

Self-Correcting Self-Consuming Loops for Generative Model Training

Nate Gillman, Michael Freeman, Daksh Aggarwal,
Chia-Hong Hsu, Calvin Luo, Yonglong Tian, Chen Sun.
10 Jun 2024.

ICML 2024

背景

合成データが急増中

生成モデルが自身の出力データで再訓練される状況が増加

合成データ：生成モデルが生成した人工的なデータ

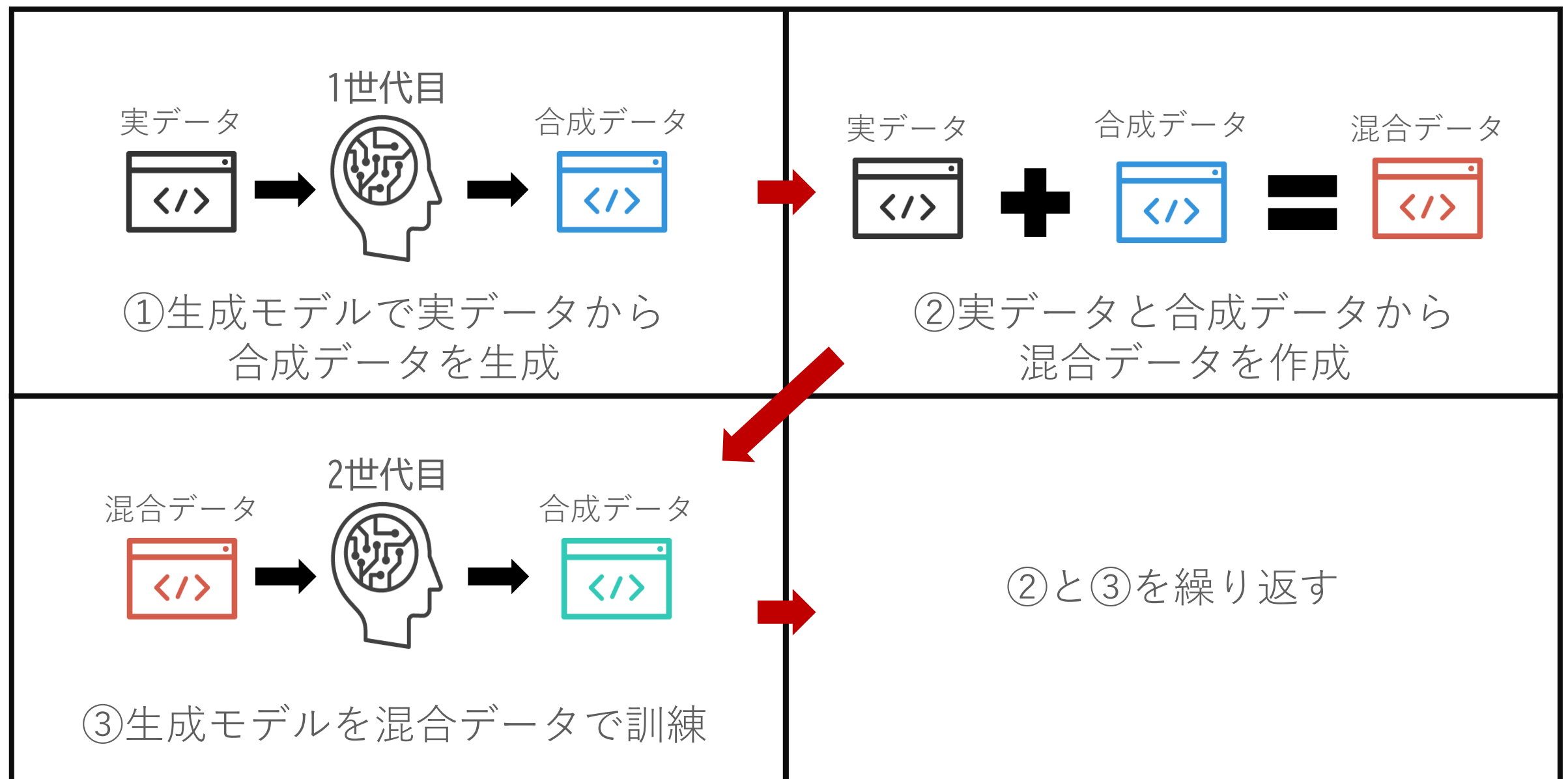
- ・ 知らないうちに合成データを使用している可能性も
- ・ 生成モデルにどの程度影響を与えるのかが未だ解明されていない

使用すること自体は問題ではない

- ・ 画像分類, コントラスト学習では実データに匹敵する成果
- ・ 問題は繰り返し訓練を行うとデータ汚染が起きること
(モデル崩壊)

既存手法：自己消費ループ

実データと合成データを混ぜ合わせて使用する



モデル崩壊

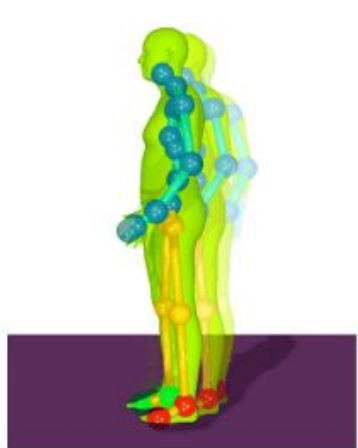
自己消費ループを繰り返すと起こる現象

例) MDMで学習を50世代繰り返した結果

MDM : テキストから人体の動作を生成するモデル

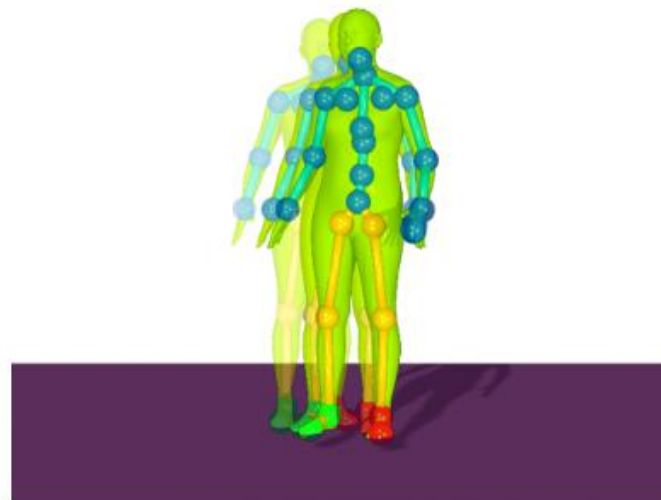
- ・ テキストプロンプトに従わなくなる
- ・ 足が床を貫通するなどの**物理法則を無視した動作**が出現

prompt: *“side-skips from left to right repeatedly”*



Self-Consuming

prompt: *“stand and touch the head”*



Self-Consuming

研究目的

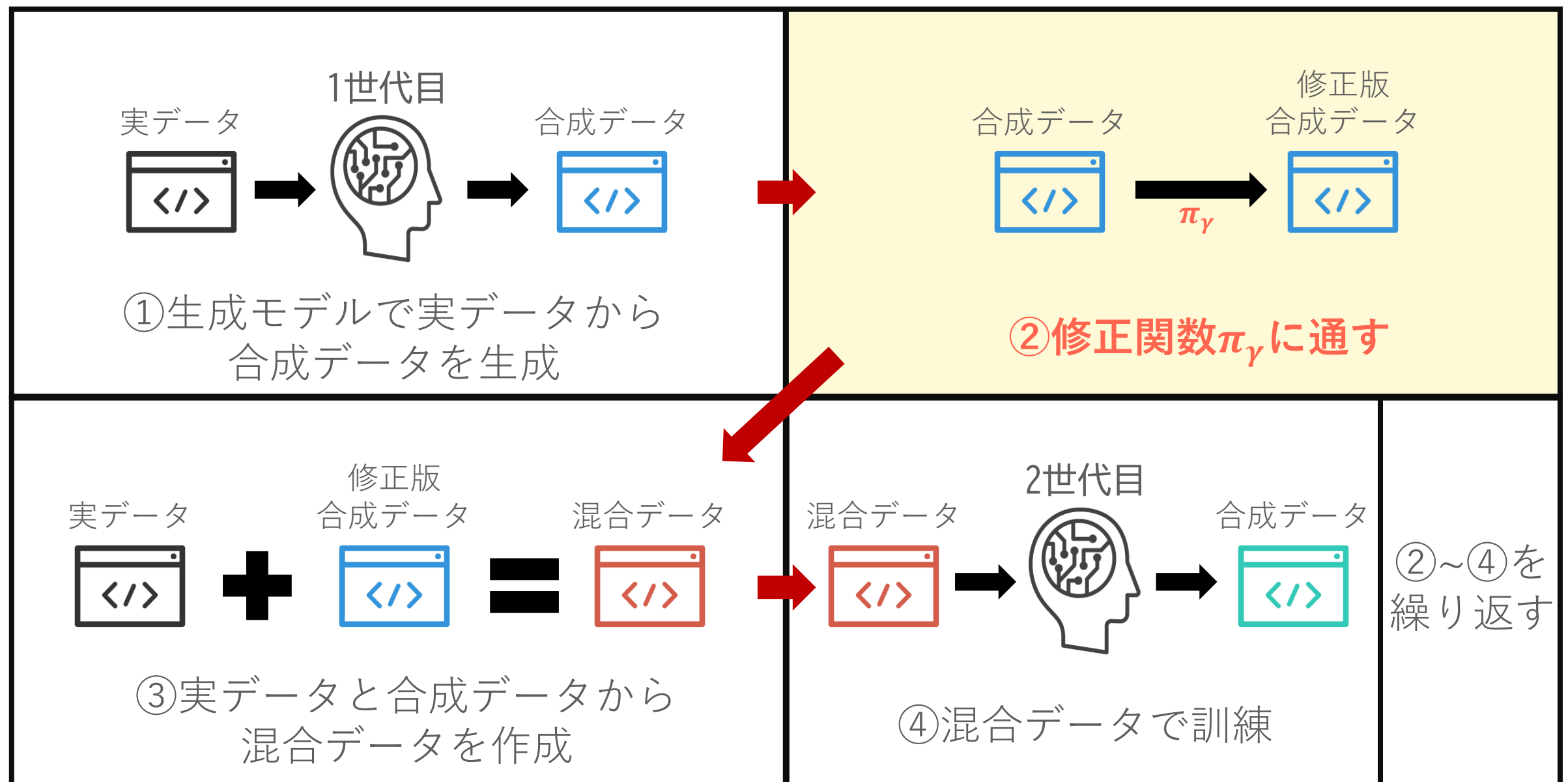
データ量に依存しない崩壊回避の実用手法を提供
先行研究では合成データの「量」という仮定に依存
先行研究での結論：合成データの割合が小さければ小さいほど崩壊しない

▶現実では合成データの量は制御・定量化できない
混合データ内の混合率は設定できない

○合成データを混合する前に修正をかければいいのか

提案手法：自己修正ループ

合成データの「誤り」を修正してから訓練に使用



提案手法：自己修正ループ

修正関数の数学的定義

$$\pi_{\gamma}p_{\theta}(x) = \frac{p_{\theta}(x) + \gamma p_{\theta^*}(x)}{1 + \gamma}, \quad p_{\theta^*}(x) \leq p_{\theta data}(x)$$

$\pi_{\gamma}p_{\theta}(x)$: 修正後の確率分布

$p_{\theta^*}(x)$: 最も理想的な確率分布

$p_{\theta data}(x)$: 真の確率分布

制御を行う 2 つのハイパーパラメータ

修正強度 γ

修正関数が修正をどれだけ強くかけるか

合成拡張割合 λ

実データ n 件に対して、合成データを何割使うか

例) $\lambda = 0.25$ なら実データの 25% の量の合成データを利用

提案手法：自己修正ループ

修正関数の数学的定義

$$\pi_{\gamma}p_{\theta}(x) = \frac{p_{\theta}(x) + \gamma p_{\theta^*}(x)}{1 + \gamma}$$

$$p_{\theta^*}(x) \neq p_{\theta data}(x)$$

$\pi_{\gamma}p_{\theta}(x)$: 修正後の確率分布

$p_{\theta^*}(x)$: 修正関数

$\gamma = 0$: 修正なし

$\gamma = 1$: $p_{\theta}(x)$ と $p_{\theta^*}(x)$ を半々で混合

$\gamma \rightarrow \infty$: $p_{\theta}(x)$ が完全に $p_{\theta^*}(x)$ となる

▶ $p_{\theta^*}(x)$ をどう作るかがカギ

合成拡張割合 λ

実データ n 件に対して、合成データを何倍使うか

例) $\lambda = 0.25$ なら実データの25%の量の合成データを利用

実験内容

使用モデルとデータセット

使用モデル「MDM」

テキストプロンプトから骨格ポーズのシーケンスを作成するモデル

例) 床を這って移動する ► 時系列の骨格動作データを作成

データセット「HumanML3D」

人間の動きの内容が詳細に書いてあるテキストデータ

訓練データ2,794件, テストデータ546件,

小規模設定 : $n \in \{64, 128, 256\}$ でデータ不足シナリオも検証

実験内容

自己修正関数 “UHC + MuJoCo物理シミュレータ”

物理的に無理な動作を妥当性のある動作に変更する

例) 足が床に貫通 ➡ 床面接触を維持した動作に変換

比較する 3 条件

- ベースライン：実データのみで訓練
- 自己消費ループ
- 自己修正ループ

実験内容

自己修正関数 “UHC + MuJoCo物理シミュレータ”

物理的に無理な動作を妥当性のある動作に変更する

例) 足が床に貫

$$\pi_{\gamma} p_{\theta}(x) = \frac{p_{\theta}(x) + \gamma p_{\theta}^*(x)}{1 + \gamma}$$

比較する3条件

- ベースラインのみで訓練

$p_{\theta}(x)$: MDMが作成した合成データ (修正前)

$p_{\theta}^*(x)$: UHC + MuJoCoが作成する理想データ

γ : UHC + MuJoCoの模倣精度

$\pi_{\gamma} p_{\theta}(x)$: 次世代に送る修正後データ

実験結果

評価指標

FID：生成動作の分布と真の分布の類似度（低いほど◎）

多様性：生成動作のバリエーションの豊富さ（高いほど◎）

マッチングスコア：テキストプロンプトへの追従度（高いほど◎）

結果

小データ（n=64，拡張100%）

- ・修正なしは崩壊，修正ありは安定

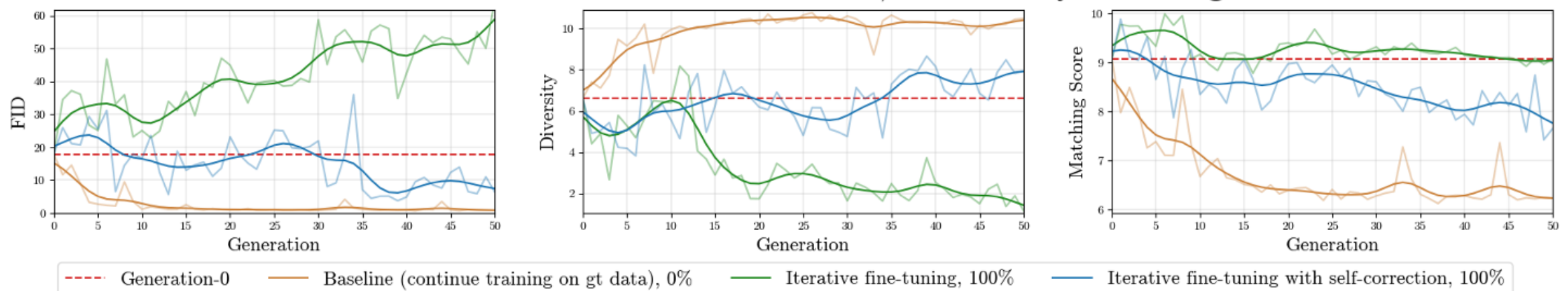
大データ（n=2794，拡張25%）

- ・修正ありは安定し，最終的にベースラインに収束

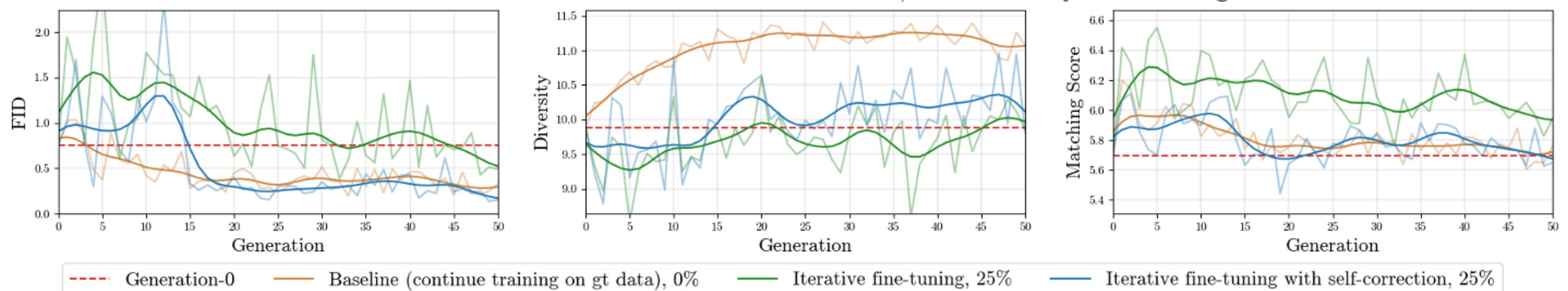
実験結果

ベースラインよりは崩壊するものの、緩やかに
左グラフ：低いほど良い 中央・右グラフ：高いほど良い

Human Motion Generation Results: Dataset Size 64, with 100% Synthetic Augmentation



Human Motion Generation Results: Dataset Size 2794, with 25% Synthetic Augmentation



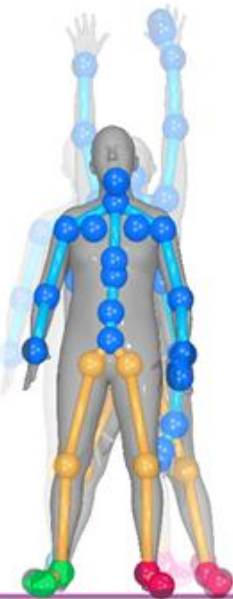
実験結果

修正を行うと，物理的に妥当な操作を行えるように

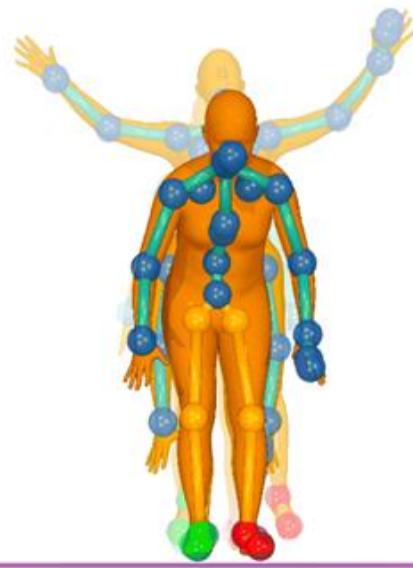
内容：足を広げて立ち、両手を頭上に伸ばし、腰のあたりまで振り下ろして腕を垂らしてから立ち上がる

Self-Correcting Self-Consuming Loops for Generative Model Training

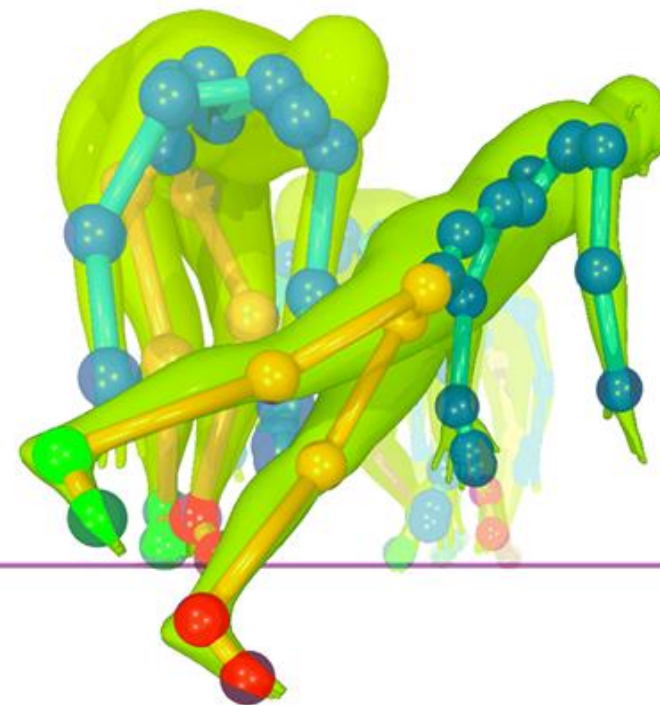
Ground Truth



Baseline



Iterative Fine-tuning



Iterative Fine-tuning
with Self-Correction



まとめ

自己修正関数を施すことでモデル崩壊を防げる

- ・ 専門的なシミュレータを用いることで、大規模自動運用も可能
- ・ 合成データ比率が100%でも崩壊を回避

今後の課題

他分野のタスクでの検証

例) 言語モデリング, テキストから画像生成など

所感

| γ を作るのがむずかしい

γ が現実の物理シミュレータにどの程度対応するかが不明

| 修正関数自体がボトルネックになるのでは

作ることができるのはわかったが、コスト、精度が不明

| 真の分布に近づいているのではない

今回は真の分布に近い理想分布を作れただけ

| 使用するシミュレータにかかっている

UHC自体がモデル崩壊を起こすとかについて議論されていない

補足資料

以下本実験の前の段階の検証実験の内容

- 修正関数が機能しているのか実験
- 今回は「MDMに機能するか」が本実験
- 真の分布の有無で結果が変わるのかも見ている

検証実験

検証の設定① ガウス分布（真の分布**有**）

- 合成拡張割合 $\lambda = 0.5$
- 修正関数 γ を0から5.0まで変化させ、**500世代**繰り返す
- 推定分布と真の分布でWasserstein距離を計測（近いほど良い）

検証の設定② MNIST（真の分布**無**）

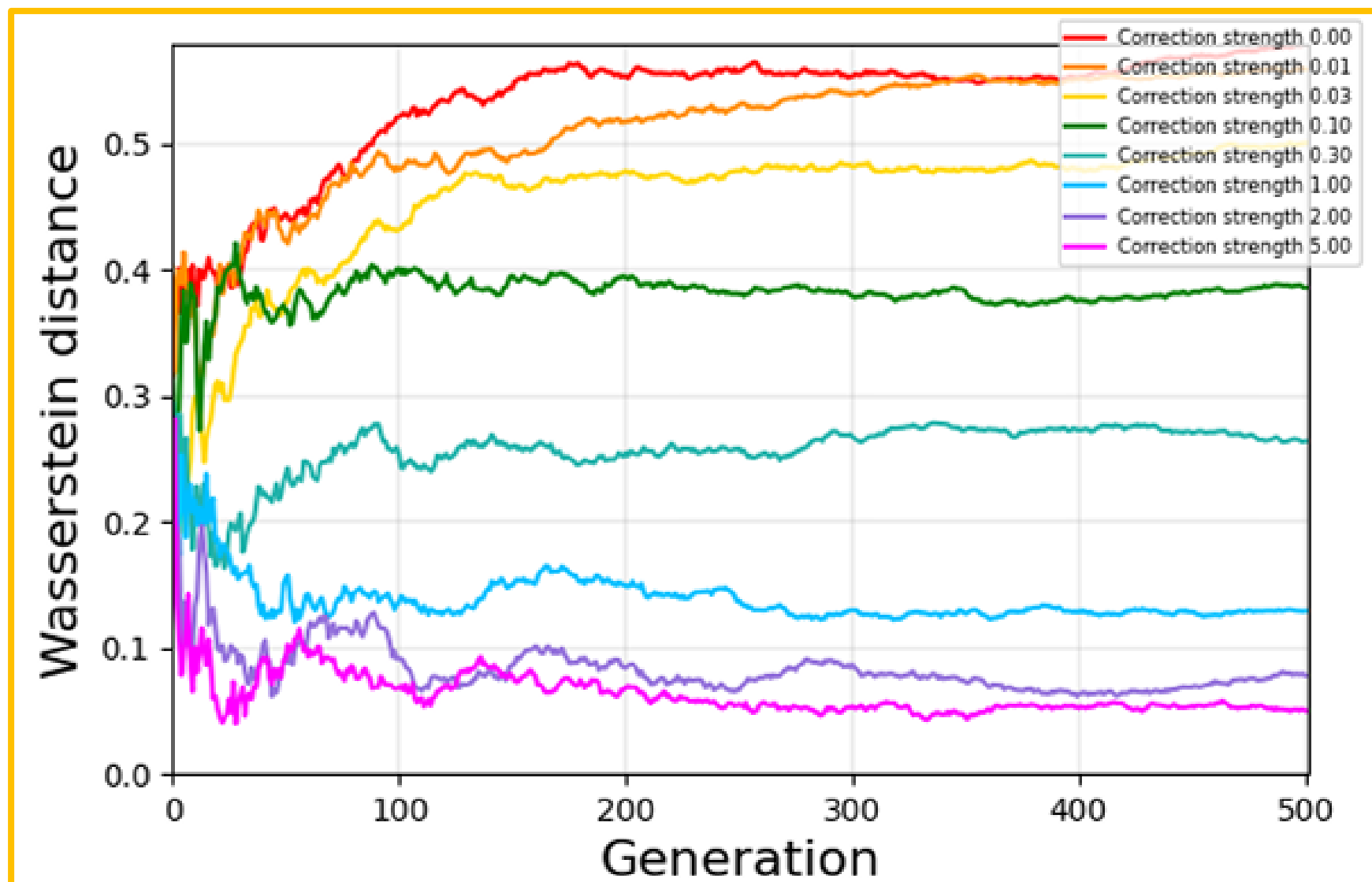
- 合成拡張割合 $\lambda = 0.2$
- 修正関数 γ を0から1.5まで変化させ、**50世代**繰り返す
- 各数字でK-meansクラスタリングを実施し目標分布を用意、分類（K=16）

検証結果①ガウス分布

小さな数値変更だけでも，距離が縮まる

$\gamma = 0$ のとき，世代を重ねるごとに不安定になる

$\gamma = 0.01$ にするだけでも，明確な改善が見られる



検証結果②MNIST

真の分布を知らなくても近似的な修正で分類可能

- 修正なしだと世代ごとに低品質な文字に
- 修正を行うと，合成データでも高品質で，正答できる画像に.

0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9

Iterative Fine-tuning

0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9

Iterative Fine-tuning with Self-Correction