Security, Privacy and Explainability in Machine Learning

SS 2019

Exercise 1

Name	Mat.Nummer
Maximilian Bachl	01100143
Alexander Hartl	01125115

May 11, 2019

1 Dataset Selection

We selected the "Airline Customers" dataset available on kaggle's online platform[1], which seems to be taken from an airline company's frequent-flyer program. Since a customer's bonus points presumably show a strong correlation with the customer's financial wealth, the dataset contains sensitive data.

1.1 Contained Information

The dataset contains several, partially redundant, attributes regarding a customer's flight frequency and bonus points. For demonstration purposes we reduced the attributes to

- Gender
- Age
- Work Country
- Work Province
- Work City
- First flight date
- Total flight count
- Total bonus points

1.2 Quasi-Identifiers

The combination of quasi-identifying attributes allows a third-party to uniquely identify an individual in the dataset. In our case the set of quasi-identifiers consists of **Gender, Age and Work Country/Province/City**. Other attributes could contribute to identifying an individual but are usually not known to a third-party.

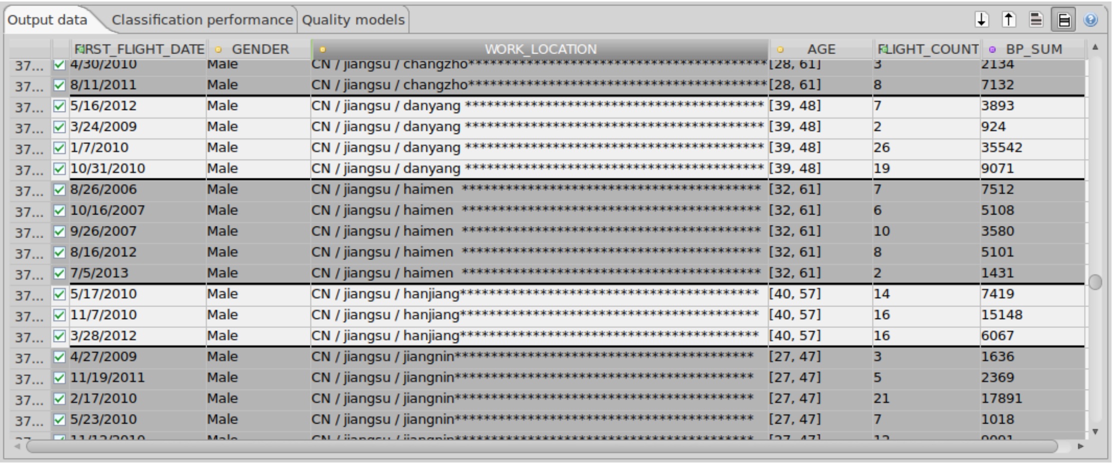
2 Anonymization

We used ARX[2] for the anonymization process and deployed several anonymization techniques for the different attributes:

- Gender: Generalization, suppressing the attribute, if necessary.

[1] `https://www.kaggle.com/diezerg/airline-customers`

[2] `https://arx.deidentifier.org/`



		FIRST_FLIGHT_DATE	○ GENDER	○ WORK_LOCATION	○ AGE	FLIGHT_COUNT	○ BP_SUM
37...	☑	4/30/2010	Male	CN / jiangsu / changzho**	[28, 61]	3	2134
37...	☑	8/11/2011	Male	CN / jiangsu / changzho**	[28, 61]	8	7132
37...	☑	5/16/2012	Male	CN / jiangsu / danyang **	[39, 48]	7	3893
37...	☑	3/24/2009	Male	CN / jiangsu / danyang **	[39, 48]	2	924
37...	☑	1/7/2010	Male	CN / jiangsu / danyang **	[39, 48]	26	35542
37...	☑	10/31/2010	Male	CN / jiangsu / danyang **	[39, 48]	19	9071
37...	☑	8/26/2006	Male	CN / jiangsu / haimen **	[32, 61]	7	7512
37...	☑	10/16/2007	Male	CN / jiangsu / haimen **	[32, 61]	6	5108
37...	☑	9/26/2007	Male	CN / jiangsu / haimen **	[32, 61]	10	3580
37...	☑	8/16/2012	Male	CN / jiangsu / haimen **	[32, 61]	8	5101
37...	☑	7/5/2013	Male	CN / jiangsu / haimen **	[32, 61]	2	1431
37...	☑	5/17/2010	Male	CN / jiangsu / hanjiang**	[40, 57]	14	7419
37...	☑	11/7/2010	Male	CN / jiangsu / hanjiang**	[40, 57]	16	15148
37...	☑	3/28/2012	Male	CN / jiangsu / hanjiang**	[40, 57]	16	6067
37...	☑	4/27/2009	Male	CN / jiangsu / jiangnin**	[27, 47]	3	1636
37...	☑	11/19/2011	Male	CN / jiangsu / jiangnin**	[27, 47]	5	2369
37...	☑	2/17/2010	Male	CN / jiangsu / jiangnin**	[27, 47]	21	17891
37...	☑	5/23/2010	Male	CN / jiangsu / jiangnin**	[27, 47]	7	1018

Figure 1: Exemplary equivalence classes as found by ARX.

- Age: Microaggregation, reducing the exact age to intervals, if necessary.
- Work Location: Generalization, using a hierarchy to mask the data, if necessary. For this to work properly, we merged the work location attributes to one attribute in the form <Work Country> / <Work Province> / <Work City> as a preprocessing step, so that more fine-grained information will be suppressed first.

We used k-Anonymity with $k = 3$ and $k = 50$ as privacy model. Furthermore, as total bonus points constitutes a sensitive attribute, we used t-closeness with $t = 0.2$ and “EMD with ordered distance” as distance measure.

3 Discussion

Fig. 2 shows the anonymization paths that ARX finds for $k = 3$ and $k = 50$, respectively. To achieve the same level of anonymity, either the gender attribute can be suppressed or the contained information about the work location can be reduced, resulting in the paths shown in Fig. 2.

For different k, the paths don’t show significant differences. However, aiming at the same level of anonymity, ARX has to suppress more information when selecting a lower k.

Fig. 1 shows an excerpt of an solution ARX finds for $k = 3$. Some of the equivalence classes indeed assume the desired size of 3, while others are substantially larger.

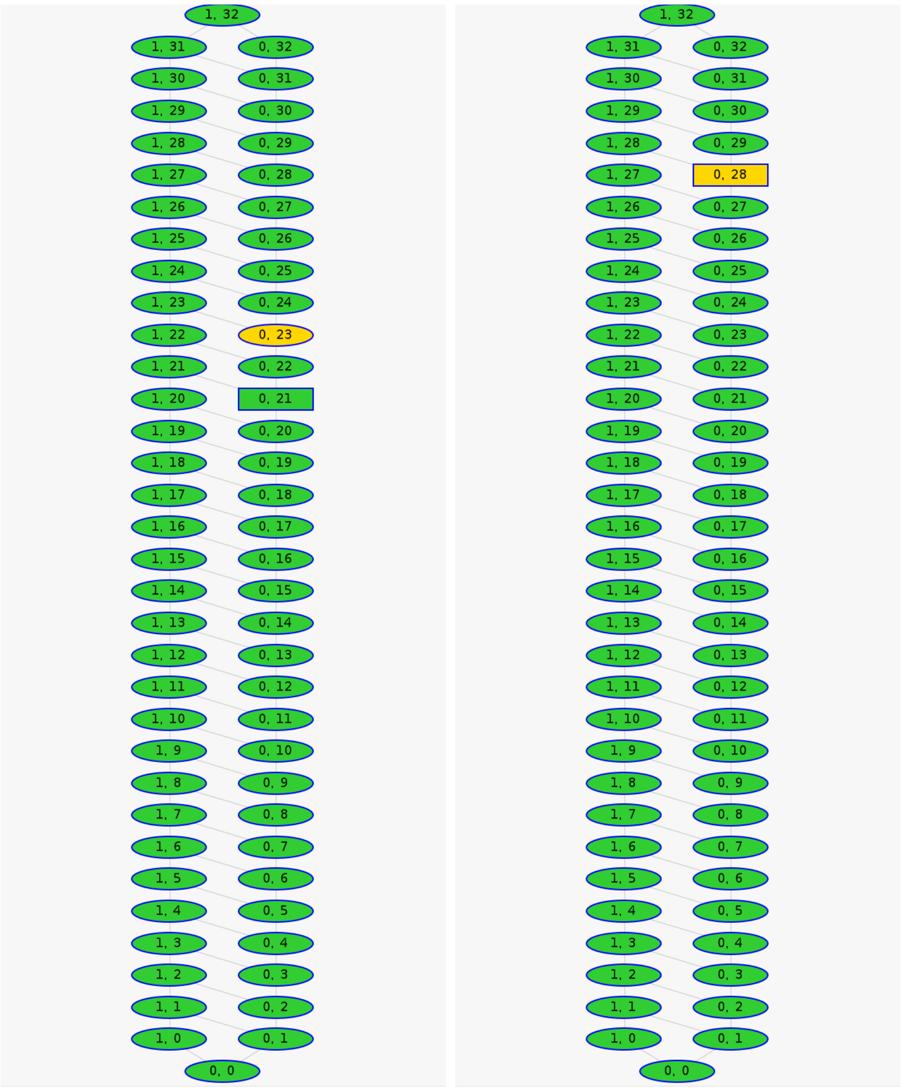


Figure 2: Anonymization paths for $k = 3$ (left) and $k = 50$ (right).