Laws should also evolve themselves to regulate newly sprouted things.

The summary is that, faced with the GDPR regulations, governments and data-owning organizations should take joint measures via technology and law to help technologies develop without relying heavily on trespassing people's raw privacy.

2.4.2 *From the perspective of the data subject*

The foremost demand of the data subject might be a well-acknowledged template of contract, which allows individuals to breezily select which data can be used for what purposes. Contract templates enable individuals to exercise their rights much more easily, without having to employ lawyers and raise long-running litigations. This would be a must for the data subject in order to practice the ideas in GDPR.

The following demand is to actually force organizations, which may own big personal data, to use them transparently. However, this may be another hard problem, not even easier that retreating data from AI agents. It is almost impossible to require that the medical institutions shred their data on time, because it is difficult to integrally investigate the true purpose of keeping data. Organizations can always make excuses that some data are critical for future diagnosis on the patient. Besides, there is a legal paradox in keeping track of each organization's computers, since organizations also have their privacy and trade secrets. In most cases, we may only be able to regulate a few protruding cases of data misusing.

In a word, there is a long way to go, both legally and technically, if we would like to penetrate into all the nooks of transparent data processing.

3 REFERENCES

1. Carlini N., Tramer F., Wallace E., Jagielski M., Herbert-Voss A., Lee K., Roberts A., et al., 2020, arXiv, arXiv:2012.07805