Cyclic Perturbation: Protecting Confidentiality in Tabular Data

George T. Duncan

Stephen F. Roehrig

Carnegie Mellon University

Start With Some Microdata

Individual	v	w
1	v_1	w_3
2	v_1	w_2
3	v_4	w_3
4	v_2	w_1
5	v_1	w_3
6	v_3	w_4
$\vdots$	$\vdots$	$\vdots$

$$v \in \{v_1, \ldots, v_I\}$$
$$w \in \{w_1, \ldots, w_J\}$$

Count Up to Make a Table

	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 Sensitive 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

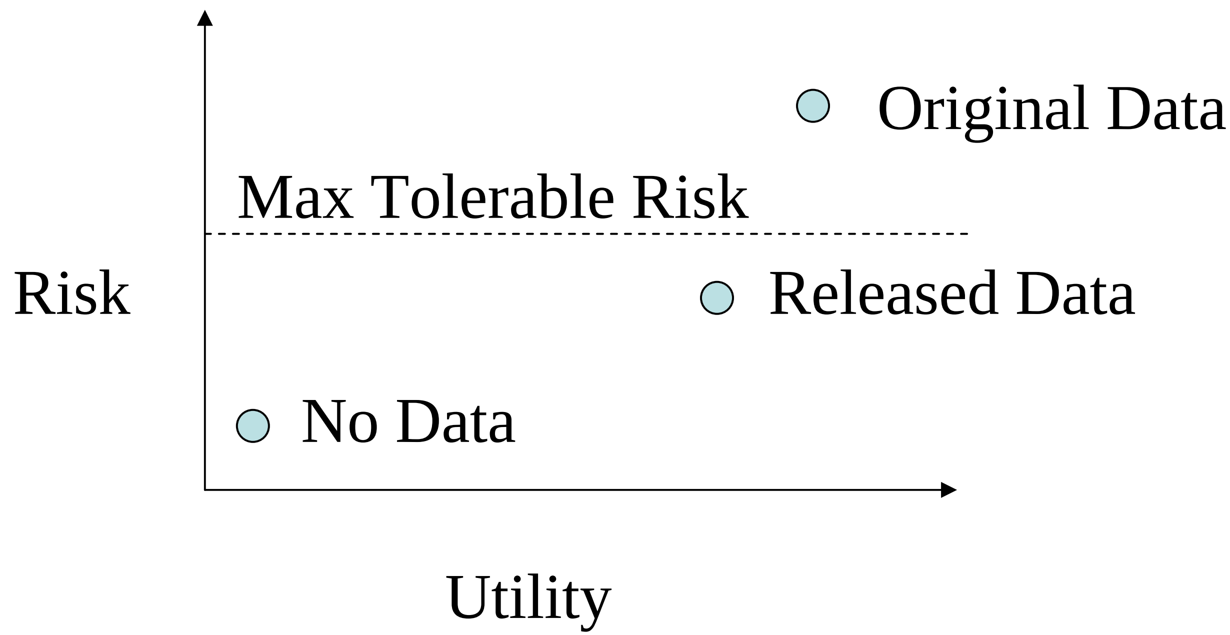
Apply a Disclosure Limitation Method

- Suppress some cells
  - Publish only the marginal totals
  - Suppress the sensitive cells, plus others as necessary
- Perturb some cells
  - Controlled rounding
  - Cyclic perturbation

How to Choose a Method?

- Disclosure risk:
  - the degree to which confidentiality might be compromised
  - perhaps consider feasibility intervals, or better, distributions of possible cell values
- Data utility
  - a measure of the value to a legitimate user
  - higher if errors in a user’s analysis are smaller
  - higher if the user can *estimate* magnitude of errors in analysis based on the released table

The R-U Confidentiality Map



Releasing Only the Margins

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

Suppress Sensitive Cells & Others

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

- This may not be a good suppression pattern: only three possible original tables…
- Hard to do correctly.
- 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.

Cyclic Perturbation: Basics

- Choose cycles that leave the margins fixed.

Original

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

+

Cycle

1	0	-1	0
-1	0	1	0
0	0	0	0
0	0	0	0

=

Perturbed table

16	1	2	1
19	10	11	15
3	10	10	2
12	14	7	2

- 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	+	-

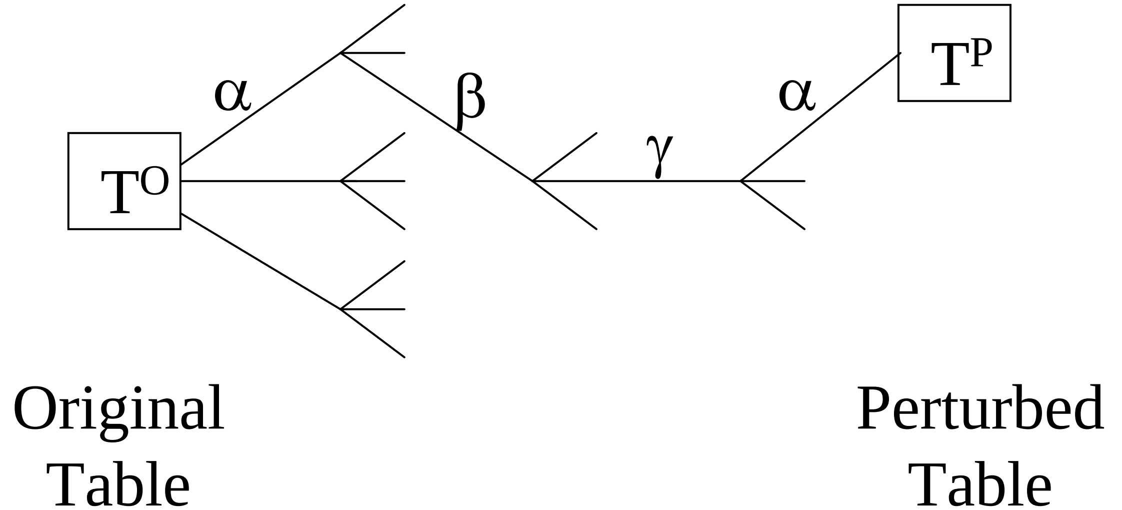
Each cell has exactly two "chances" to move.

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 ± 2.



Cyclic Perturbation: Details

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

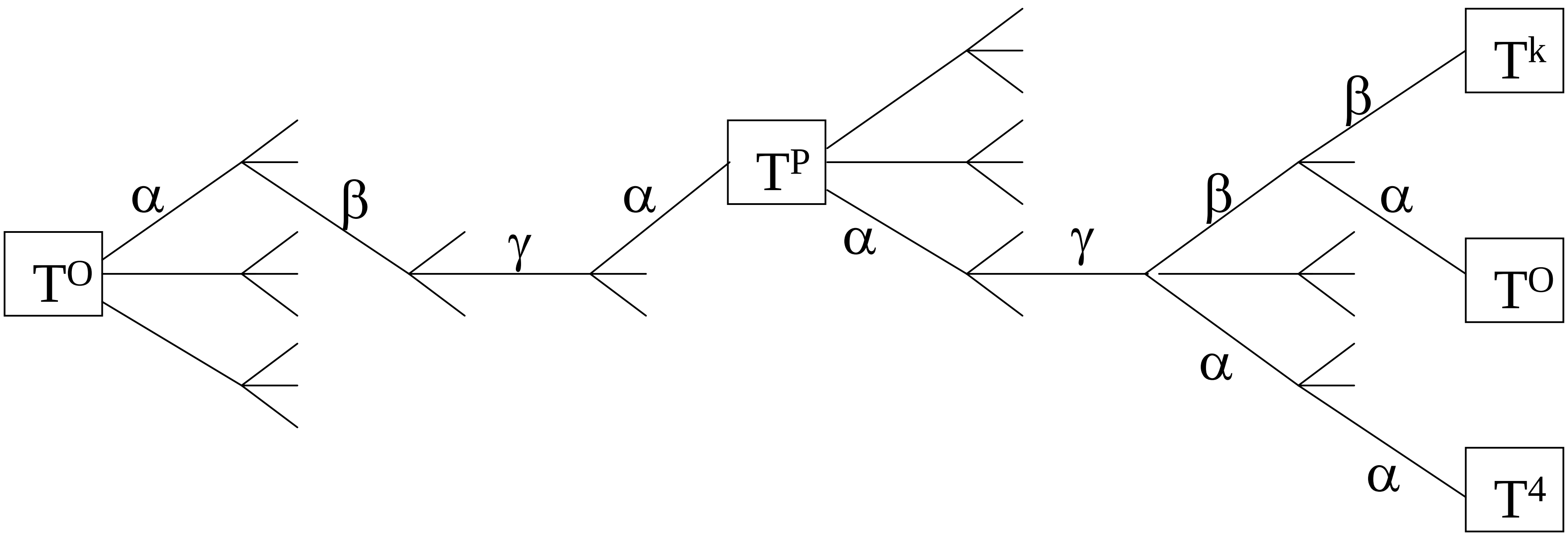
Original

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

[redacted]

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

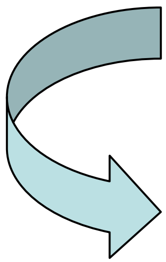
4	80	2	1
4	2	2	1
3	4	4	45
61	3	55	4

k = 3

(Source: Java Random.nextInt())

A Set of Margin-Preserving Perturbations

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

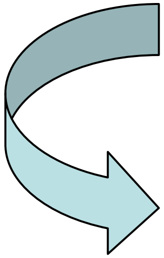


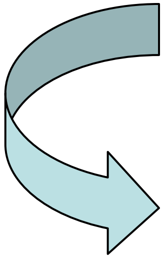
A Set of Margin-Preserving Perturbations

$M_1 =$

+	-	0	·
·	+	-	0
0	·	+	-
-	0	·	+

0	+	-	·
·	0	+	-
-	·	0	+
+	-	·	0





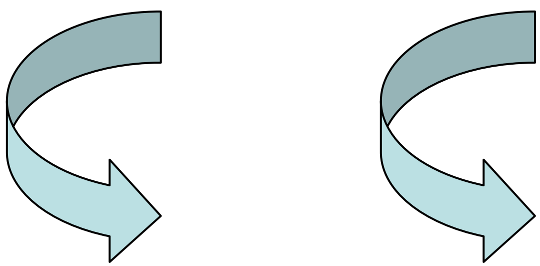
A Set of Margin-Preserving Perturbations

$M_1 =$

+	-	0	·
·	+	-	0
0	·	+	-
-	0	·	+

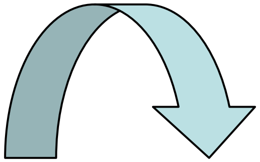
0	+	-	·
·	0	+	-
-	·	0	+
+	-	·	0

-	0	+	·
·	-	0	+
+	·	-	0
0	+	·	-



A Set of Margin-Preserving Perturbations

$$M_1 = \begin{bmatrix} + & - & 0 & \cdot \\ \cdot & + & - & 0 \\ 0 & \cdot & + & - \\ - & 0 & \cdot & + \end{bmatrix} \quad \begin{bmatrix} 0 & + & - & \cdot \\ \cdot & 0 & + & - \\ - & \cdot & 0 & + \\ + & - & \cdot & 0 \end{bmatrix} \quad \begin{bmatrix} - & 0 & + & \cdot \\ \cdot & - & 0 & + \\ + & \cdot & - & 0 \\ 0 & + & \cdot & - \end{bmatrix}$$



A Set of Margin-Preserving Perturbations

$M_1 =$

+	-	0	·
·	+	-	0
0	·	+	-
-	0	·	+

0	+	-	·
·	0	+	-
-	·	0	+
+	-	·	0

-	0	+	·
·	-	0	+
+	·	-	0
0	+	·	-

$M_2 =$

-	0	·	+
+	-	0	·
·	+	-	0
0	·	+	-

+	-	·	0
0	+	-	·
·	0	+	-
-	·	0	+

0	+	·	-
-	0	+	·
·	-	0	+
+	·	-	0

A Set of Margin-Preserving Perturbations

$M_1 =$

+	-	0	·
·	+	-	0
0	·	+	-
-	0	·	+

0	+	-	·
·	0	+	-
-	·	0	+
+	-	·	0

-	0	+	·
·	-	0	+
+	·	-	0
0	+	·	-

$M_2 =$

-	0	·	+
+	-	0	·
·	+	-	0
0	·	+	-

+	-	·	0
0	+	-	·
·	0	+	-
-	·	0	+

0	+	·	-
-	0	+	·
·	-	0	+
+	·	-	0

$M_3 =$

0	·	+	-
-	0	·	+
+	-	0	·
·	+	-	0

-	·	0	+
+	-	·	0
0	+	-	·
·	0	+	-

+	·	-	0
0	+	·	-
-	0	+	·
·	-	0	+

A Set of Margin-Preserving Perturbations

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

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

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

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

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

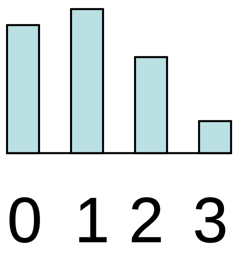
2	3	3	67
227	4	78	4
2	4	6	61
10	4	0	2

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):

Value	0	1	2	3
Probability	0.34	0.39	0.22	0.05



Structural Zeros

- Depending on how they are placed, things can be done.
  - If a complete row, find perturbations for a smaller table, then expand to accommodate the row.
  - Find a Markov or Gröbner basis for the table with fixed values, and use a “knapsack” approach to build perturbations.

Structural Zeros Example

- A table with two structural zeros:
- Compute a Markov basis for the set of moves that leave these cells and the margins unchanged.

0			
	0		

- There are 21 moves in one basis (versus 36 for the unrestricted 4×4 table).
- Solve a knapsack-like problem to find suitable combinations.

	-1	0	1
0		0	0
0	1	0	-1
0	0	0	0

	0	1	-1
0		0	0
0	0	-1	1
0	0	0	0

	0	0	0
0		0	0
1	-1	0	0
-1	1	0	0

	0	0	0
0		1	-1
0	0	-1	1
0	0	0	0

	0	0	0
0		0	0
1	0	-1	0
-1	0	1	0

	0	0	0
0		0	0
0	1	-1	0
0	-1	1	0

	0	0	0
0		0	0
0	0	-1	-1
0	0	1	1

	0	1	-1
0		-1	1
0	0	0	0
0	0	0	0

	0	0	0
-1		0	1
0	0	0	0
1	0	0	-1

	0	0	0
0		0	0
-1	0	0	1
1	0	0	-1

	-1	0	1
0		0	0
0	0	0	0
0	1	0	-1

	0	0	0
0		-1	1
0	0	0	0
0	0	1	-1

	-1	1	0
0		0	0
0	1	-1	0
0	0	0	0

	0	0	0
-1		1	0
1	0	-1	0
0	0	0	0

	0	0	0
0		0	0
0	-1	0	1
0	1	0	-1

	0	0	0
-1		1	0
0	0	0	0
1	0	-1	0

	0	0	0
-1		0	1
1	0	0	-1
0	0	0	0

	-1	1	0
0		0	0
0	0	0	0
0	1	-1	0

	0	-1	1
0		0	0
0	0	0	0
0	0	1	-1

	0	1	-1
0		0	0
0	0	-1	1
0	0	0	0

	0	0	0
0		1	-1
0	1	-1	0
0	-1	0	1

Structural Zeros Example

- These perturbations will work:

	-1	0	1
0		0	0
1	1	-1	-1
-1	0	1	0

1 & 5

	0	0	0
0		1	-1
0	1	-1	0
0	-1	0	1

6 & 12

	-1	1	0
-1		0	1
1	0	0	-1
0	1	-1	0

17 & 18

	0	-1	1
-1		1	0
0	0	0	0
1	0	0	-1

16 & 19

- In higher dimensions, this is currently computationally difficult.
- We can break large tables into smaller sub-tables if necessary.

What's Next

- We need a perturbation generator
  - The table disseminator enters the table size, and locations of any structural zeros.
  - The generator deterministically produces a set of perturbations.
  - The table is perturbed and released.
  - The generator is made available to data users.

Summary

- Cyclic perturbation protects sensitive data by stochastic modifications that are revealed to data users.
- It respects structural and other zeros.
- Disclosure limitation with cyclic perturbation is fast, and scales to large tables and high dimensions.
- For moderate sized tables, cell distributions can be computed.
- For uniform priors, the published value is the most likely value.