SATGPA - Probabilistic Graphical Models (Minutemen DP-pgm)

Evaluation Synthetic Data Creation

Steffen Moritz, Hariolf Merkle, Felix Geyer, Michel Reiffert, Reinhard Tent (DESTATIS)

January 31, 2022

Executive Summary

We tested **minutemen** method using the available python scripts. As you could expect from a **second place submission** of the 2021 NIST differential privacy challenge, minutemen scored quite well for our main privacy metrics. Out of all different methods we tested (`FCS`, `IPSO`, `GAN`, `Simulation`, `Minutemen`) minutemen was (together with the simulation approach) the **best method in terms of privacy**. Unfortunately, the minuteman method could not produce useful synthetic data based on SAT in our case. There is **barely any measure that would indicate a high utility**. The Kolmologorov-Smirnov test, the mahalanobis distance based on the regression parameters as well as the `S_pMSE` for tables and for distributions do not indicate substantial quality. There is **no reasonable utility** according to Mlodak's information loss criterion.

USE CASE RECOMMENDATIONS

Releasing_to_Public	Testing_Analysis	Education	Testing_Technology
NO	NO	YES	MAYBE

Based an our synthetic SAT dataset, we would not recommend minuteman for the use case **releasing to the public**. The synthetic dataset does not reproduce correlations and distributions in a sufficient way, which could lead to misunderstandings. The same is true for **testing analysis**. What we can imagine is undergrad students playing around with the data to improve their data science skills. Thus, since the privacy risk is low **education** might be a suitable use case. Also **testing technology** might be feasible, but there are faster and less complicated options for this use case available.

Dataset Considerations

When deciding, if data is released to the public it is of utmost importance to define, **which variables** are the **most relevant** in terms of **privacy and utility**. This process is very **domain and country specific**, since different areas of the world have different privacy legislation and feature specific overall circumstances. This step would require input and discussions with actual domain experts. Since we are foreign to US privacy law and there is no SAT equivalent in Germany, the assumptions made for the Synthetic Data Challenge are basically a **educated guess** from our side.

From a **utility perspective** it is important to know which variables and correlations are most interesting for actual users of the created synthetic dataset. Different use cases might require focus on different variables and correlations. We could not single out a most important variable, thus in our utility analysis we decided to focus on the overall SAT utility and **not to prioritize a specific variable**. From a data plausibility perspective it was essential to us, that the `sat_v + sat_m = sat_sum` stay consistent.

From a **privacy perspective** it has to be decided, which variables are **confidential** and which are **identifying**. As already mentioned, specifying this depends on multiple factors e.g. **regulations** or also **other public information**, that could be used for **de-anonymization**. For our analysis, we made the following assumptions: Feature `sex` is an identifying value. For the SAT percentiles (`sat_v`, `sat_m`, `sat_sum`) there can be argued in both directions, but we decided for it to be an identifying variable. The same holds for the grade point average `fy_gpa`. We assumed the grade point average to be more confidential than the SAT results. It is very likely for example that students who passed the SAT exchanged about their grades with their fellow students or that teachers know about the SAT results of their students. So these (older) information potentially can be used to **identify a student** within a dataset and find out about the **(newer) information of grade point average**. The calculus behind this decision is that the older information about a test, that is only used to get the college admission, is **less confidential than the newer information** about actual grades, which might give information about a student's current situation.

Method Considerations

Minutemen was the second place submission in the third round of the 2021 NIST differential privacy temporal map challenge. The technique is based on **probabilistic graphical models** and according to their authors best for **categorical and discrete features**. We used the python scripts as descibed by the Synthetic Data challenge. We also used the **descretize** and **un-discretize** steps.

Privacy and Risk Evaluation

Disclosure Risk (R-Package: synthpop with own Improvements)

Our starting point was the **matching of unique records**, as described in the disclosure risk measures chapter of the starter guide. The synthpop package provides us with an easy-to-use implementation of this method: `replicated.uniques`. However, one downside of just using `replicated.uniques` is that it does **not consider almost exact matches in numeric variables**. Imagine a data set with

information about the respondents' income. If there is a matching data point in the synthetic data set for a unique person in the original data set, that only differs by a slight margin, the original function would not identify this as a match. **Our solution** is to borrow the notion of the **p% rule** from **cell suppression methods**, which identifies a data point as critical, if one can guess the original values with **some error of at most p%**. Thus, **our improved risk measure** is able to evaluate disclosure risk in numeric data. Our Uniqueness-Measure for **"almost exact"** matches provides us with the following outputs:

- **Replication Uniques** | Number of unique records in the synthetic data set that replicates unique records in the original data set w.r.t. their quasi-identifying variables. In brackets, the proportion of replicated uniques in the synthetical data set relative to the original data set size is stated.
- **Disclosure in >= 1 CVar** | Number of replicated unique records in the synthetical data set that have a real disclosure risk in at least one confidential variable, i.e. there is at least one confidential variable where the record in the synthetical data set is "too close" to the matching unique record in the original data set. We identify two records as "too close" in a variable, if they differ in this variable by at most p%. In brackets, the described number is given in proportion to the original data set size.
- **Disclosure in 2 CVars** | Number of replicated unique records in the synthetical data set that have a real disclosure risk in both confidential variables, i.e. in both of the confidential variables the record in the synthetical data set is "too close" to the matching unique record in the original data set. We identify two records as "too close" in a variable, if they differ in this variable by at most p%. In brackets, the described number is given in proportion to the original data set size.

For our selected best parametrized solution in this method-category, we got the following results:

Replication.Uniques	Disclosure.in.>=1.CVar	Disclosure.in.2.CVars
2 (0.2%)	0 (0%)	0 (0%)

Perceived Disclosure Risk (R-Package: synthpop)

Unique records in the synthetic dataset may be **mistaken for unique records** based on the fact, that **only the identifying variables match**. This can lead to problems, even if the associated confidential variables significantly differ from the original record. E.g. people might assume a certain income for a person, because they believe to have identified him from the identifying variables. Even if his real income **is not leaked** (as the confidential variables are different), this assumed (but wrong) information about him **might lead to disadvantages**. The **perceived risk** is measured by matching the unique records among the identifying variables, in our case `sex`, `sat_v`, `sat_m` and `sat_sum`. We applied the method `replicated.uniques` of the synthpop package. There is no fixed threshold that must not be exceeded in this measure, however, a smaller percentage of unique matches (referred to as Number Replications) is preferred to minimize the perceived disclosure risk.

These are the results variables for perceived disclosure risk:

- **Number Uniques** | Number of unique individuals in the original data set.

- **Number Replications** | The number of matching records in the synthetic data set (based only on identifying variables). This is the number of individuals, which might perceived as disclosed (real disclosures would also count into this metric)
- **Percentage Replications** | The calculated percentage of duplicates in the synthetic data

For our selected best parametrized solution in this method-category, we got the following results:

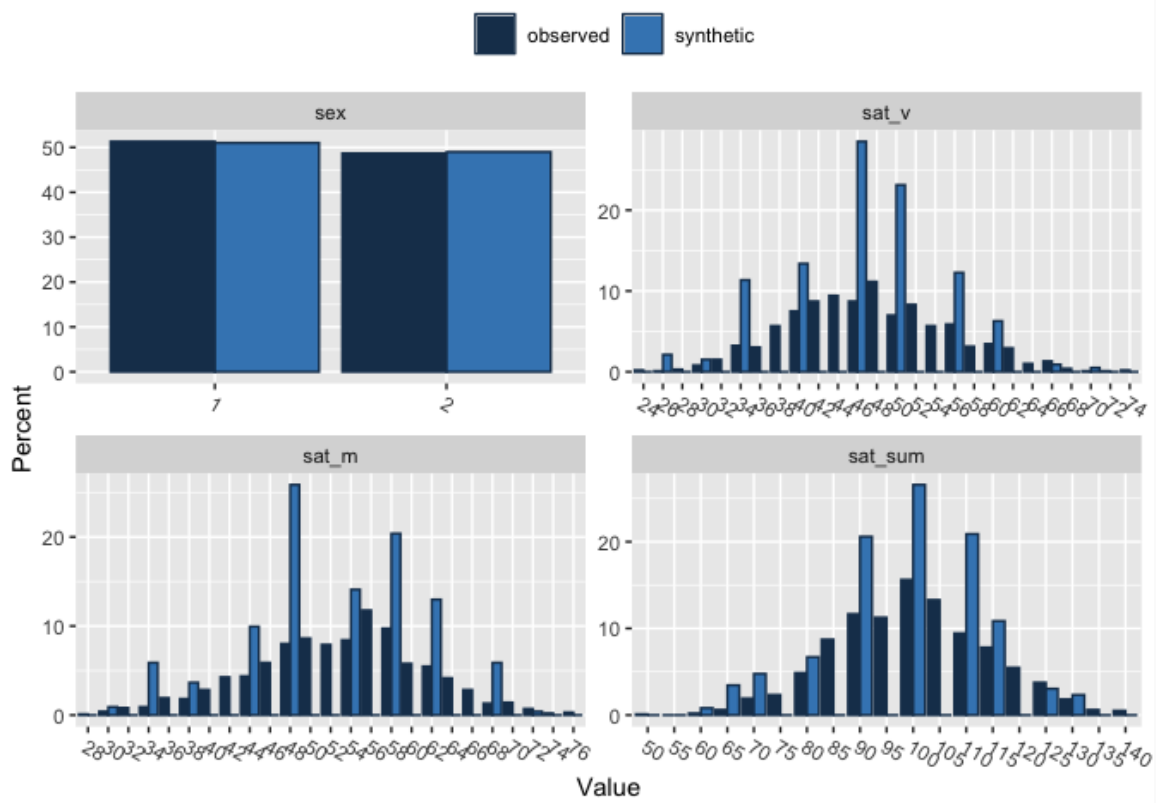
Metric	Number.Uniques	Number.Replications	Percentage.Replications
Perceived Risk	551	2	0.2

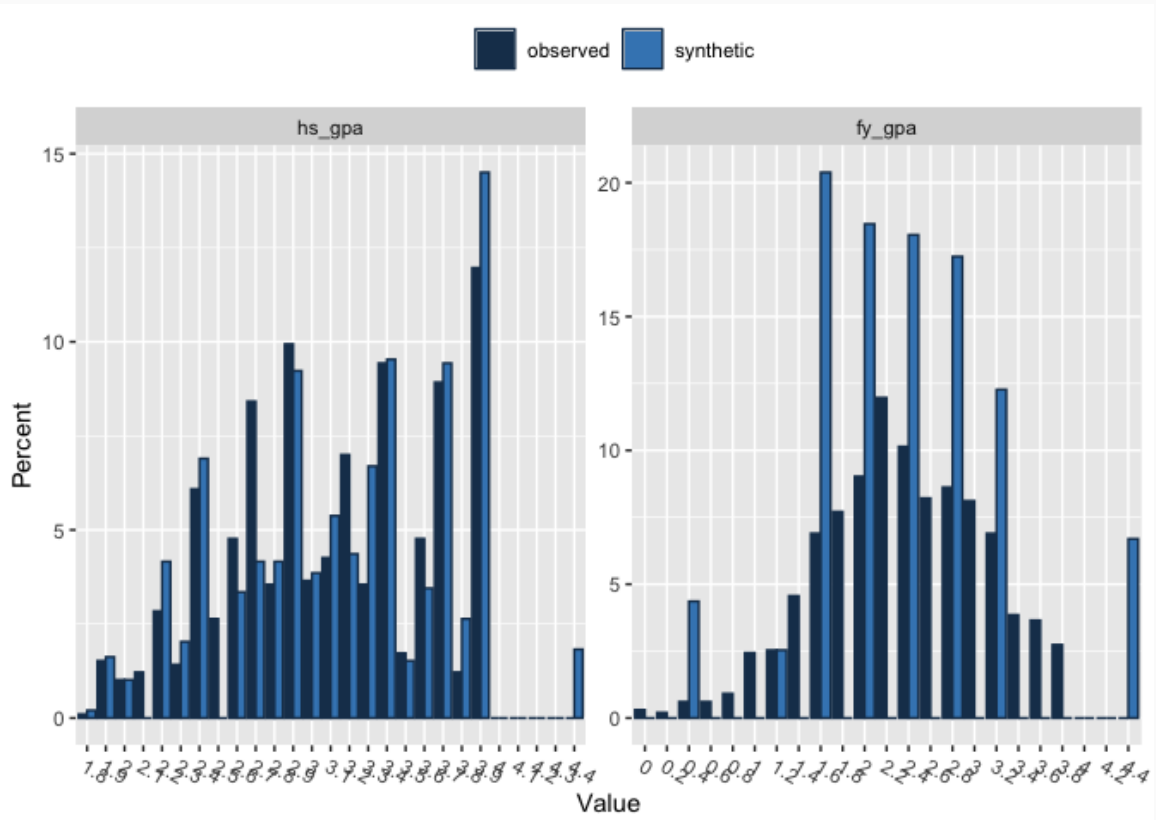
Utility Evaluation

Different utility measures are applied in this section. These utility measures are the basis of the utility evaluation of the generated synthetic dataset. These are the utility measures for our selected dataset after optimization and tuning.

Graphical Comparison for Margins (R-Package: synthpop)

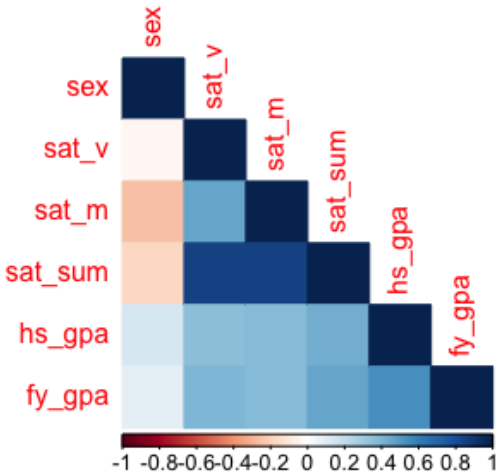
The following histograms provide an ad-hoc overview on the marginal distributions of the original and synthetic dataset. Matching or close distributions are related to a high data utility.

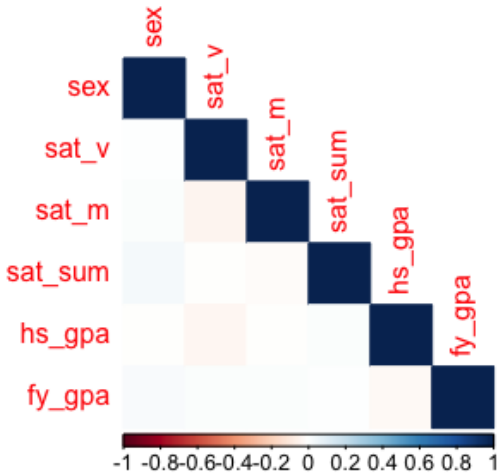




Correlation Plots for Graphical Comparison of Pearson Correlation

Synthetic Datasets should represent the dependencies of the original datasets. The following correlation plots provide an ad-hoc overview on the Pearson correlations of the original and synthetic dataset. The left plot shows the original correlation whereas the right plot provides the correlation based on the synthetic dataset.





Kolmogorov-Smirnov Test

The Kolmogorov-Smirnov test is a classic way to compare (marginal) distributions. A significant result indicates that the two distributions are not identical. The following statistic show the share of variables in the synthetic dataset that have a p-value > 5%. (1: 100%, 0: 0%)

Mean_KS_not_signif
0.17

Mahalanobis Distance for Regression Parameters

To assess testing analysis, coefficients and standard errors calculated based on synthetic dataset should lead to the same results when calculated on the original data. The evaluate differences and taking the variance covariance matrix into account, we calculated the mahalanobis distance between the respective regression parameters. Since we used several regression models, we present the mean of cases in which the mahalanobis distance exceeded the critial value (0: excellent; 1: poor).

Mahalanobis.Distance
1

Distributional Comparison of Synthesised Data (R-Package: synthpop) by (S_)pMSE

Propensity scores are calculated on a combined dataset (original and synthetic). A model (here: CART) tries to identify the synthetic units in the dataset. Since both datasets should be identically structured, the pMSE should equal zero. The S_pMSE (standardised pMSE) should not exceed 10 and for a good fit

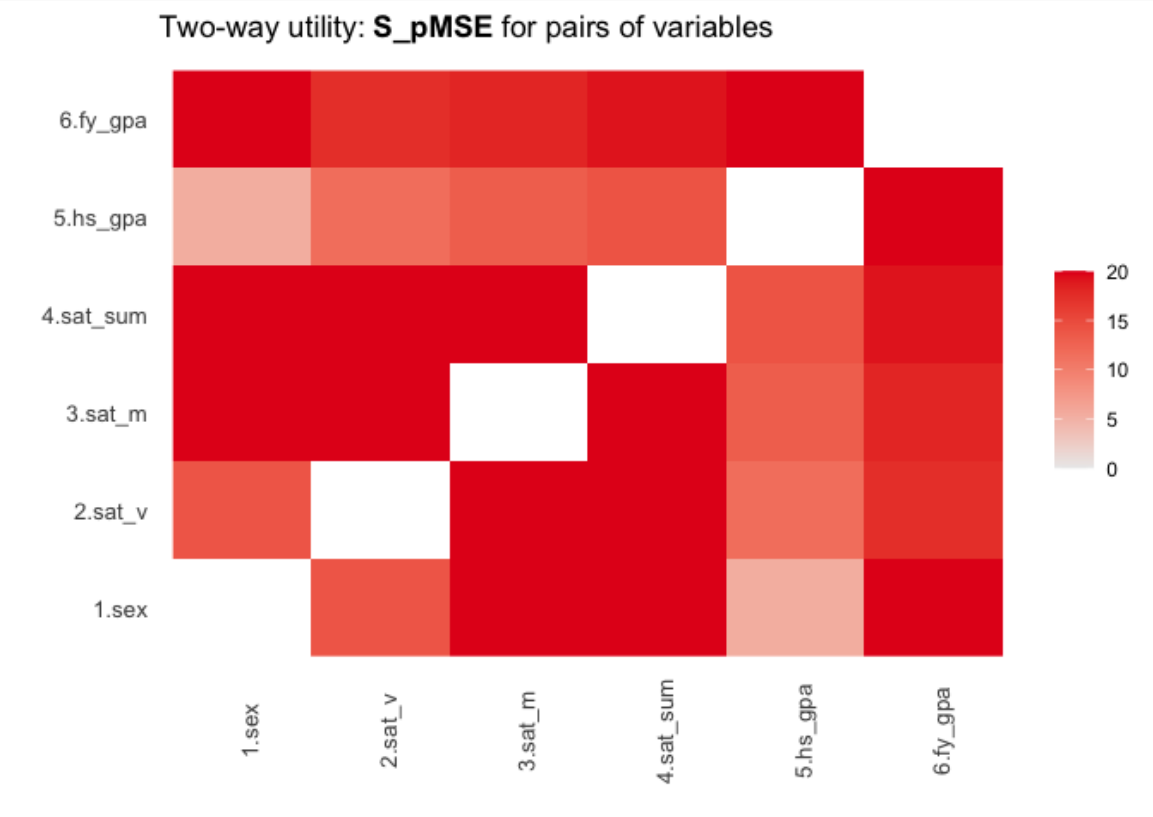
below 3 according to Raab (2021, https://unece.org/sites/default/files/2021-12/SDC2021_Day2_Raab_AD.pdf)

	pMSE	S_pMSE	df
sex	0.0000023	0.036531	1
sat_v	0.0073295	28.907457	4
sat_m	0.0088567	34.930988	4
sat_sum	0.0087139	34.367791	4
hs_gpa	0.0018019	7.106789	4
fy_gpa	0.0121734	48.011889	4

pMSE	S_pMSE
0.2360304	6.078917

Two-way Tables Comparison of Synthesised Data (R-Package: synthpop) by (S_)pMSE

Two-way tables are evaluated based on the original and the synthetic dataset. Here, tables/cells are also evaluated based on pMSE and S_pMSE (see above). We also present the results for the mean absolute difference in densities (MabsDD).



	pMSE	S_pMSE	MabsDD
1.sex:2.sat_v	0.0080081	14.037395	0.3022312

	pMSE	S_pMSE	MabsDD
1.sex:3.sat_m	0.0127741	22.391644	0.3975659
1.sex:4.sat_sum	0.0121017	21.212860	0.3853955
1.sex:5.hs_gpa	0.0030885	5.413782	0.1825558
1.sex:6.fy_gpa	0.0125796	22.050573	0.3549696
2.sat_v:3.sat_m	0.0318758	20.953029	0.6105477
2.sat_v:4.sat_sum	0.0683884	44.953963	0.8904665
2.sat_v:5.hs_gpa	0.0178043	11.703328	0.4259635
2.sat_v:6.fy_gpa	0.0265092	17.425363	0.5375254
3.sat_m:4.sat_sum	0.0723831	47.579835	0.9188641
3.sat_m:5.hs_gpa	0.0202252	13.294672	0.4604462
3.sat_m:6.fy_gpa	0.0277191	18.220697	0.5456389
4.sat_sum:5.hs_gpa	0.0215621	14.173472	0.4908722
4.sat_sum:6.fy_gpa	0.0292751	19.243529	0.5517241
5.hs_gpa:6.fy_gpa	0.0314999	20.705920	0.5862069

Information Loss Measure Proposed by Andrzej Mlodak (R-Package: sdcMicro)

The value of this information loss criterion is between 0 (no information loss) and 1. It is calculated overall and for each variable.

Information.Loss
0.6311789

Individual Distances for Information Loss:

sex	sat_v	sat_m	sat_sum	hs_gpa	fy_gpa
0.4959432	0.8421066	0.8389337	0.8942229	0.3219322	0.3939348