TALL SOM FORTELLER

A Disclosure-Based Framework for Comparing Frequency Table Protection

DANIEL P. LUPP AND ØYVIND LANGSGRUD

Statistisk sentralbyrå
Statistics Norway

Background

- Work as part of a grant for publishing multigrid geographical data on the 2021 population census
- Goal: compare perturbative methods to determine best solution for Norway

This talk:

- Present comparison framework
- Discuss results for 2021 population census

Comparison framework

- Measure risk
  - Describe disclosure scenarios
  - Count and compare disclosures in original and perturbed data
  - Exclude methods with unacceptable risk
- Measure utility
  - Of remaining measures, keep methods with highest utility

Disclosure scenario

Attribute disclosure

- all records in a table marginal share the same attribute for a given variable

Municipality	Unemployed	Employeed	Self-employed	Total
M1	12	0	0	12
M2	5	6	0	11

Disclosure scenario

Attribute disclosure when total is 1*

- Similar to ordinary attribute disclosure, but limited to marginal cells where the population total is (known to be) 1

Municipality	Unemployed	Employeed	Self-employed	Total
M1	*3*	0	0	*3* (1)
M2	5	6	0	11

Value is known to be 1

*relevant in, e.g., sparsely populated countries, where even large geographical areas can contain very few inhabitants

Disclosure scenario

Negative attribute disclosure

- When no record contributing to a marginal cell has a certain attribute

Municipality	Unemployed	Employeed	Self-employed	Total
M1	12	0	0	12
M2	5	6	0	11

Disclosure scenario

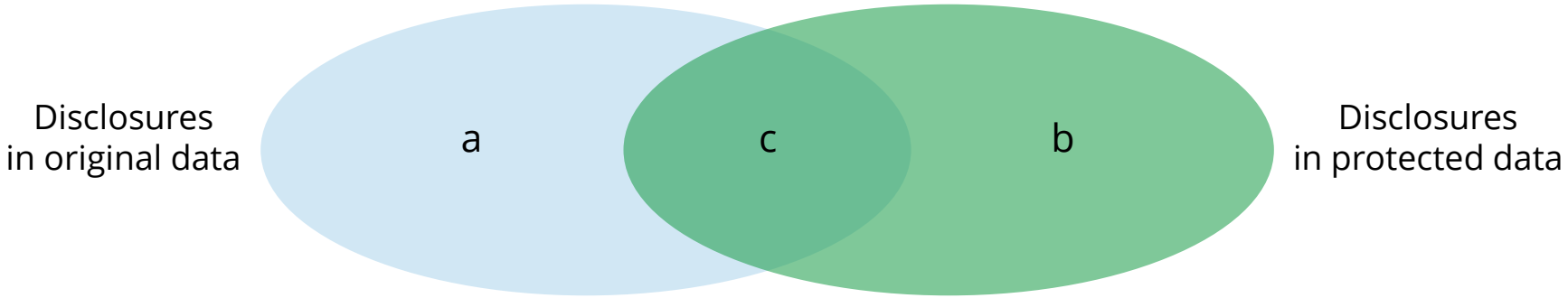
Disclosure of existence

- Any non-zero frequency discloses that at least one record has a certain attribute

Municipality	Unemployed	Employeed	Self-employed	Total
M1	12	0	0	12
M2	5	6	0	11

Measuring risk

- Use measures from information retrieval



- Precision: $\frac{c}{b}$ *Approx. probability that a disclosure is real*
- Recall: $\frac{c}{a}$ *Proportion of real disclosures in «visible» data*

Measuring utility

- Maximum absolute deviation

$$\max_i |y_i^* - y_i|$$

- Average absolute deviation

$$\frac{1}{n}\sum_{i=1}^{n} |y_i^* - y_i|$$

- Hellinger distance

$$\sqrt{\frac{1}{2}\sum_{i=1}^{n}\left(\sqrt{y_i^*} - \sqrt{y_i}\right)^2}$$

Applied to 2021 population census grids

- Cell key method
  - Idea: noise based on which records contribute to a cell
  - No additivity in tables
- Targeted record swapping
  - Idea: swap units with risk of disclosure with units from neighboring areas
- Small count rounding
  - idea: round the inner cells (microdata aggregated to frequencies)
  - Maintains additivity within and consistency across tables

Different flavors considered

Comparison was done with many (combinations of) methods. For illustration, we only show:

- Cell key method with/without targetted record swapping:
  - Labels CK and CKswk2r01 respectively
- Small count rounding:
  - SCRsimple: simple method, inner cells that are 1 or 2 are rounded to 0 or 3
  - SCRzeros: same as simple, but zeros rounded as well
  - SCRforceInner: all inner cells are rounded to multiple of 3

Risk threshold

Need to define what is «acceptable risk»

- This was difficult, so we rather defined «unacceptable risk» as precision or recall at 100%
- This was actually sufficient to reach a conclusion

Results: Risk

TABLE 2. Attribute disclosure risk (ordinary and where original population is 1) measured as precision and recall.

	Precision		*Recall*	
Method	Ordinary	Total is 1	Ordinary	Total is 1
~~CK~~	~~61.09~~	~~100.00~~	~~67.50~~	~~26.27~~
CKswk2r01	42.88	58.36	42.38	58.04
~~SCRsimple~~	~~59.84~~	~~100.00~~	~~63.14~~	~~24.43~~
SCRzeros	55.95	85.05	57.54	23.97
SCRforceInner	52.92	79.48	53.15	22.48

TABLE 3. Risk of disclosure of existence measured as precision and limited to cases where the perturbed frequency has a specific value (1-6). Values less than 3 are not published, hence the first two columns are empty.

Method	1	2	3	4	5	6
~~CK~~			~~100.00~~	~~100.00~~	~~100.00~~	~~100.00~~
CKswk2r01			80.99	84.88	88.89	92.89
~~SCRsimple~~			~~100.00~~	~~100.00~~	~~100.00~~	~~100.00~~
~~SCRzeros~~			~~92.77~~	~~100.00~~	~~100.00~~	~~99.71~~
SCRforceInner			89.65			99.16

Results: Utility

TABLE 4. Utility measures for each perturbative method.

Method	Maximum absolute deviation	Average abs… deviation	…tance
~~CK~~	~~5~~	~~…~~	~~886.6~~
~~CKswk2r01~~	~~13401~~	~~2.098~~	~~1245.8~~
~~SCRsimple~~	~~17~~	~~0.944~~	~~891.5~~
~~SCRzeros~~	~~15~~	~~1.008~~	~~968.6~~
SCRforceInner	19	1.304	1052.3

Approx. 35% of original cell value

Concluding remarks

- Comparison done with Norwegian use case in mind
- Possible refinements: consider loss of information as utility measure
  - E.g., Kullbach-Leibler divergence, variation of information
- Risk measures can work on non-perturbative measures, but work is needed to compare utility loss between non-perturbative and perturbative measures.

TALL SOM FORTELLER

Takk!

Statistisk sentralbyrå
Statistics Norway