Homework 1

Manoel Cortes Mendez
manocormen@gatech.edu

1 QUESTION 1

1.1 Construct a semantic network representing the problem.

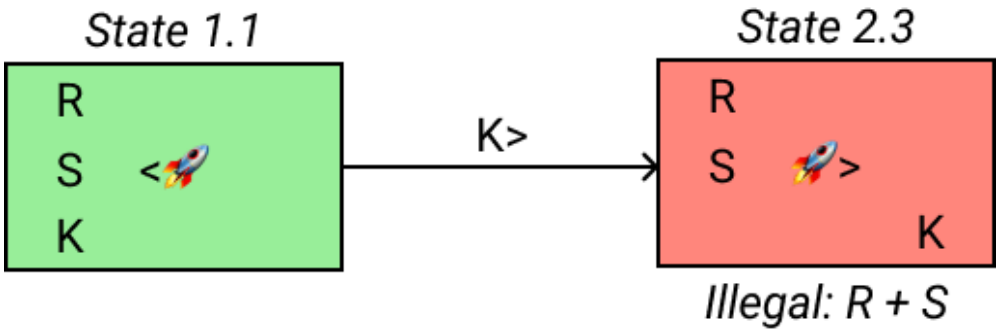

Figure 1—Semantic network: example of states and transition.

In *Figure 1*, you can see the semantic network I used to represent the problem. Here's how to interpret its various components:

- **States**: Each rectangle represents a state in the problem. Each state has a unique label. The left part of the rectangle is Quesh; the right part is the orbiting ship. Characters are represented by their initials: *R* for Rey, *S* for Snoke, and *K* for Kylo Ren. When the letters are on the left, they're on Quesh; when they're on the right, they're on the orbiting spaceship. Finally, in the center of each rectangle, a rocket emoji with a *greater-than* or *smaller-than* sign shows the current position of the shuttle.
- **Transitions**: Arrows represent transitions from one state to another — that is, a valid shuttle movement, with or without a passenger. Each arrow is labeled with a transition operator which consists of the initials of the passenger (if there's one) and a *greater-than* or *smaller-than* that shows the direction of the shuttle, Quesh-to-ship or ship-to-Quesh, respectively.
- **Validity**: Illegal states are represented with red rectangles, and a label below them explains why they're illegal. Legal states are represented with green rectangles. Duplicate states are explicitly denoted by indicating the previous identical state.

1.2 Apply generate & test to this semantic network to solve the problem.

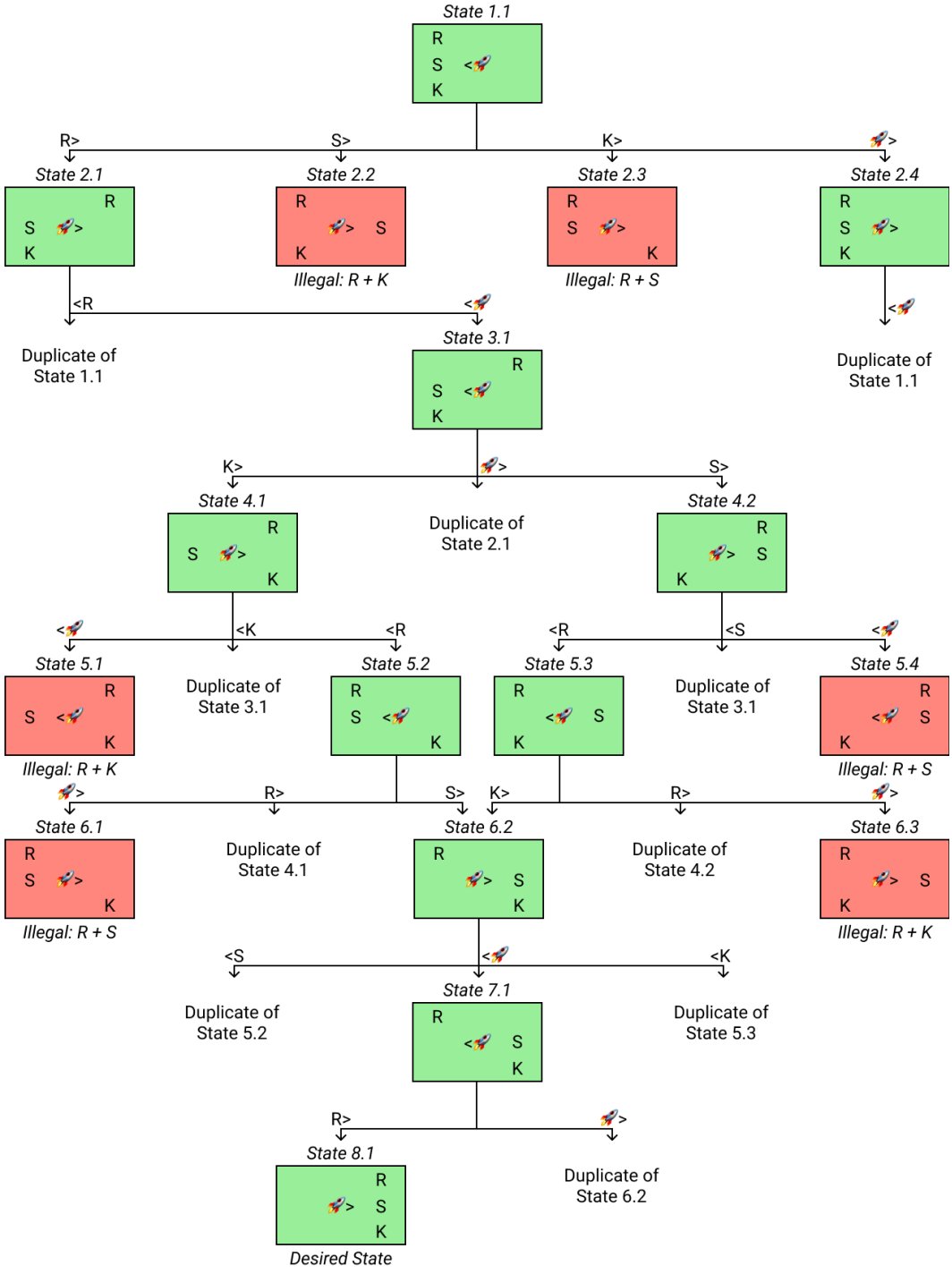

Figure 2—Applying generate & test to the semantic network

QUESTION 2

2.1 Research GDPR and describe what it says about the usage of personal data to personalize individual user experiences online.

Simply put, GDPR is a set of rules that govern how personal data of EEA citizens can be processed by organizations. *Personal data* are any data about a person that can allow to identify them or are sensitive in nature, like name or religion.

GDPR is a broad regulation. It's not exclusively about what's allowed when "personalizing individual user experiences". But it's comprehensive enough to subsume how personal data can be used to personalize user experiences.

GDPR is structured around seven principles (EU, 2016). Here are these principles and how they can be interpreted:

- **Lawful, fair, transparent**: Data should be collected legally (e.g. with consent), fairly (e.g. no deceptive communication), and transparently (eg. the user should know what their data will be used for).
- **Purposeful**: Data should only be used for the goal it was collected.
- **Minimum data**: You should collect as little data as possible for your goal.
- **Accurate**: The data should be kept accurate (e.g. users should be allowed to correct it).
- **Minimum duration**: Data shouldn't be stored indefinitely, but rather for as little time as possible for your stated goal.
- **Security**: Data should be moved and stored securely.
- **Accountability**: You should be able to demonstrate compliance with all the principles above (e.g. in case of an audit).

2.2 Analyze how that regulation might apply to the use of artificial intelligence to create personalized experiences.

AI, and machine learning in particular, can require massive amounts of data. Since GDPR regulates data processing, let's consider how the GDPR principles might apply to using AI to create personalized experiences:

- **Lawful, fair, transparent**. If you're collecting personal data to match users with other users through an AI recommendation system, you should let the user know beforehand and ask them for consent.

- **Purposeful**: If you told users their personal data would be used to match them with other users via AI, you can't turn around and sell their data.
- **Minimum data**: If you're matching users according to, say, their musical tastes using AI, you shouldn't collect unrelated data like religion.
- **Accurate**: If the personal data being used in the AI pipeline is wrong, users should be able to correct it.
- **Minimum duration**: If you're collecting personal data to match users using AI , and a user deletes their account, their data should be removed.
- **Security**: The AI pipeline should be secured at all levels.
- **Accountability**: A data officer should be appointed and compliance with the principles above should be documented in regards to the AI activities.

2.3 Select an example of a device, company, or industry for which personalization is deeply embedded in its functional purpose or business model.

One example of a device is health trackers, like FitBit and Apple Watch. To be able to use all the features of these devices, you have to share some personal data, like your age, sex, and weight. These data serve to establish a baseline and tailor the experience to your specifics.

For instance, FitBit can tell if your heart rate is within the normal range, but for this, it needs to know your age. In addition, FitBit can tell you your BMI, but for this, it needs to know your height.

If you don't provide this information, you can still use the device, but the experience won't be nearly as personalized. For instance, FitBit might still be able to tell you your heart rate, but it won't know if it's within the normal range.

2.4 Select another example of a device, company, or industry for which, without personalization, there *is* no service.

One example of an industry is genealogy companies, like Ancestry or 23andMe. These companies sell DNA kits that one can use to learn where their ancestors came from, or even detect genetic predispositions to certain illnesses.

This industry is underpinned by the collection of genetic data, which is very sensitive personal information. So without the ability to collect this data, this industry can't exist.

2.5 Define the European Economic Area (EEA).

According to the European Commission Glossary (Eurostat, 2022), the *European Economic Area* (EEA) is a agreement between the 27 countries of the European Union (like Poland, Belgium, and Spain) as well as 3 countries that aren't part of the European Union (Norway, Iceland, and Liechtenstein) to facilitate the free movement of people, goods, services, and capital between these countries.

2.6 Cite which section of GDPR is relevant to the examples you chose.

Here are some sections relevant to my examples, health trackers and DNA kits:

- **Chapter 2, Article 9, 2.a–2.j**: These clauses list the circumstances in which highly-sensitive data like health data and genetic data can be processed. Outside these circumstances, processing these data is prohibited.
- **Chapter 2, Article 9, 4**: This clause specifies that individual countries can further restrict the circumstance in which genetic data can be processed.
- **Chapter 3, Article 13, 1.c**: This clause specifies that the data collector should disclose to the user the reason his personal data is being collected (e.g. will the health or genetic data be used for research?).
- **Chapter 4, Article 32, 1.a**: This clause specifies that the data collector should encrypt personal health data, because it's highly sensitive data.
- **Chapter 5, Article 46, 1**: This clause specifies that personal data may be transferred to a third country only if done securely and if the third country offers comparable data freedoms and rights to the user.

2.7 Explain how the sections you cited are relevant to the examples you chose with respect to the EEA.

GDPR applies to any organization that processes personal data of EEA citizens, whether the organization is based in an EEA country or not. So the fact that FitBit, for instance, is a Google-owned US company doesn't preclude them from having to abide by GDPR when it comes to EEA users.

Here's how the sections I cited apply to my examples with respect to the EEA:

- **Chapter 2, Article 9, 2.a–2.j**: Health tracker and DNA kit companies can only collect health data about EEA citizens if they satisfy one of the

conditions in these clauses — for instance, if the user has given explicit consent for their personal health data to be processed.

- **Chapter 2, Article 9, 4**: EEA countries can elect to have tighter regulations regarding genetic data than required by GDPR — for instance, in France, DNA kits are banned (EPRS, 2021).
- **Chapter 3, Article 13, 1.c**: EEA citizens should be clearly informed about why their personal data is being collected.
- **Chapter 4, Article 32, 1.a**: Genetic data of EEA citizens, even when stored in, or transiting through, countries outside the EEA should be encrypted.
- **Chapter 5, Article 46, 1**: Moving the health data of EEA citizens to a country outside the EEA would require upholding comparable regulation in said country and being able to demonstrate that.

2.8 Evaluate how these devices, sites, or services may be adapted to these GDPR restrictions.

To adhere to GDPR, a health tracking or genealogy company may consider:

- Clearly asking for consent to use personal data and documenting it.
- Expanding operations in countries with favorable legislation.
- Communicating in the user's local language to ensure understanding.
- Encrypting data by default, to palliate the consequences of a breach.
- Buildinging infrastructure in the EEA to preempt the need to move data.

2.9 Determine and defend whether it is even possible to allow users in the EEA to use these tools without waiving their GDPR rights.

I think it's possible to allow users to use health trackers and DNA kits in the EEA without them having to waive their GDPR rights, as long as these aren't forbidden by the nation's laws. In France, for instance, there is no way around the DNA kit ban (EPRS, 2021), besides deliberately doing something illegal.

But as long as there's a lawful approach, companies with means to implement compliance measures have been able to adapt their offering to GDPR. I've seen some of these changes myself: I've been using health trackers for a long time and noticed that consent requests and general communication about the usage of my personal data became more frequent and comprehensive over the years.

4 REFERENCES

1. EU (2016) GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council. In the Official Journal of the European Union. [Online]
2. EPRS (2021) What if consumers could use devices to sequence DNA? In Scientific Foresight. [Online]
3. Eurostat (2022) European Economic Area (EEA). In Eurostat Glossary. [Online]