

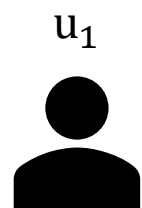
多値時系列データの遷移情報を用いた 局所差分プライバシー手法 Transition RRの提案

山本 悠太¹, 牛田 芽生恵^{1,2}, 菊池 浩明¹

¹明治大学, ²富士通

問題設定

- テレビ、動画配信サイトでの視聴率の推定を目的とする



u_1

u_1	T	1	2	3	4
NHK	1	0	0	0	0
テレビ朝日	0	1	1	1	0
日本テレビ	0	0	0	0	1



u_2

u_2	T	1	2	3	4
NHK	1	1	0	0	0
テレビ朝日	0	0	0	0	0
日本テレビ	0	0	1	0	0



u_3

u_3	T	1	2	3	4
NHK	0	0	0	0	0
テレビ朝日	0	1	0	0	0
日本テレビ	0	0	1	0	0

$n = 3$



調査会社A

T	T=1	2	3	4
NHK	2	1	0	0
テレビ朝日	0	2	1	0
日本テレビ	0	0	2	1
視聴せず	1	0	0	2

問題：自分がどのチャンネルを視聴しているかAに知られたくない
＝個々人のプライバシー保護が必要

局所差分プライバシー(LDP)を用いる



利活用

ベースライン：GRR, 時系列の課題

- 真の値 y を値域 M 内で摂動する

$$\Pr[Y = y \mid x] = \begin{cases} p = \frac{e^\varepsilon}{e^\varepsilon + M - 1}, & y = x \\ q = \frac{1}{e^\varepsilon + M - 1}, & y \neq x \end{cases}$$

- 推定： $\hat{f}_j = \frac{n_j/n - q}{p - q}$
- 全体の予算消費 $T\varepsilon$

- 課題： T に比例してプライバシー予算が増大する



先行研究(時系列LDP)

- 一般LDPを視聴率推定のような**継続収集**にそのまま適用すると精度が劣化する
- 継続収集向けの時系列LDPの先行研究
 - dBitFlipPM[1]：メモ化により、繰り返し収集で予算が累積しない
 - **DDRM**[2]：予算消費の機会を制限し、長い時系列に対応

[1] Ding, B., Kulkarni, J. and Yekhanin, S.: Collecting Telemetry Data Privately, NeurIPS, pp.~3574--3583 (2017).

[2] Xue, Q., Ye, Q., Hu, H., Zhu, Y. and Wang, J.: DDRM: A Continual Frequency Estimation Mechanism With Local Differential Privacy, IEEE Trans. Knowl. Data Eng, Vol.~35, No.~7, pp.~6784--6797 (2023).

DDRM(Dynamic Difference Report Mechanism)[2]

- 予算消費イベントを k 回に制限し、イベント1回あたり予算 α を割り当てる

$$\hat{v} = \tilde{v} \frac{e^{\alpha} + 1}{e^{\alpha} - 1}, \quad \mathbb{E}[\hat{v}] = v$$

- データを補正するために2分木を採用
- 欠点：2値しか扱えない

$T = 4$

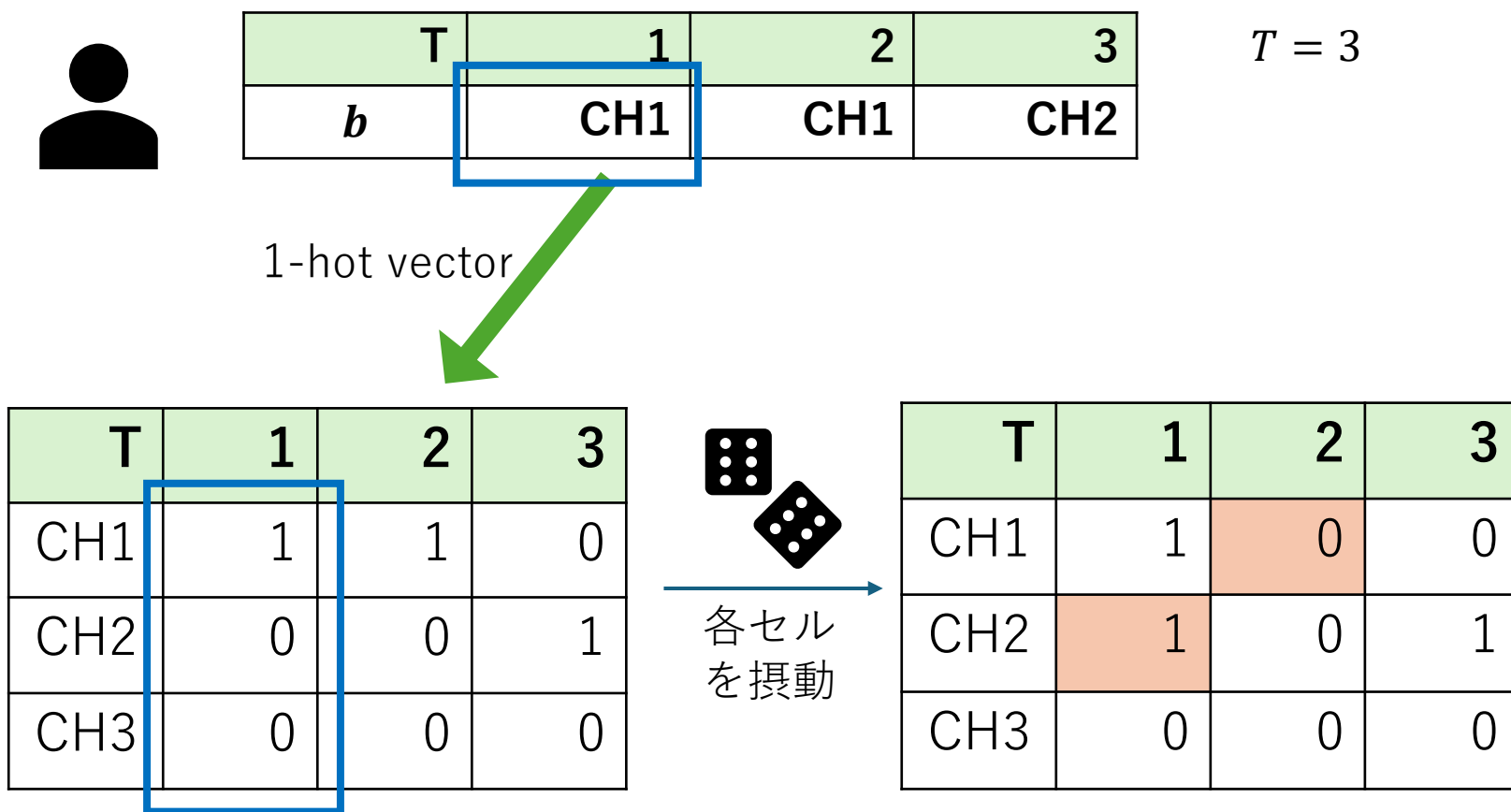
T	1	2	3	4
b	1	1	0	1
Δb	-	0	-1	+1
$\widehat{\Delta b}$	-	+1	-1	-1

変位がない場合
 ± 1 を1/2で出力
(予算を消費しない)

ε ε
変位があれば
予算を消費して摂動

1-hot RR

- 視聴状況 b を1-hot vectorにエンコード
 - 今回DDRMもこの方法で多値に拡張する
- 全体の予算消費が $CT\varepsilon$ (欠点)



提案手法のアイデア

- 多値データを状態遷移 (x^{t-1}, x^t) で報告する。変化がない時刻には、入りに依存しない一様ランダムな遷移を出力する。

- 例



T	1	2	3	4	5	$M = 3$
b	CH1	CH1	CH1	CH2	CH3	
Δb	-	0	0	CH1→CH2	CH2→CH3	

Diagram showing transitions from Δb row to b row:

- From $\Delta b = 0$ (T=2,3) to $b = \text{CH1}$ (T=1,2,3): 予算を消費しない
- From $\Delta b = \text{CH1} \rightarrow \text{CH2}$ (T=4) and $\Delta b = \text{CH2} \rightarrow \text{CH3}$ (T=5) to $b = \text{CH2}$ (T=4) and $b = \text{CH3}$ (T=5): 6-GRRで摂動し、報告

定義域 : $\mathcal{T} = \{(a, b) \mid a, b \in \mathcal{X}, a \neq b\}$ 

$\mathcal{T} = \{\text{CH1} \rightarrow \text{CH2}, \text{CH1} \rightarrow \text{CH3}, \text{CH2} \rightarrow \text{CH1}, \text{CH2} \rightarrow \text{CH3}, \text{CH3} \rightarrow \text{CH1}, \text{CH3} \rightarrow \text{CH2}\}$
要素数 $L = M(M - 1)$ で $L = 6$

提案手法：Transition RR

- 定義： $\alpha = \frac{\varepsilon}{k}$ の下で,

$$\Pr[Y = y \mid c] = \begin{cases} p = \frac{e^\alpha}{e^\alpha + L - 1}, & y = c \\ q = \frac{1}{e^\alpha + L - 1}, & y \neq c \end{cases}$$

$c \notin \mathcal{T}$ のとき, または予算を使い切った後は, $\Pr[Y = y] = 1/L$ で $\mathcal{T}$ から一様に報告

- 推定

$s = p - q = (e^\alpha - 1)/(e^\alpha + L - 1)$ とおくと、収集者は

$$\Delta \hat{f}^t = \frac{1}{n} \sum_i \frac{\varphi(Y_i^t)}{s}, \quad \hat{f}^t = \hat{f}^{t-1} + \Delta \hat{f}^t$$

により頻度ベクトルを更新する.

前状態からの変位を積み上げて推定

手法の比較

	DDRM
報告する情報	bitの差分
値域の大きさ	2
全体のプライバシー予算	ϵ
無変化時の予算消費	なし
短所	<u>2値しか扱えない</u>

GRR	1-hot RR	Transition RR
状態 b	各チャンネルのbit	状態遷移(x^{t-1}, x^t)
M	2	$M(M - 1)$
$T\epsilon$	$CT\epsilon$	ϵ
あり	あり	なし
予算がTに比例して増大	予算がT, Cに比例して増大	値域の拡大 $O(M^2)$ →Cの増大に弱い

Research Question

RQ1. Transition RRは個人のプライバシーを保護できるか？

RQ2. Transition RRはベースラインとなる手法(GRR, 1-hot RR)よりも高い推定精度か？

RQ3. Transition RRの精度が1-hot DDRMを上回る条件は何か？

Transition RRの理論解析

定理2(差分プライバシー)

Transition RR は T 時刻全体で ε -LDP を満たす. (サーバはすべての時間で $\widehat{\Delta b}$ からユーザの真の値を識別できない.)

定理3(Transition RRの誤差上界)

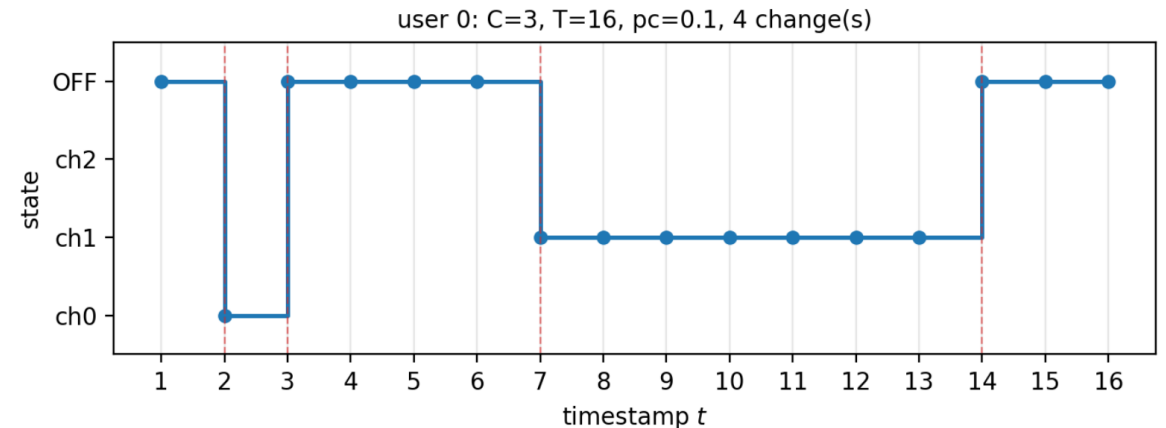
各ユーザの状態変化回数が k 回以下であり、予算枯渇が生じないとき、Transition RR の ℓ_2 誤差は

$$\mathbb{E}[\ell_2^2] \leq \frac{T(T+1)}{n} \left(\frac{1}{s^2} - \rho \right)$$

である. ここで $s = \frac{e^{\varepsilon/k} - 1}{e^{\varepsilon/k} + M(M-1) - 1}$, また ρ は b の変化率である.

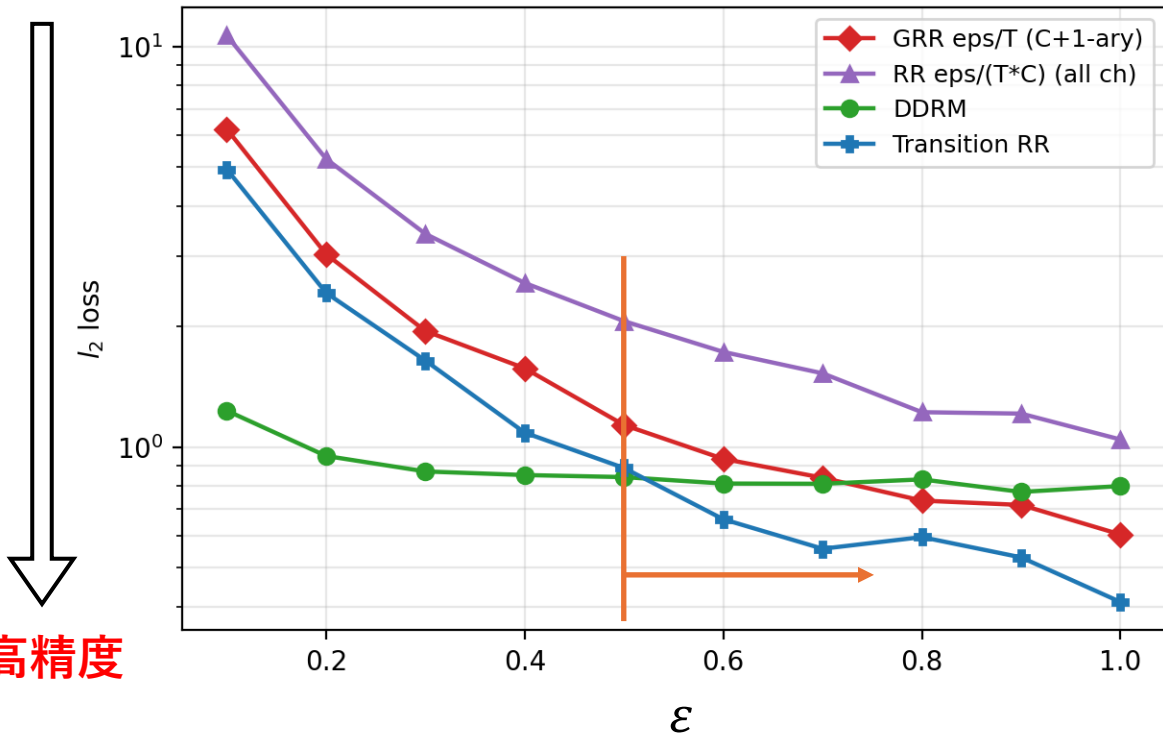
実験

- ユーザを $n = 100,000$ (合成) で用意し, 確率 $\rho = 0.1$ で, $b^t \neq b^{t-1}$ となるように b^t を変位させる.
- LDP方式: **(1)時刻分割GRR, (2)1-hot RR, (3)1-hot DDRM, (4)提案方式Transition RR**を用い,
 1. チャンネル数 $C = 3, T = 16$ に固定し予算 $\varepsilon \in [0.1, 1.0]$ について各頻度を推定する.
 2. $\varepsilon = 1.0$ に固定し, 時間長 $T \in \{2, 4, 8, 16, 32, 64\}$ について各頻度を推定する.
 3. $\varepsilon = 1.0$ に固定し, チャンネル数 $C \in \{1, 2, 4, 8, 16\}$ について各頻度を推定する.またこの実験に関して, 誤差の理論値と実験での誤差の乖離について検証した.



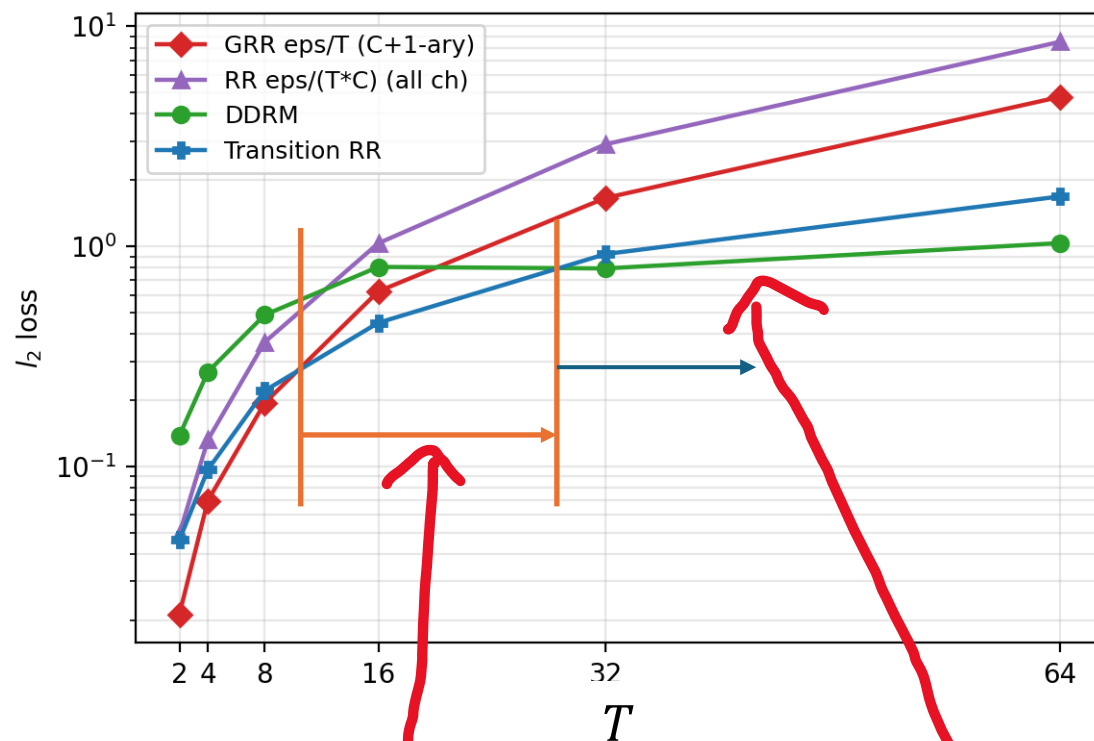
結果1, 2(ε と T についての l_2 誤差)

1
 $n=100000, C=3, T=16, \rho=0.1$



$\varepsilon \geq 0.5$ でTransition RRが最適

2
 $n=100000, \varepsilon=1, C=3, \rho=0.1$



Transition RRが最適

DDRMが最適

結果3(C についての l_2 誤差, 理論値との誤差)

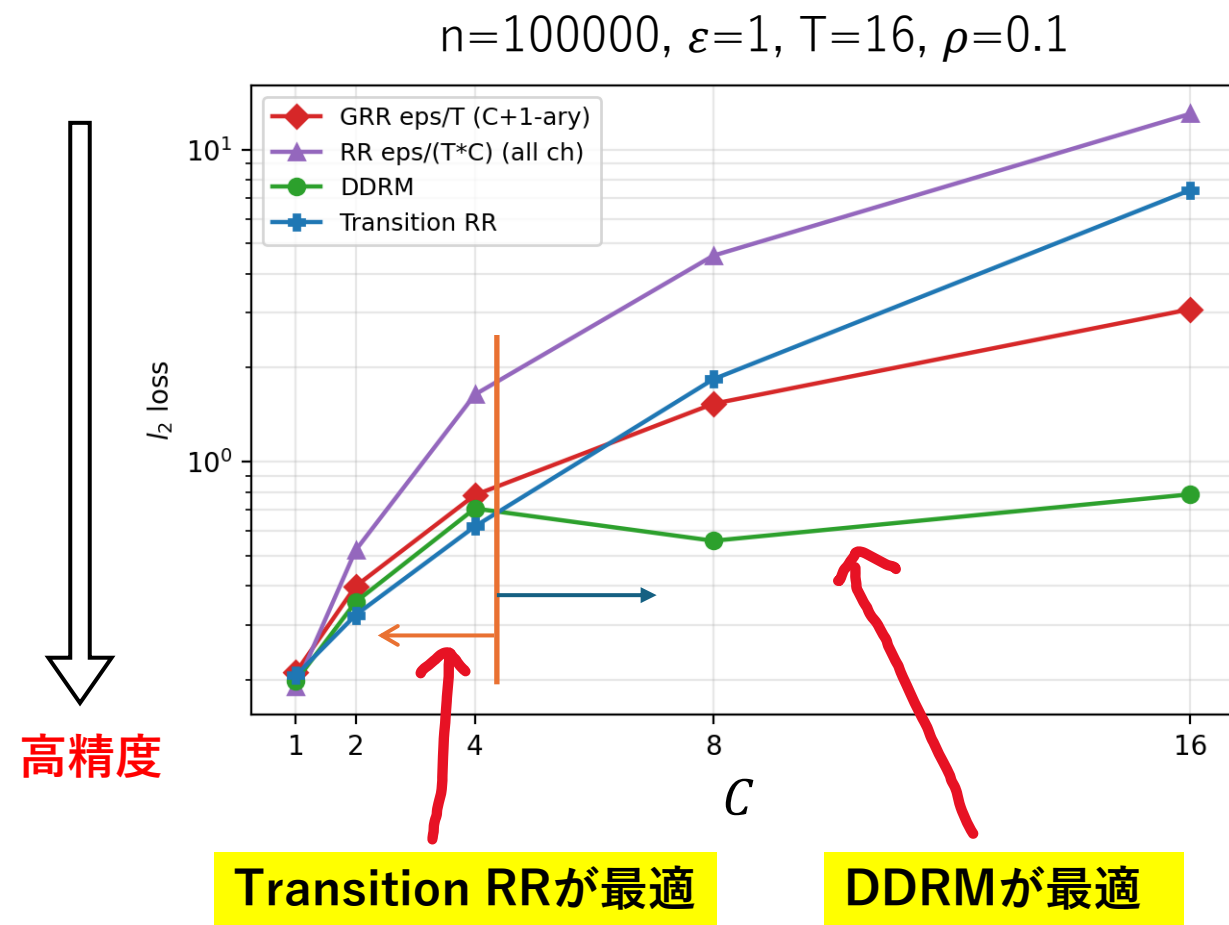
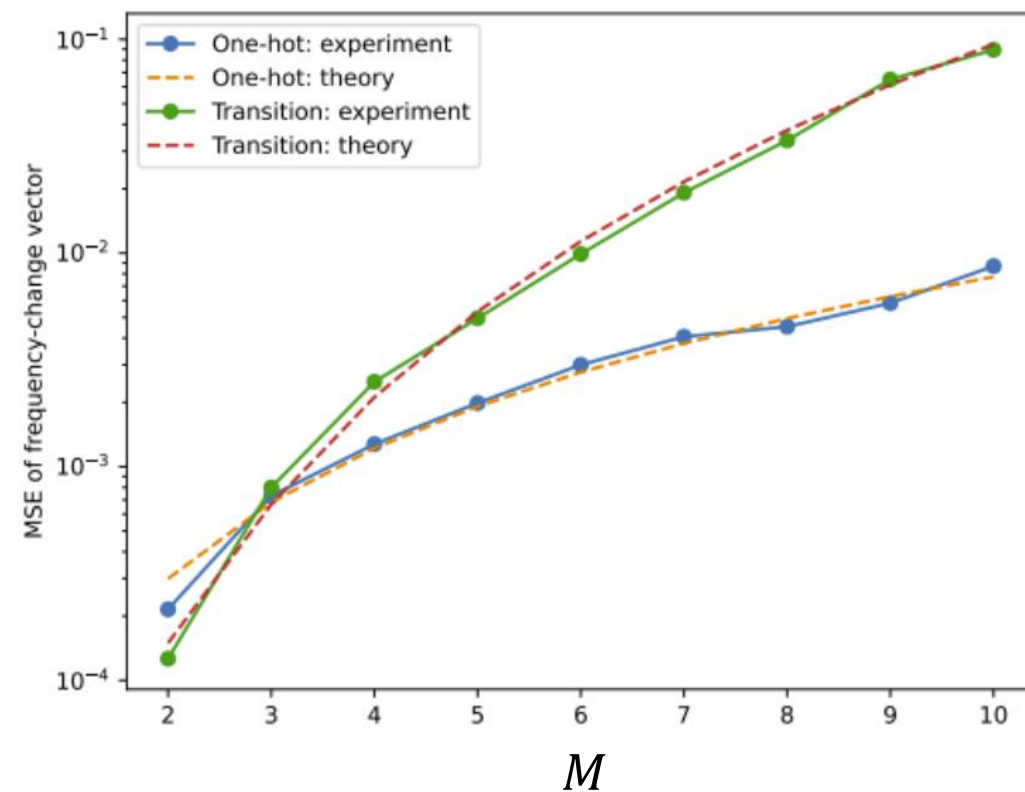


図 6 理論上と実験上の l_2 誤差 ($\varepsilon = 1.0, C \in \{2, 10\}$)

Transition RRの最適条件

Transition RR の誤差上界が 1-hot DDRM の誤差上界を下回る条件は定理1, 定理3から,

$$\sqrt{T+1}(e^{\frac{\varepsilon}{k}} + C^2 + C - 1) < 2C(e^{\frac{\varepsilon}{k}} + 1)$$

これを T について解くと, $T < \left\{ \frac{2C(e^{\frac{\varepsilon}{k}} + 1)}{\varepsilon(e^{\frac{\varepsilon}{k}} + C^2 + C - 1)} \right\}^2 - 1$ で**十分**, これが成立するためには $T < 4C^2 - 1$ が**必要**

- 今回の実験の適用範囲では, **小 C , 小 T で有利**
 - ε の大きさによって上回る C, T の条件は変化する
- この条件は[予算が枯渇しない仮定](#)のもとである

終わりに

RQ1. Transition RRは個人のプライバシーを保護できるか？

→ **保護できる**。定理2により証明されており, これは k に依らない。

RQ2. Transition RRはベースラインとなる手法(GRR, 1-hot RR)よりも高い推定精度か？

→ **特定の条件で高い**。今回の実験では $T < 8, C > 8$ でのGRRとの比較を除き上回る。

RQ3. Transition RRの精度が1-hot DDRMを上回る条件は何か？

• → **総プライバシー予算に応じたチャンネル数, 時刻数の条件に支配される**。今回の実験では小 C , 小 T で上回った。

未達成事項：予算枯渇時の精度評価、実データでの評価