Protecting Tabular Data through Cyclic Perturbation

George Duncan and Steve Roehrig

NCES
2006 December 7

Carnegie Mellon
Policy • Management • Information Technology
Heinz School

Table of Counts

	w_1	w_2	w_3	w_4	
v_1	15	1	3	1	20
v_2	20	10	10	15	55
v_3	3	10	10	2	25
v_4	12	14	7	2	35
	50	35	30	20	135

Look For Risky Cells

	w_1	w_2	w_3	w_4	
v_1	15	1	3	1	20
v_2	20	10	10	15	55
v_3	3	10	10	2	25
v_4	12	14	7	2	35
	50	35	30	20	135

Apply Disclosure Limitation

- Coarsening
  - Aggregate attributes
- Suppress some cells
  - Publish only the marginal totals
  - Suppress the sensitive cells, plus others as necessary
- Perturb some cells
  - Round
  - Fuzz

Perturbation Methods

- Controlled rounding (Cox)
- Controlled tabular adjustment (Cox & Dandekar)
  – Replace sensitive cell values with safe values and adjust other cells so that the table “adds up”
- Cyclic perturbation (Duncan & Roehrig)
  – Stochastically modify cell values in a known way, allowing a Bayesian analysis of cell value distributions

Releasing Only the Margins

- 18,272,363,056 tables have our margins (thanks to De Loera & Sturmfels)
- Low disclosure risk, but low data utility
- Easy!
- Very commonly done
- Statistical users might estimate internal cells with, e.g., iterative proportional fitting

Suppress Primary Cells + Complementary Cells

	w_1	w_2	w_3	w_4	
v_1	15	s	s	s	20
v_2	20	10	10	15	55
v_3	3	10	s	s	25
v_4	12	s	7	s	35
	50	35	30	20	135

- This may not be a good suppression pattern: only three possible original tables ...
- Hard to do well
- Users have no way of estimating cell value, probabilities

Controlled Rounding

	w_1	w_2	w_3	w_4	
v_1	15	0	3	0	18
v_2	21	9	12	15	57
v_3	3	9	9	3	24
v_4	12	15	6	3	36
	51	33	30	21	135

Example of base 3 rounding

- Uniform (and known) feasibility interval
- Easy for 2-D tables, perhaps impossible for 3-D
- If we know the *exact* method, we can find the cell distributions
- 1,025,908,683 possible original tables

Alternative Approach: Cyclic Perturbation

- Make perturbation consistent with common error structure—misclassification
- Methods for misclassified categorical data
  - T. Timothy Chen (1989) Statistics in Medicine
  - Jouni Kuha and Chris Skinner (1997) “Categorical data analysis and misclassification”

Cyclic Perturbation: Basics

- Choose cycles that leave the margins fixed, like

Original, Cycle, Perturbed table

$$\begin{array}{|cccc|} \hline 15 & 1 & 3 & 1 \\ 20 & 10 & 10 & 15 \\ 3 & 10 & 10 & 2 \\ 12 & 14 & 7 & 2 \\ \hline \end{array} + \begin{array}{|cccc|} \hline 1 & 0 & -1 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline \end{array} = \begin{array}{|cccc|} \hline 16 & 1 & 2 & 1 \\ 19 & 10 & 11 & 15 \\ 3 & 10 & 10 & 2 \\ 12 & 14 & 7 & 2 \\ \hline \end{array}$$

- The set of cycles determines the published table's feasibility interval

Cyclic Perturbation: Details

- Choose a set of cycles that covers all table cells “equally”. Example:

+	-	0	0
0	+	-	0
0	0	+	-
-	0	0	+

0	+	-	0
0	0	+	-
-	0	0	+
+	-	0	+

0	0	+	-
-	0	0	+
+	-	0	0
0	+	-	0

-	0	0	+
+	-	0	0
0	+	-	0
0	0	+	-

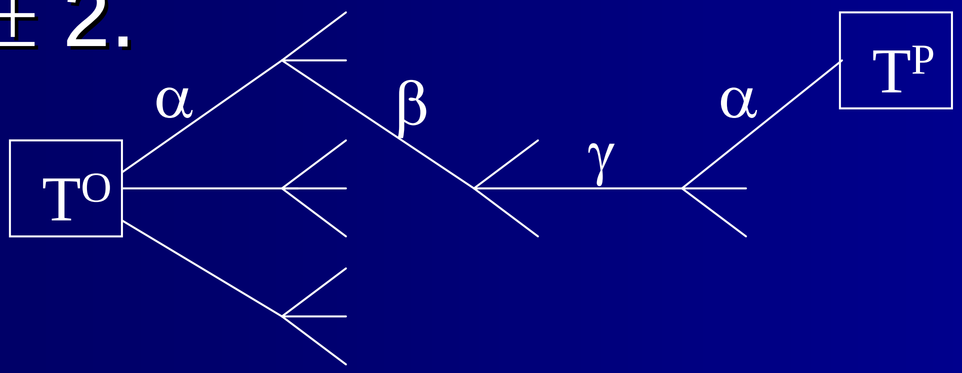
Each cell has exactly two “chances” to move.

Cyclic Perturbation: Details

- Flip a three-sided coin with outcomes
  - A (probability = α)
  - B (probability = β)
  - C (probability = γ)
- If A, add the first cycle (unless there is a zero in the cycle)
- If B, subtract the first cycle (unless there is a zero in the cycle)
- If C, do nothing
- Repeat with the remaining cycles

Cyclic Perturbation: Details

- For the chosen set of cycles, there are $3^4 = 81$ possible perturbed tables.
- The feasibility interval is original value $\pm$ 2.



Original Table

Perturbed Table

Cyclic Perturbation: Details

- Choose α, β.
- Perturb.
- Publish the resulting table.
- *Publish the cycles and α, β.*

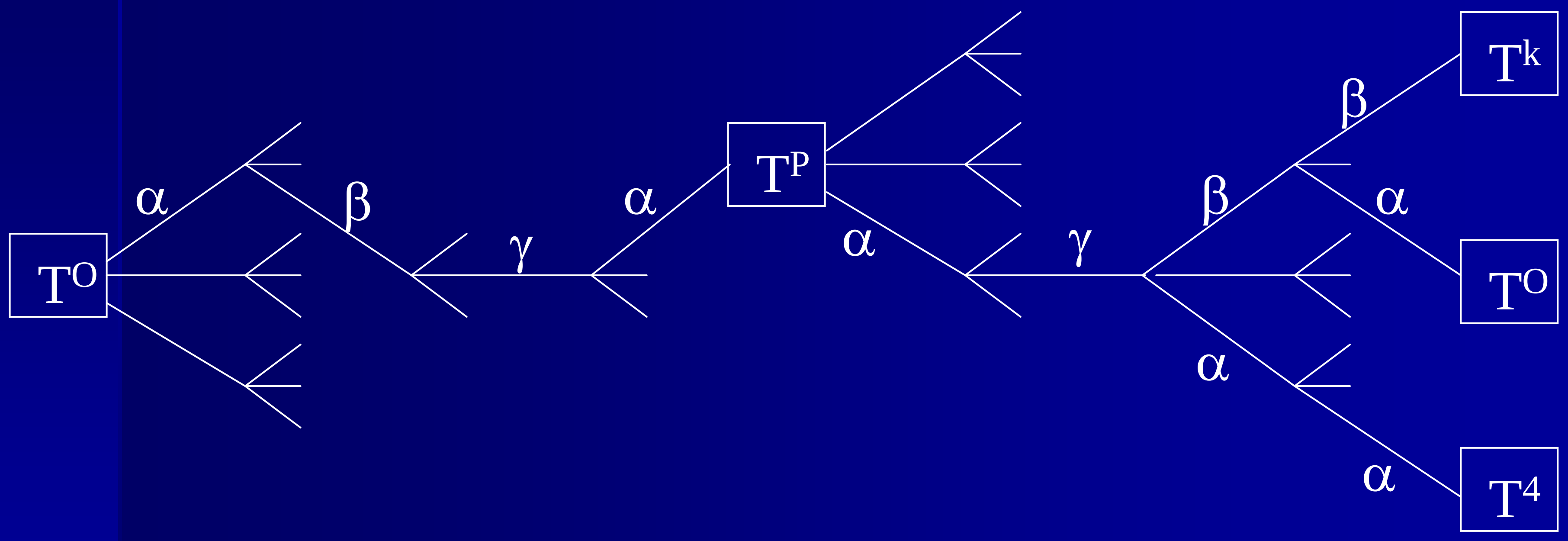
Original

15	1	3	1
20	10	10	15
3	10	10	2
12	14	7	2

Perturbed table

16	0	2	2
21	11	9	14
2	11	11	1
11	13	8	3

Analysis of Cell Probabilities



Original Table

Perturbed Table

Possible Tables

Distributions of Cell Values

- Since the mechanism is public, a user can calculate the distribution of true cell values.
- Compute every table T^k that *could have been* the original, along with the probability $\Pr(T^P \mid T^k)$.
- Specify a prior distribution over all the possible original tables T^k.
- Apply Bayes' theorem to get the posterior probability $\Pr(T^k \mid T^P)$ for each T^k.
- The distribution for each cell is

$$\Pr(t(i,j)=q) = \sum_{k:t_k(i,j)=q} \Pr(T_k \mid T^P)$$

Results for the Example

Original

15	1	3	1
20	10	10	15
3	10	10	2
12	14	7	2

Perturbed table

16	0	2	2
21	11	9	14
2	11	11	1
11	13	8	3

q =	0	1	2	3	4	5
$\Pr(\, t(1,2) = q \mid T^P \,)$	0.71	0.25	0.04	0.00	0.00	0.00
$\Pr(\, t(1,4) = q \mid T^P \,)$	0.06	0.25	0.38	0.25	0.06	0.00
$\Pr(\, t(3,4) = q \mid T^P \,)$	0.00	0.71	0.25	0.04	0.00	0.00
$\Pr(\, t(4,4) = q \mid T^P \,)$	0.00	0.05	0.29	0.44	0.21	0.01

Properties

- It’s not difficult to quantify data utility and disclosure risk (*cf.* cell suppression and controlled rounding).
- Priors of data users and data intruders can be different.
- **Theorem:** For a uniform prior, the mode of each posterior cell distribution is it’s published value.

Scaling

- Sets of cycles w/ desirable properties are easy to find for larger 2-D tables.
- Extensions to 3 and higher dimensions also straightforward.
- Computing the perturbation for any size table is easy & fast.
- The complete Bayesian analysis is feasible to at least 20×20 (with no special TLC)

What Might Priors Be?

- They could reflect historical data
- If I'm in the survey, I know my cell is at least 1
- Public information
- Insider information

Cell Suppression & Rounding

- A similar Bayesian analysis can be done, provided the *exact* algorithm is available.
- It's generally *much* harder to do.
- Using a deterministic version of Cox's `87 rounding procedure, we must consider "only" 17,132,236 tables.
- For uniform priors, the posterior cell distributions were nearly uniform.
- Three days of computing time for a 4×4 table...

A 3-Way Categorical Table (margins not shown)

j

i

1	4	66	3
1	2	3	1
4	4	3	1
2	7	1	3

k = 1

2	3	2	68
228	4	78	3
1	5	6	61
10	3	1	2

k = 2

4	80	2	1
4	2	2	1
3	4	4	45
61	3	55	4

k = 3

(Source: Java Random.nextInt())

A Set of Margin-Preserving Perturbations

$$M_1 = \boxed{\begin{matrix} + & - & 0 & \cdot \\ \cdot & + & - & 0 \\ 0 & \cdot & + & - \\ - & 0 & \cdot & + \end{matrix}}$$

A Set of Margin-Preserving Perturbations

$$M_1 = \boxed{\begin{array}{cccc} + & - & 0 & \cdot \\ \cdot & + & - & 0 \\ 0 & \cdot & + & - \\ - & 0 & \cdot & + \end{array}} \quad \boxed{\begin{array}{cccc} 0 & + & - & \cdot \\ \cdot & 0 & + & - \\ - & \cdot & 0 & + \\ + & - & \cdot & 0 \end{array}}$$

A Set of Margin-Preserving Perturbations

$$M_1 = \begin{array}{|cccc|}\hline + & - & 0 & \cdot \\ \cdot & + & - & 0 \\ 0 & \cdot & + & - \\ - & 0 & \cdot & + \\ \hline \end{array} \quad \begin{array}{|cccc|}\hline 0 & + & - & \cdot \\ \cdot & 0 & + & - \\ - & \cdot & 0 & + \\ + & - & \cdot & 0 \\ \hline \end{array} \quad \begin{array}{|cccc|}\hline - & 0 & + & \cdot \\ \cdot & - & 0 & + \\ + & \cdot & - & 0 \\ 0 & + & \cdot & - \\ \hline \end{array}$$

A Set of Margin-Preserving Perturbations

$$M_1 = \boxed{\begin{array}{cccc} + & - & 0 & \cdot \\ \cdot & + & - & 0 \\ 0 & \cdot & + & - \\ - & 0 & \cdot & + \end{array}} \quad \boxed{\begin{array}{cccc} 0 & + & - & \cdot \\ \cdot & 0 & + & - \\ - & \cdot & 0 & + \\ + & - & \cdot & 0 \end{array}} \quad \boxed{\begin{array}{cccc} - & 0 & + & \cdot \\ \cdot & - & 0 & + \\ + & \cdot & - & 0 \\ 0 & + & \cdot & - \end{array}}$$

A Set of Margin-Preserving Perturbations

$$M_1 = \begin{array}{|cccc|}\hline + & - & 0 & \cdot \\ \cdot & + & - & 0 \\ 0 & \cdot & + & - \\ - & 0 & \cdot & + \\ \hline\end{array} \quad \begin{array}{|cccc|}\hline 0 & + & - & \cdot \\ \cdot & 0 & + & - \\ - & \cdot & 0 & + \\ + & - & \cdot & 0 \\ \hline\end{array} \quad \begin{array}{|cccc|}\hline - & 0 & + & \cdot \\ \cdot & - & 0 & + \\ + & \cdot & - & 0 \\ 0 & + & \cdot & - \\ \hline\end{array}$$

$$M_2 = \begin{array}{|cccc|}\hline - & 0 & \cdot & + \\ + & - & 0 & \cdot \\ \cdot & + & - & 0 \\ 0 & \cdot & + & - \\ \hline\end{array} \quad \begin{array}{|cccc|}\hline + & - & \cdot & 0 \\ 0 & + & - & \cdot \\ \cdot & 0 & + & - \\ - & \cdot & 0 & + \\ \hline\end{array} \quad \begin{array}{|cccc|}\hline 0 & + & \cdot & - \\ - & 0 & + & \cdot \\ \cdot & - & 0 & + \\ + & \cdot & - & 0 \\ \hline\end{array}$$

A Set of Margin-Preserving Perturbations

$$M_1 = \boxed{\begin{array}{cccc} + & - & 0 & \cdot \\ \cdot & + & - & 0 \\ 0 & \cdot & + & - \\ - & 0 & \cdot & + \end{array}} \quad \boxed{\begin{array}{cccc} 0 & + & - & \cdot \\ \cdot & 0 & + & - \\ - & \cdot & 0 & + \\ + & - & \cdot & 0 \end{array}} \quad \boxed{\begin{array}{cccc} - & 0 & + & \cdot \\ \cdot & - & 0 & + \\ + & \cdot & - & 0 \\ 0 & + & \cdot & - \end{array}}$$

$$M_2 = \boxed{\begin{array}{cccc} - & 0 & \cdot & + \\ + & - & 0 & \cdot \\ \cdot & + & - & 0 \\ 0 & \cdot & + & - \end{array}} \quad \boxed{\begin{array}{cccc} + & - & \cdot & 0 \\ 0 & + & - & \cdot \\ \cdot & 0 & + & - \\ - & \cdot & 0 & + \end{array}} \quad \boxed{\begin{array}{cccc} 0 & + & \cdot & - \\ - & 0 & + & \cdot \\ \cdot & - & 0 & + \\ + & \cdot & - & 0 \end{array}}$$

$$M_3 = \boxed{\begin{array}{cccc} 0 & \cdot & + & - \\ - & 0 & \cdot & + \\ + & - & 0 & \cdot \\ \cdot & + & - & 0 \end{array}} \quad \boxed{\begin{array}{cccc} - & \cdot & 0 & + \\ + & - & \cdot & 0 \\ 0 & + & - & \cdot \\ \cdot & 0 & + & - \end{array}} \quad \boxed{\begin{array}{cccc} + & \cdot & - & 0 \\ 0 & + & \cdot & - \\ - & 0 & + & \cdot \\ \cdot & - & 0 & + \end{array}}$$

A Set of Margin-Preserving Perturbations

$$M_1 = \boxed{\begin{array}{cccc} + & - & 0 & \cdot \\ \cdot & + & - & 0 \\ 0 & \cdot & + & - \\ - & 0 & \cdot & + \end{array}} \quad \boxed{\begin{array}{cccc} 0 & + & - & \cdot \\ \cdot & 0 & + & - \\ - & \cdot & 0 & + \\ + & - & \cdot & 0 \end{array}} \quad \boxed{\begin{array}{cccc} - & 0 & + & \cdot \\ \cdot & - & 0 & + \\ + & \cdot & - & 0 \\ 0 & + & \cdot & - \end{array}}$$

$$M_2 = \boxed{\begin{array}{cccc} - & 0 & \cdot & + \\ + & - & 0 & \cdot \\ \cdot & + & - & 0 \\ 0 & \cdot & + & - \end{array}} \quad \boxed{\begin{array}{cccc} + & - & \cdot & 0 \\ 0 & + & - & \cdot \\ \cdot & 0 & + & - \\ - & \cdot & 0 & + \end{array}} \quad \boxed{\begin{array}{cccc} 0 & + & \cdot & - \\ - & 0 & + & \cdot \\ \cdot & - & 0 & + \\ + & \cdot & - & 0 \end{array}}$$

$$M_3 = \boxed{\begin{array}{cccc} 0 & \cdot & + & - \\ - & 0 & \cdot & + \\ + & - & 0 & \cdot \\ \cdot & + & - & 0 \end{array}} \quad \boxed{\begin{array}{cccc} - & \cdot & 0 & + \\ + & - & \cdot & 0 \\ 0 & + & - & \cdot \\ \cdot & 0 & + & - \end{array}} \quad \boxed{\begin{array}{cccc} + & \cdot & - & 0 \\ 0 & + & \cdot & - \\ - & 0 & + & \cdot \\ \cdot & - & 0 & + \end{array}}$$

$$M_4 = \boxed{\begin{array}{cccc} \cdot & + & - & 0 \\ 0 & \cdot & + & - \\ - & 0 & \cdot & + \\ + & - & 0 & \cdot \end{array}} \quad \boxed{\begin{array}{cccc} \cdot & 0 & + & - \\ - & \cdot & 0 & + \\ + & - & \cdot & 0 \\ 0 & + & - & \cdot \end{array}} \quad \boxed{\begin{array}{cccc} \cdot & - & 0 & + \\ + & \cdot & - & 0 \\ 0 & + & \cdot & - \\ - & 0 & + & \cdot \end{array}}$$

Properties of the Perturbations

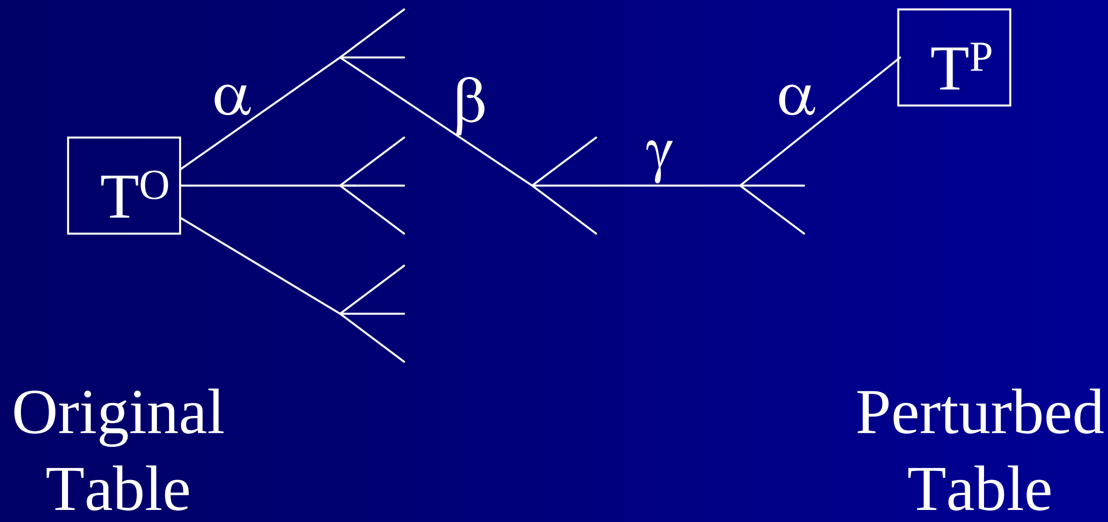
- Each cycle maintains 2-d margins
- Each cell has the same (small) number of “opportunities” to move
- Small cells are not “favored”, so no disclosure from knowledge of the perturbation set

Cyclic Perturbation: Details

- Flip a three-sided coin with outcomes
  - A, with probability = α
  - B, with probability = β
  - C, with probability = $\gamma = 1 - (\alpha + \beta)$
- If A, add the first cycle to the table (unless there is a zero in the cycle)
- If B, subtract the first cycle (unless there is a zero in the cycle)
- If C, do nothing
- Repeat with the remaining cycles

Cyclic Perturbation: Details

- For the chosen set of cycles, there are $3^4=81$ possible perturbed tables.
- The feasibility interval of each cell is its original value $\pm$ 2.



Cyclic Perturbation: Details

- Choose a perturbation set
- Choose α, β
- Perturb
- Publish the resulting table
- *Publish the perturbation set and* α, β

Original & Perturbed Tables

1	4	66	3
1	2	3	1
4	4	3	1
2	7	1	3

2	3	2	68
228	4	78	3
1	5	6	61
10	3	1	2

4	80	2	1
4	2	2	1
3	4	4	45
61	3	55	4

1	5	65	3
1	2	4	0
3	4	3	2
3	6	1	3

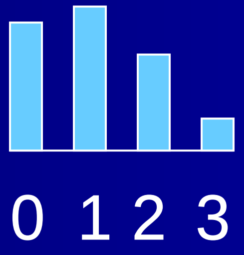
2	3	3	67
227	4	78	4
2	4	6	61
10	4	0	2

4	79	2	2
5	2	1	1
3	5	4	44
60	3	56	4

Results for the Example

- There are 28 tables that could have been the original
- We have a posterior probability for each
- We can find distributions for cell values
- Example: cell (1,1,1) with $\alpha = \beta = \gamma$

Value	0	1	2	3
Probability	0.34	0.39	0.22	0.05



Cyclic Perturbation Advantages

- Quantify disclosure risk (perhaps using an "intruder prior")
- Quantify data utility (perhaps using a "user prior")
- Perform statistical analyses on the set of possible true tables and their associated probabilities
- The procedure is unbiased with $\alpha=\beta$, and for uniform priors, the mode of every cell distribution is the published value

More Advantages …

- Users know exactly how the data have been modified, up to a known stochastic component
- The “protection interval” is determined by the set of perturbations; more “opportunities” to move give a wider interval