Celebrate Paul Dupuis and his contributions

Markos Katsoulakis Mathematics & Statistics

UMassAmherst

ICERM 2024 — Robust Optimization and Simulation of Complex Stochastic Systems September 2024

A Mean-field games laboratory for generative modeling: implications for robust generative algorithms





Generative modeling



Stable diffusion



ChatGPT



Hoogeboom et al. 2022





CIFAR10





ANHIR²

- 1. Ciompi et al., Zenodo 2019
- 2. Borovec et al., IEEE Transactions on Medical Imaging 2020



What is Generative Modeling?

Given a dataset, e.g., images of bedrooms (LSUN dataset), create more data More pressing math challenges in GMs





Generative modeling

 $\mathcal{D} = \{x_1, x_2, \dots, x_n\} \longrightarrow p_{\theta^*}(x) \approx \pi(x) \longrightarrow \widetilde{\mathcal{D}} = \{\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_n\}$















•••



Generative modeling approaches

distribution π , reproduce <u>new</u> samples from π

- Pick a source distribution ρ , easy to simulate (e.g. Gaussian).
- Generative map (one-shot): Learn a transport map Φ such that:
- Generative flow: Learn a transport flow via a vector field v(x, t) such that

 $dx(t) = v(x(t), t) dt + \sigma dW(t) \quad \text{s.t. } x(0) \sim \rho \qquad x(T) \sim \pi$

<u>Normalizing flows</u> ($\sigma = 0$) learn an ODE **<u>Diffusion models</u>** ($\sigma > 0$) learn a SDE

Main Goal: Given data $X_i \sim \pi, i = 1, \dots, N$ from an (unknown) **target**

 $\Phi_{\#}\rho \approx \pi$ (e.g. GANs, distillation methods) <u>Or</u>

Flow-based generative modeling • Given dataset $\{X_i\} \sim \pi$ data distribution viewed as particles Flow-based generative modeling: based on ODE or SDE for

- transport of probability measures



Score-based generative models^{*x*}

Wasserstein **Gradient flows**

JKO '98 Santambrogio '15

Continuous normalizing flows

Grathwohl et al. '18



Song et al. '20 Ho et al. '20

Continuous-time normalizing flows Reference: $\rho_{ref}(x) = \mathcal{N}(0,\mathbf{I})$ Target: $\pi(x)$



Grathwohl et al. '18

$$\frac{dx}{dt} = v_{\theta}(x(t))$$

(0) ~ $\pi(x), x(T) \sim \rho_{ref}(x)$

$$KL(\pi \| f_{\theta \sharp} \rho_0)$$
 The 'usual' divergence

$$\operatorname{ref}(x(0)) + \int_{T}^{0} \nabla \cdot v_{\theta}(x(s), s) \, ds \left[x(s) = x + \int_{T}^{s} v_{\theta}(x(s'), s') \, ds', x \right]$$



Highlights in this talk

- 1. Mean-field games as a mathematical framework for generative flows:
- optimal control of particle dynamics + cost functions/distances to target π
- <u>backward</u> Hamilton-Jacobi + <u>forward</u> Transport PDE

- 2. Model-form UQ + PDE regularity theory for generative flows:
- Score-based, diffusion generative models are robust
- 3. Structure-informed learning:
- Equivariance provably enhances generative algorithms

See the posters by Hyemin Gu and Ben Zhang

See poster by Ziyu Chen



L. Rey-Bellet



Ziyu Chen, UMass Amherst



N. Mimikos-Stamatopoulos, Université Côte d'Azur



Hyemin Gu, UMass Amherst



Benjamin Zhang, UMass Amherst → Brown



P. Dupuis



S. Osher, UCLA



W. Li, U of SC



S. Liu, UC Riverside



W. Zhu, GaTech



Jeremiah Birrell, Texas State



Y. Pantazis, FORTH, Greece



P. Birmpa, Heriot-Watt, UK





A Mean-field games laboratory for generative modeling:

Neural ODE flows & diffusion-based generative algorithms as MFG



Benjamin Zhang, Brown



Mean-field games



Hamilton-Jacobi-Bellman

http://www.science4all.org/article/mean-field-games/





Fokker-Planck-Kolmogorov



Transport

PDE

Motivation Mean-field games as a unifying mathematical framework

- Explaining Understanding generative models in relation to each other
- Enhancing MFGs inform exploitable mathematical structure
- Inventing A laboratory for experimenting with new models
- Normalizing flows as solutions of MFGs
- Score-based generative models as solutions of MFGs

Mean-field games

$$dx(t) = v(x(t), t) ds + \sigma(x(t), t) dW(t)$$
$$x(0) = x_0$$





Potential Mean-field games and optimality conditions



Hamiltonian

$$H(x, p) = \sup_{v} - p^{\top}v - L(x, v)$$
Optimal velocity field

$$v^*(x, t) = -\nabla_p H(x, \nabla U)$$

$$\partial_t \rho - \nabla \cdot \\ -\partial_t U + H(x) = U(x, T) = U(x, T)$$



Why mean-field games for generative modeling? Training flow-based models looks like solving MFGs



Generative model

Reference distribution

Target distribution

s.t. $dx(t) = v(x(t), t) dt + \sigma dW(t)$ $x(0) \sim \rho_0$ π





Generative models as solutions to MFGs



Generative models as solutions to MFGs





Optimality conditions & well-posedness

Hamiltonian

$$H(x,p) = \sup_{v} - p^{\mathsf{T}}v - L(x,v)$$

Forward in time: Fokker-Planck

$$\partial_t \rho - \nabla \cdot (\nabla_p H(x, \nabla U) \rho)$$

 $\rho(x, 0) = \rho_0(x)$
Generator





Exhibit A: Continuous normalizing flows Reference: $\rho_{ref}(x) = \mathcal{N}(0,\mathbf{I})$ Target: $\pi(x)$



Grathwohl et al. '18

Sensitive to parametrization!

$$\frac{dx}{dt} = v_{\theta}(x(t))$$

(0) ~ $\pi(x), x(T) \sim \rho_{ref}(x)$

$$Y_{KL}(\pi \| f_{\theta \ddagger} \rho_0)$$
 The 'usual' divergence

$$v_{ef}(x(0)) + \int_T^0 \nabla \cdot v_\theta(x(s), s) \, ds \left[x(s) = x + \int_T^s v_\theta(x(s'), s') \, ds', x \right]$$

CNFs trained with KL divergence are ill-posed: discretization-dependent





Continuous normalizing flows are ill-posed Well-noted that CNFs are ill-posed. Study CNFs as MFG

$$\inf_{v,\rho} \left\{ \mathcal{M}(\rho(\cdot,T)) + \int_{0}^{T} \mathcal{F}(\rho(\cdot,t)) dt + \int_{0}^{T} \int_{\mathbb{R}^{d}} L(x,v)\rho(x,t) dx dt \right\}$$

s.t. $\partial_{t}\rho + \nabla \cdot (v\rho) = \frac{\sigma^{2}}{2} \Delta \rho, \qquad \rho(x,0) = \pi(x)$

Reference distribution $\inf_{v \in \mathcal{O}} \left\{ \mathscr{D}_{KL}(\rho(\cdot, T) \| \rho_{ref}) \right\}$

s.t. $\partial_t \rho + \nabla \cdot (v\rho) = 0$, $\rho(x,0) = \pi(x)$

Hamiltonian is degenerate! $H(x,p) = \sup - p^{\mathsf{T}}v - L(x,v)$ $= \sup - p^{\mathsf{T}} v$ $= \infty$ if $p \neq 0$ H(x, p) = 0 if p = 0



Continuous normalizing flow as an MFG Additional constraints yield well-posedness & math structure!

Option 1: Bound the set of feasible velocities

$$\inf_{v,\rho} \left\{ \mathscr{D}_{KL}(\rho(\cdot, T) \| \rho_{ref}) : \|v\| \le c \right\}$$

s.t. $\partial_t \rho + \nabla \cdot (v\rho) = 0, \qquad \rho(x,0) = \pi(x)$

$$\partial_t \rho - c \nabla \cdot \left(\rho \frac{\nabla U}{\|\nabla U\|} \right) = 0$$

$$-\partial_t U + c \|\nabla U\| = 0$$

$$U(x, T) = 1 + \log \frac{\rho(x, T)}{\rho_{ref}(x)}, \quad \rho(x, 0) = 0$$

Fokker-Planck

JB: A **level set** equation!

$= \pi(x)$

Hamiltonian

$$H(x,p) = \sup_{\|v\| < c} - p^{\top}$$
$$= c \|p\|$$

Optimal velocity field $\nabla U(x,t)$

$$v^*(x,t) = -c \frac{1}{\|\nabla U(x,t)\|}$$



Continuous normalizing flow as an MFG Additional regularizations yield well-posedness and structure

Option 2: Optimal transport cost [Onken et al. '21]

$$\inf_{\nu,\rho} \left\{ \mathscr{D}_{KL}(\rho(\cdot,T) \| \rho_{ref}) + \int_0^T \int_{\mathbb{R}^d} \frac{1}{2} \| \nu(x,t) \|^2 \rho(x,t) \, dx \, dt \right\}$$

s.t. $\partial_t \rho + \nabla \cdot (\nu \rho) = 0, \qquad \rho(x,0) = \pi(x)$

$$\partial_t \rho - \nabla \cdot \left(\rho \nabla U \right) = 0$$

$$-\partial_t U + \frac{1}{2} \|\nabla U\|^2 = 0$$
$$U(x,T) = 1 + \log \frac{\rho(x,T)}{\rho_{ref}(x)},$$

Fokker-Planck

HJB

$$\rho(x,0) = \pi(x)$$

Hamiltonian $H(x,p) = \sup_{v} - p^{\mathsf{T}}v - \frac{1}{2} ||v||^{2}$ $= \frac{1}{2} ||p||^{2}$ Optimal velocity field

 $v^*(x,t) = -\nabla U(x,t)$



Mathematical structure of CNFs

- Mean-field games provide wellposedness and structure to normalizing flows
- Well-posedness of NF training tied to well-posedness of Hamilton-Jacobi
- Empirically observed and explained via an Optimal Transport argument, **Finlay et al, 2021:**





U(x,T)

Optimal velocity field



Optimal transport regularization

Hamilton-Jacobi equation $-\partial_t U + \frac{1}{2} \|\nabla U\|^2 = 0$

$$= 1 + \log \frac{\rho(x, T)}{\rho_{ref}(x)}$$

$$,t) = -\nabla U(x,t)$$

See <u>talk</u> by L. Rey-Bellet, poster by Hyemin Gu on a complete analysis & experiments using **Wasserstein Proximals and MFG**



Score-based generative modeling with SDEs **Two SDEs**



Song et al. '20

Score-matching

$$\min_{\theta} C_{ESM}(\theta) = \min_{\theta} \int_0^T \int_{\mathbb{R}^d} \frac{\sigma(T-s)^2}{2} \|\mathbf{s}_{\theta}(y,s) - \nabla \log \eta(y,s)\|^2 \eta(y,s) \, dy \, ds$$
$$\min_{\theta} C_{ISM}(\theta) = \min_{\theta} \int_0^T \int_{\mathbb{R}^d} \sigma(T-s)^2 \left[\frac{1}{2} \|\mathbf{s}_{\theta}(y,s)\|^2 + \nabla \cdot \mathbf{s}_{\theta}(y,s)\right] \eta(y,s) \, dy \, ds$$

Noising process

 $dY(s) = -f(Y(s), T-s)ds + \sigma(T-s)dW(s)$ $Y(0) \sim \pi$ $Y(s) \sim \eta(\cdot, s)$

Denoising process $dX(t) = \left[f(X(t), t) + \sigma(t)^2 \nabla \log \eta(x, t) \right] dt + \sigma(t) dW(t)$ $X(0) \sim \eta(\cdot, T)$ Forward SDE (data \rightarrow noise) $\mathbf{x}(0)$ $\mathrm{d}\mathbf{x} = \mathbf{f}(\mathbf{x},t)\mathrm{d}t + g(t)\mathrm{d}\mathbf{w}$





Exhibit B: SGM as an MFG

$$\inf_{v,\rho} \left\{ \mathcal{M}(\rho(\cdot,T)) + \int_{0}^{T} \mathcal{F}(\rho(\cdot,t)) dt + \int_$$

Cross Entropy

$$\inf_{v,\rho} \left\{ -\int \rho(x,T) \log \pi(x) dx + \int_0^T \int_{\mathbb{R}^d} \left(\frac{1}{2} \| v \right) \right\}$$
s.t. $\partial_t \rho + \nabla \cdot \left((f + \sigma v) \rho \right) = \frac{\sigma^2}{2} \Delta \rho, \quad \rho$

Running cost $\left\{\int_{0}^{T}\int_{\mathbb{R}^{d}}L(x,v)\rho(x,t)\,dx\,dt\right\}$ $= \rho_0(x)$ $v\|^2 - \nabla \cdot f
ight)
ho(x, t) dx dt$

 $p(x,0) = \eta(x,T)$

Cross Entropy $CE(\pi, \rho) = -\mathbb{E}_{\rho}[\log \pi]$ $= -\mathbb{E}_{\rho}[\log\rho] + \mathbb{E}_{\rho}\left[\log\frac{\pi}{\rho}\right]$ = Entropy + KL Divergence

Wasserstein **Proximal** of Cross Entropy when f=0





SGM as an MFG: optimality conditions

$$\partial_t \rho + \nabla \cdot \left(\rho(f - \sigma^2 \nabla U)\right) = \frac{\sigma^2}{2} \Delta \rho$$
$$-\partial_t U - f^\top \nabla U + \frac{1}{2} \|\sigma \nabla U\|^2 + \nabla \cdot f$$

$$U(x, T) = -\log \pi(x), \quad \rho(x, 0) = \eta(x)$$

$$\partial_t \rho + \nabla \cdot (\rho(f + \sigma^2 \nabla \log \eta)) = \frac{\sigma^2}{2}$$
$$\partial_s \eta + \nabla \cdot (-f\eta) = \frac{\sigma^2}{2} \Delta \eta$$
$$\eta(y, 0) = \pi(y), \quad \rho(x, 0) = \eta(x, T)$$





Controlled Fokker-Planck

Uncontrolled **Fokker-Planck**

See also optimal control perspective [Berner et al. 2022]



SGM as an MFG: Noising SDE is a HJB

$$\partial_t \rho + \nabla \cdot ((f + \sigma^2 \nabla \log \eta)\rho) =$$

$$\partial_s \eta + \nabla \cdot (-f\eta) = \frac{\sigma^2}{2} \Delta \eta$$

$$\eta(y,0) = \pi(y), \quad \rho(x,0) = \eta(x, \eta)$$





Continuous normalizing flows <u>vs</u> score-based generative models

<u>Less</u> than meets the eye



	$\mathscr{M}(\rho)$	$\mathcal{I}(\rho)$	L(x, v)	Dynamics
OT-Flow (Alternate formulation)	$\mathcal{D}_{KL}(\pi \ ho)$	0	$\frac{1}{2}\ v\ ^2$	dx = v dt
SGM via SDEs	$-\mathbb{E}_{\rho}\left[\log\pi\right]$	0	$\frac{1}{2} \ v\ ^2 - \nabla \cdot f$	$dx = (f + \sigma v) dt + \sigma dW$

From cost

$$F(\cdot, t))dt + \int_{0}^{T} \int_{\mathbb{R}^{d}} L(x, v)\rho(x, t) dx dt$$

$$\rho(x, 0) = \rho_{0}(x)$$



SGM vs. Normalizing Flows: an optimality conditions comparison

Score-based Generative Model

$$\inf_{v,\rho} \left\{ -\int \rho(x,T) \log \pi(x) dx + \int_0^T \int_{\mathbb{R}^d} \left(\frac{1}{2} \|v\|^2 - \nabla \cdot f \right) \rho(x,t) dx dt \right\}$$

s.t. $\partial_t \rho + \nabla \cdot \left((f + \sigma v) \rho \right) = \frac{\sigma^2}{2} \Delta \rho, \qquad \rho(x,0) = \eta(x,T)$

$$\partial_t \rho + \nabla \cdot ((f - \sigma^2 \nabla U)\rho) = \frac{\sigma^2}{2} \Delta \rho$$
$$-\partial_t U - f^{\mathsf{T}} \nabla U + \frac{1}{2} \|\sigma \nabla U\|^2 + \nabla \cdot f = \frac{\sigma^2}{2} \Delta U$$
$$U(x, T) = -\log \pi(x), \quad \rho(x, 0) = e^{-U(x, 0)}$$
In SGM: HJB decouples from FP due to terminal condition
and can be solved first, to provide the optimal velocity
field for the FP (see reverse SDE)

OT Normalizing flow (alternate form)

$$\inf_{v,\rho} \left\{ \mathscr{D}_{KL}(\pi \| \rho(\cdot, T)) + \int_0^T \int_{\mathbb{R}^d} \frac{1}{2} \| v(x,t) \|^2 \rho(x,t) d \right\}$$

s.t. $\partial_t \rho + \nabla \cdot (v\rho) = 0, \qquad \rho(x,0) = \rho$

Hamilton-Jacobi-Bellman

initial/terminal conditions

$$\partial_t \rho - \nabla \cdot \left(\rho \nabla U\right) = 0$$
$$-\partial_t U + \frac{1}{2} \|\nabla U\|^2 = 0$$
$$(x, T) = -\frac{\pi(x)}{\rho(x, T)}, \quad \rho(x, 0) = \rho_0(x)$$









MFG-informed generative models

MFG formulation describes math structure We learn in a restricted, more relevant space

Provably yields:

- Better generative models
- Better training objectives
- Better regularizers

See posters by Hyemin Gu, Ben Zhang



A modular mean-field games laboratory

		Mean-field				
Model	$\mathcal{M}(ho)$	$\mathcal{I}(ho)$	L(x,v)	Dynamics	H(x,p)	$\mathbf{Optimal} \ v^*$
Continuous normalizing flow	$\mathcal{D}_{KL}(\pi \ ho)$	0	0	$\mathrm{d}x = v\mathrm{d}t$	$\sup_{v \in K} -p^\top v$	$- abla_p H(x, abla U)$
Score-based generative modeling	$-\mathbb{E}_{ ho}\left[\log\pi ight]$	0	$\frac{ v ^2}{2} - \nabla \cdot f$	$dx = (f + \sigma v) dt + \sigma dW_t$	$\begin{vmatrix} -f \cdot p + \frac{\sigma^2}{2} p ^2 \\ +\nabla \cdot f \end{vmatrix}$	$\sigma \nabla \log \eta_{T-t}$
Score-based probability flow	$-\frac{1}{2}\mathbb{E}_{\pi}\left[\log\pi\right]$	$\mathbb{E}_{\rho}\left[\frac{ \sigma\nabla\log\rho ^2}{8}\right]$	$\frac{ v ^2}{2} - \frac{\nabla \cdot f}{2}$	$dx = (f + \sigma v) dt$	$\begin{vmatrix} -f \cdot p + \frac{\sigma^2}{2} p ^2 \\ +\nabla \cdot f \end{vmatrix}$	$\frac{\sigma}{2}\nabla\log\eta_{T-t}$
Wasserstein gradient flow (WGF) ($\epsilon \rightarrow 0$)	$\mathcal{F}(ho)e^{-T/\epsilon}$	$rac{e^{-t/\epsilon}}{\epsilon}\mathcal{F}(ho)$	$\frac{e^{-t/\epsilon}}{2} v ^2$	$\mathrm{d}x = v\mathrm{d}t$	$rac{1}{2}e^{t/\epsilon} p ^2$	$- abla rac{\delta \mathcal{F}}{\delta ho}$
OT-Flow	$\mathcal{D}_{KL}(\pi \ ho)$	0	$\frac{1}{2} v ^2$	$\mathrm{d}x = v\mathrm{d}t$	$\frac{1}{2} p ^2$	$-\nabla U$
Boltzmann generator	$ \begin{array}{c} \lambda \mathcal{D}_{KL}(\pi \ \rho) \\ + (1 - \lambda) \mathcal{D}_{KL}(\rho \ \pi) \end{array} $	0	0	$\mathrm{d}x = v\mathrm{d}t$	$\sup_{v \in K} -p^\top v$	$- abla_p H(x, abla U)$
Schrödinger bridge	$\rho = \pi$	0	$\frac{1}{2} v ^2$	$\mathrm{d}x = \sigma v \mathrm{d}t + \sigma \mathrm{d}W_t$	$\frac{1}{2} p ^2$	$-\sigma \nabla U$
Generalized Schrödinger bridge	$\rho = \pi$	$\mathcal{I}(x, ho)$	$rac{1}{2} v ^2$	$\mathrm{d}x = \sigma v \mathrm{d}t + \sigma \mathrm{d}W_t$	$rac{1}{2} p ^2$	$-\sigma abla U$
HJB-regularized SGM	$-\mathbb{E}_{ ho}[\log\pi]$	0	$\frac{ v ^2}{2} - \nabla \cdot f$	$dx = (f + \sigma v) dt + \sigma dW_t$	$\begin{vmatrix} -f \cdot p + \frac{\sigma^2}{2} p ^2 \\ +\nabla \cdot f \end{vmatrix}$	$\sigma \nabla \log \eta_{T-t}$
Stochastic OT normalizing flow	$\mathcal{D}_{KL}(\pi \ ho)$	0	$\frac{1}{2} v ^2$	$\mathrm{d}x = \sigma v \mathrm{d}t + \sigma \mathrm{d}W_t$	$rac{1}{2} p ^2$	$-\sigma \nabla U$
OT-Boltzmann generator	$ \begin{array}{c} \lambda \mathcal{D}_{KL}(\pi \ \rho) \\ + (1 - \lambda) \mathcal{D}_{KL}(\rho \ \pi) \end{array} $	0	$\frac{1}{2} v ^2$	$\mathrm{d}x = v\mathrm{d}t$	$\frac{1}{2} p ^2$	$-\nabla U$
Generalized OT-Flow (Relaxed WGF $\epsilon > 0$)	$\mathcal{F}(ho)e^{-T/\epsilon}$	$rac{e^{-t/\epsilon}}{\epsilon}\mathcal{F}(ho)$	$\frac{e^{-t/\epsilon}}{2} v ^2$	$\mathrm{d}x = v\mathrm{d}t$	$rac{1}{2}e^{t/\epsilon} p ^2$	$-\nabla U$
Build your own generative model	Choose your	own cost	functions and	dynamics here	?	?

See full chart: arXiv:2304.1353!



Experiment with your own algorithm here...





Successful generative flows & diffusions are mean-field games **Generative modeling benefits from PDE analysis**

Common **backward-forward** mathematical structure

Backward equation determines optimal velocity field

Other related topics & recent extensions

- Score probability flow as an MFG Fisher information as interaction
- Learn **robustly** distributions on manifolds via MFG & Wasserstein proximals, see poster by Hyemin Gu
- **SGM MFG approximates Wasserstein** proximal operator, poster by Ben Zhang

Forward equation determines generation

Applies to all flow and diffusion-based models





Ben Zhang, Siting Liu, Wuchen Li, M.K., & Stan Osher



Score-based generative models are provably robust: a UQ perspective





Benjamin Zhang, Brown

Mimikos-Stamotopoulos, N., Zhang, B. J., & Katsoulakis, M. A. (2024). arXiv preprint arXiv:2405.15754





Score-based generative modeling with SDEs



Song et al. '20

Different score-matching objectives

$$\begin{split} \min_{\theta} C_{ESM}(\theta) &= \min_{\theta} \int_{0}^{T} \int_{\mathbb{R}^{d}} \frac{\sigma(T-s)^{2}}{2} \|\mathbf{s}_{\theta}(y,s) - \nabla \log \eta(y,s)\|^{2} \eta(y,s) \, dy \, ds \\ \min_{\theta} C_{ISM}(\theta) &= \min_{\theta} \int_{0}^{T} \int_{\mathbb{R}^{d}} \sigma(T-s)^{2} \left[\frac{1}{2} \|\mathbf{s}_{\theta}(y,s)\|^{2} + \nabla \cdot \mathbf{s}_{\theta}(y,s) \right] \eta(y,s) \, dy \\ \min_{\theta} C_{DSM}(\theta) &= \min_{\theta} \int_{0}^{T} \int_{\mathbb{R}^{d}} \int_{\mathbb{R}^{d}} \sigma(T-s) \|\mathbf{s}_{\theta}(y,s) - \nabla \log \eta(y,s|y')\|^{2} \eta(y,s) \, dy \end{split}$$

 $Y(s) \sim \eta(\cdot, s)$

Denoising process $X(0) \sim \eta(\cdot, T)$

ds

Errors of SGM

- Finite sample error e_1
- Choice of score-matching objective e_2
- Score function approximation e_3

Research question:

How well does generative distribution $m_g(T)$ approximate data distribution π ? $"\mathbf{d}(m_g(T), \pi) \leq \mathscr{F}(e_1, e_2, e_3, e_4, e_5)"$

Integral probability metric (IPM): d(

E.g., Wasserstein-1, $\mathscr{X} = \{ \psi : \Omega \rightarrow \mathbb{R} \}$

K. Chowdhary and **P. Dupuis**, *Distinguishing and integrating aleatoric and epistemic variation in uncertainty quantification*, ESAIM: M^2NA (2013)

- Reference measure e_4
- Early stopping e_5
- Discretization error e_6

$$\begin{aligned} \left\| \nu_1, \nu_2 \right\| &= \sup_{\psi \in \mathcal{X}} \int \psi(x) \, d(\nu_1 - \nu_2) \\ \mathbb{R}, \left\| \nabla \psi \right\|_{\infty} \leq 1 \end{aligned}$$

Model form uncertainty quantification for SGMs

Wasserstein Uncertainty Propagation (WUP) theorem (partial)

Two SDEs with drifts b^1 and b^2 on domain $\Omega = R \mathbb{T}^d$ $\partial_t m^1 - \nabla \cdot (m^1 b^1) = \Delta m^1, m^1(0) = m$

If $L^2(m^2)$ error is bounded

 $\mathbf{d}_1(m^2(T), m^1(T)) \le CR^{3/2}$

Direct bound for Wasserstein-1 without appealing to KL divergence!

$$a_1 \qquad \partial_t m^2 - \nabla \cdot (m^2 b^2) = \Delta m^2, m^2(0) = m^2$$

 $\|b^2 - b^1\|_{L^2(m^2)}^2 = \int_0^T \int_{\Omega} \|b^2(x,t) - b^1(x,t)\|^2 m^2(t,x) \, dx \, dt \le \varepsilon^2$

Then the Wasserstein distance between distributions $m^1(T)$ and $m^2(T)$ is bounded

$$\left(1 + \sqrt{\|\nabla b^1\|_{\infty}}\right) (\mathbf{d}_1(m_1, m_2) + \varepsilon)$$

Robustness under explicit score matching <u>Application of WUP to SGM with explicit score matching</u>

Data distribution $\pi \in \mathscr{P}(\Omega)$ on domain $\Omega = R \mathbb{T}^d$ Two SDEs: True drift $\nabla \log \eta^{\pi}$ and approximate drift: $\mathbf{b}_{\theta} = \mathbf{s}_{\theta}(T - t, x)$

$$\partial_t m_g - \nabla \cdot (m_g \mathbf{b}_{\theta}) = \Delta m_g, m_g(0)$$

If ESM error is
$$e_{nn}$$
:
$$\int_{0}^{T} \int_{\mathbb{R}^{d}} ||\mathbf{s}_{\theta}(s, y)|$$

$$\mathbf{d}_{1}(\pi, m_{g}(T)) \leq CR^{3/2} \left(1 + \sqrt{\|\nabla \mathbf{s}_{\theta}\|_{\infty}}\right) \left(Re^{-\frac{\omega T}{R^{2}}} \mathbf{d}_{1}\left(\pi, \frac{1}{vol(R\mathbb{T}^{d})}\right) + \sqrt{e_{nn}}\right)$$

Choice of reference measure ESM error

Direct bound for Wasserstein-1 without appealing to KL divergence!

oproximate drift: $\mathbf{b}_{\theta} = \mathbf{s}_{\theta}(T - t, x)$ $0) = \frac{1}{vol(R\mathbb{T}^d)}$ Denoising process

Model form error

 $-\nabla \log \eta(y,s) \|^2 \eta(y,s) \, dy \, ds < e_{nn}, \text{ then}$

Robustness under denoising score matching Main result Assume score s_{θ} learned via DSM with early stopping, which provides density lower bound

$$C_{DSM}^{N}(\theta) = \int_{\epsilon}^{T} \int_{\mathbb{R}^{d}} \int_{\mathbb{R}^{d}} \sigma(T-s) \| s_{\theta}(y,s) - s_{\theta}(y,s) - s_{\theta}(y,s) - s_{\theta}(y,s) + s_{\theta}($$

Then,

$$\mathbf{d}_{1}(\pi, m_{g}(T)) \lesssim \sqrt{\epsilon} + R^{3/2}(1 + \sqrt{\|\nabla \mathbf{s}_{\theta}\|_{\infty}}) \left(Re^{-\frac{\omega T}{R^{2}}} \mathbf{d}_{1}\left(\pi, \frac{1}{vol(R\mathbb{T}^{d})}\right) + \sqrt{e_{nn}'} \right),$$

where

Direct bound for IPMs without appealing to **KL** divergence!

$$\sqrt{e'_{nn}} \lesssim \sqrt{e_{nn}} + \sqrt{\left(1 + \frac{|\log(\delta)|}{\sqrt{\epsilon}} + T ||\mathbf{s}_{\theta}||^{2}_{C^{2}([0,T] \times \Omega)}\right)} \mathbf{d}_{1}(\pi^{N}, \pi) .$$
DSM error
DSM error
Einite sample error

$\pi^{\epsilon} > \delta, \hat{\pi}^{N,\epsilon} > \delta$ Model form error

 $-\nabla \log \eta(y, s | y') \|^2 \eta(y, s | y') \hat{\pi}^N(y') dy dy' ds < e_{nn}$

Choice of reference measure

of score matching objective

 Regularizing test functions allows us to bound stronger TV norm with a weaker Wasserstein-1 norm.

Step 1: Kolmogorov backward equation determines suitable test functions

Step 2: Integral probability metrics bounds depend on gradient estimates

Step 3: Bernstein estimates from HJB equations provide gradient estimates

$$\partial_t m^1 - \nabla \cdot (m^1 b^1) = \Delta m^1, m^1(0) = m$$

 $\lambda = m^1 - m^2$ satisfies

Difference of measures evolution $\partial_t \lambda - \Delta \lambda - \nabla \cdot (\lambda b^1 + m^2(b^1 - b^2)) = 0$ in $(0,T) \times \Omega$, $\lambda(0) = m_2 - m_1$ in Ω .

Integrate against a test function $\phi(t, x)$ that satisfies KBE with terminal condition $\psi \in \mathscr{X}$ $-\partial_t \phi - \Delta \phi + b^1 \cdot \nabla \phi = 0 \text{ in } [0,T) \times \Omega, \quad \phi(T,x) = \psi(x) \text{ in } \Omega$

Step 1: Kolmogorov backward equation (KBE) determines suitable test functions

$$\partial_t m^2 - \nabla \cdot (m^2 b^2) = \Delta m^2, m^2(0) = m_2$$

Step 2: Integral probability metrics bounds depend on gradient estimates

$$\begin{cases} \partial_t \lambda - \Delta \lambda - \nabla \cdot (\lambda b^1 + m^2(b^1 - b^2)) = 0 \text{ in } (0,T) \times \Omega, \quad \lambda(0) = m_2 - m_1 \text{ in } \Omega, \\ -\partial_t \phi - \Delta \phi + b^1 \cdot \nabla \phi = 0 \text{ in } [0,T) \times \Omega, \quad \phi(T,x) = \psi(x) \text{ in } \Omega \end{cases}$$

Integrate first equation against the second, then integrate by parts. Then,

$$\mathbf{d}(m^{1}(T), m^{2}(T)) \leq \sup_{\psi \in \mathcal{X}} \left| \int_{\Omega} \lambda(0, x) \phi(0, x) dx \right| + \sup_{\psi \in \mathcal{X}} \left| \int_{0}^{T} \int_{\Omega} m^{2} \nabla \phi \cdot (b^{2} - b^{1}) dx dt \right|.$$

Bounds needs gradient estimates! For Wasserstein-1, $\sup_{\psi \in \mathcal{X}} \left| \int_{\Omega} \lambda(0,x) \phi(0,x) dx \right| \leq \mathbf{d}_1(m_1,m_2) \|\nabla \phi(0,x)\|_{\infty}$

ward-forward ure once again!

Step 3: Bernstein estimates from HJB theory provide gradient estimates

$$\mathbf{d}(m^{1}(T), m^{2}(T)) \leq \sup_{\psi \in \mathcal{X}} \left| \int_{\Omega} \lambda(0, x) \phi(0, x) dx \right| + \sup_{\psi \in \mathcal{X}} \left| \int_{0}^{T} \int_{\Omega} m^{2} \nabla \phi \cdot (b^{2} - b^{1}) dx dt \right|$$

$$-\partial_t \phi - \Delta \phi + b^1 \cdot \nabla \phi = 0$$

• Derive a PDE for
$$z = \frac{1}{2} \|\nabla \log \phi\|^2$$

- Apply the maximum principle to obtain a bound on $z(t, x) \leq C \|\log \psi\|_{\infty} + c \|\nabla \log \psi\|_{\infty}$
- Derive a bound for $\nabla \phi(t, x)$, bound the IPM.

in $[0,T) \times \Omega$, $\phi(T,x) = \psi(x)$ in Ω

Conclusion and ongoing work UQ and PDE regularity theory contributes to analysis, robustness of generative AI algorithms

the quality of a generative model

- e.g., normalizing flows

• Making the bounds explicitly computable: provide a posteriori estimates on

 Most useful for guarantees in likelihood-free inference settings & use IPM: $\left|\mathbb{E}_{\pi}h - \mathbb{E}_{m_g(T)}h\right| \leq \mathbf{d}(m_g(T), \pi) \leq \mathcal{F}(e_1, e_2, e_3, e_4, e_5).$

• Extensions to other generative flows with similar UQ issues (learning a drift)

Structure-informed generative modeling

Jeremiah Birrell, Texas State, see <u>poster</u>

Ziyu Chen, UMass Amherst

Structured-informed learning: target data & distribution π

π

 ${\cal T}$

Learning from data, math- & physics-informed structures We learn in (an even more) restricted & relevant space

- How to build embedded distribution learning?
- Can we use structure/
- Quantify the gains in performance

Sample Complexity of Probability Divergences under Symmetry: Quantify the gains in data needed for the same performance

$$|D_{f_{\alpha}}^{\Gamma}(P||\pi) - D_{f_{\alpha}}^{\Gamma_{\Sigma}}(P_{m}||\pi_{n})| \leq C_{1}$$

see poster by Ziyu Chen

P. Dupuis and Y. Mao, *Formulation and* properties of a divergence used to compare probability measures without absolute continuity, ESAIM: COCV, 2022 Birrell, **P. Dupuis**, M. A. Katsoulakis, Y. Pantazis, L. Rey-Bellet, (f, Γ) -Divergences: Interpolating between f-Divergences and IPMs, Journal of Machine Learning Research, 2022

-0.5

-0.5

reduction in # of needed data due to equivariance

Related papers

- •J. Birrell, M.A. Katsoulakis, L. Rey-Bellet, W. Zhu. Structure-preserving GANs. ICML 2022
- •Z. Chen, M. A. Katsoulakis, L. Rey-Bellet, W. Zhu, Sample Complexity of Probability Divergences under Group Symmetry, **ICML 2023**
- •Z. Chen, M. A. Katsoulakis, L. Rey-Bellet, W. Zhu, *Statistical Guarantees of Group-Invariant GANs, submitted*, (2024).
- •Z. Chen, M.A. Katsoulakis, B. Zhang, *Sample complexity and equivariant score matching of SGM with group symmetry*, in preparation.

Robust Generative Modeling: Mean-field Games, Hamilton-Jacobi, Proximals & UQ Α.

- B. J. Zhang, M. A. Katsoulakis, A Mean-Field Games laboratory for generative modeling, Arxiv, (2023). 1.
- 2. via well-posed generative flows, Arxiv, (2024).
- 3. *Arxiv,* (2024).
- 4. resolve memorization, Arxiv, (2024).

B. <u>Structure-informed Learning</u>

1. Z. Chen, M. A. Katsoulakis, L. Rey-Bellet, W. Zhu, Statistical Guarantees of Group-Invariant GANs, Arxiv, (2024). 2. Z. Chen, M. A. Katsoulakis, L. Rey-Bellet, W. Zhu, Sample Complexity of Probability Divergences under Group Symmetry, ICML 2023 3. J. Birrell, M.A. Katsoulakis, L. Rey-Bellet, W. Zhu, Structure-preserving GANs. ICML 2022 4. J. Birrell, M.A. Katsoulakis, L. Rey-Bellet, B. J. Zhang, W. Zhu, Nonlinear denoising score matching for enhanced learning of structured

distributions, Arxiv, (2024).

Optimal Transport Proximals for Machine Learning C.

- 1. Conference on Learning Representations, ICLR 2023
- 2. algorithms for high-dimensional scarce data, SIAM Data Science, to appear, (2024).
- 3. **Probability Metrics, Journal of Machine Learning Research & NeurIPS, (2022)**
- 4. divergences, Arxiv, (2024)

H. Gu, M. A. Katsoulakis, L. Rey-Bellet, B. J. Zhang, Combining Wasserstein-1 and Wasserstein-2 proximals: robust manifold learning

N. Mimikos-Stamatopoulos, <u>B. J. Zhang</u>, M. A. Katsoulakis, *Score-based generative models are provably robust: a UQ perspective*,

B. J. Zhang, S. Liu, W. Li, M. A. Katsoulakis, S. Osher, Wasserstein proximal operators describe score-based generative models and

References

J. Birrell, P. Dupuis, M. A. Katsoulakis, Y. Pantazis, L. Rey-Bellet, *Function-space regularized Rényi divergences*, International

H. Gu, P. Birmpa, Y. Pantazis, M. A. Katsoulakis, and L. Rey-Bellet, *Lipschitz-regularized* gradient flows and generative particle J. Birrell, P. Dupuis, M. A. Katsoulakis, Y. Pantazis, L. Rey-Bellet, (f, Γ) -Divergences: Interpolating between f-Divergences and Integral <u>Z. Chen, H. Gu</u>, M. A. Katsoulakis, L. Rey-Bellet, W. Zhu, *Learning heavy-tailed distributions with Wasserstein-proximal-regularized α-*

Extra Slides

Wasserstein gradient flows Gradient flows on the space of probability distributions

$$\frac{\partial \rho}{\partial t} = \nabla \cdot \left(\rho \, \nabla \frac{\delta \mathcal{F}}{\delta \rho} \right)$$

 $\mathscr{F}(\rho) = \mathscr{D}_{KL}(\rho \| \pi) = \mathbb{E}_{\rho} \left| \log \frac{\rho}{\pi} \right|$ $\mathscr{F}(\rho) = \mathscr{D}_{\alpha}(\rho \| \pi) = \mathbb{E}_{\pi} \left[f_{\alpha} \left(\frac{\rho}{\pi} \right) \right]$

_____Describes a path on the space of probability distributions

Overdamped Langevin

> Porous medium equation

 $f_{\alpha}(x) = \frac{x^{\alpha}}{\alpha(\alpha - 1)}$

Wasserstein gradient flows as solutions to MFGs

$$\inf_{v,\rho} \left\{ \mathscr{F}(\rho(\cdot,T)) + \int_0^T \frac{e^{-t/\epsilon}}{\epsilon} \mathscr{F}(\rho(\cdot,t)) \, dt + \int_0^T \int_{\mathbb{R}^d} \frac{e^{-t/\epsilon}}{2} \|v\|^2 \rho(x,t) \, dx \, dt \right\}$$

s.t. $\partial_t \rho + \nabla \cdot (v\rho) = 0, \qquad \rho(x,0) = \rho_0(x)$

$$-\epsilon \frac{\partial U}{\partial t} + U + \frac{\epsilon}{2} |\nabla U|^2 = \frac{\delta \mathcal{F}}{\delta \rho}$$
$$\frac{\partial \rho}{\partial t} - \nabla \cdot (\rho \nabla U) = 0$$
$$U(x, T) = \frac{\delta \mathcal{F}}{\delta \rho} (\rho(\cdot, T)), \rho(x, 0) = \rho_0(x)$$

 $\epsilon \rightarrow 0$ Relaxation limit enforces a "local equilibrium" :

 $U\approx \frac{\delta \mathcal{F}}{\delta \rho}$

$$\begin{split} U &= \frac{\delta \mathcal{F}}{\delta \rho} \\ \frac{\partial \rho}{\partial t} - \nabla \cdot \left(\rho \, \nabla U \right) = 0 \\ \rho(x, 0) &= \rho_0(x) \end{split}$$

MFGs reveal an interpolation between Wasserstein gradient flows & normalizing flows

$$\inf_{v,\rho} \left\{ \mathscr{F}(\rho(\cdot,T)) + \int_0^T \frac{e^{-t/\epsilon}}{\epsilon} \mathscr{F}(\rho(\cdot,t)) \, dt + \int_0^T \int_{\mathbb{R}^d} \frac{e^{-t/\epsilon}}{2} \|v\|^2 \rho(x,t) \, dx \, dt \right\}$$

s.t. $\partial_t \rho + \nabla \cdot (v\rho) = 0, \qquad \rho(x,0) = \rho_0(x)$

$$\epsilon \to 0$$

$$U = \frac{\delta \mathcal{F}}{\delta \rho}$$
$$\frac{\partial \rho}{\partial t} - \nabla \cdot (\rho \nabla U) = 0$$
$$\rho(x,0) = \rho_0(x)$$

Wasserstein gradient flows

 $0 < \epsilon < \infty$

$$\begin{aligned} \mathcal{E} &\to \infty \\ \inf_{\nu,\rho} \left\{ \mathscr{F}(\rho(\cdot,T)) + \int_0^T \int_{\mathbb{R}^d} \frac{1}{2} \|\nu\|^2 \rho(x,t) \\ \text{s.t. } \partial_t \rho + \nabla \cdot (\nu\rho) &= 0, \qquad \rho(x,0) = \rho_0(x,0) \end{aligned} \right. \end{aligned}$$

Optimal transport normalizing flow

