Reversible random number generation for adjoint Monte Carlo simulation of the heat equation

Emil Løvbak, Frédéric Blondeel, Adam Lee, Lander Vanroye, Andreas Van Barel, and Giovanni Samaey

Abstract In PDE-constrained optimization, one aims to find design parameters that minimize some objective, subject to the satisfaction of a partial differential equation. A major challenge is computing gradients of the objective to the design parameters, as applying the chain rule requires computing the Jacobian of the design parameters to the PDE’s state. The adjoint method avoids this Jacobian by computing partial derivatives of a Lagrangian. Evaluating these derivatives requires the solution of a second PDE with the adjoint differential operator to the constraint, resulting in a backwards-in-time simulation.

Particle-based Monte Carlo solvers are often used to compute the solution to high-dimensional PDEs. However, such solvers have the drawback of introducing noise to the computed results, thus requiring stochastic optimization methods. To guarantee convergence in this setting, both the constraint and adjoint Monte Carlo simulations should simulate the same particle trajectories. For large simulations, storing full paths from the constraint equation for re-use in the adjoint equation becomes infeasible due to memory limitations. In this paper, we provide a reversible extension to the family of permuted congruential pseudorandom number generators (PCG). We then use such a generator to recompute these time-reversed paths for the heat equation, avoiding these memory issues.
1 Introduction

Partial differential equations (PDEs) are an indispensable tool for modeling physics in many engineering fields. When solving a design problem, e.g., building the cheapest, most efficient component for a given purpose, the design must satisfy the problem’s physics, requiring a numerical solver for the PDE. To improve the design’s objective function, one can compute its gradient to the design parameters using the discrete adjoint approach. If the PDE solver is based on a particle simulation, then the adjoint solver traces the same particle trajectories in a time reversed fashion. Storing all of these paths can incur unacceptably high memory costs. We therefore propose a novel approach to recompute these paths using a reversible random number generator.

Mathematically, we consider a PDE-constrained optimization problem of the form

$$\min_{u(x)} J(y(x, t), u(x)),$$

subject to $B(y(x, t); u(x)) = 0$. (1)

Here, $B(\cdot; u(x))$ is a differential operator, parameterized by a time-independent control $u(x)$, applied to a candidate solution $y(x, t)$, a function of space $x \in D_x \subseteq \mathbb{R}^d$ and time $t \in \mathbb{R}_{\geq 0}$. The objective $J(y(x, t), u(x))$, is a scalar function to be minimized, typically involving integration over space and time. For all but the most trivial of applications, solving the PDE requires a discretization. When discretizing the PDE $B(y(x, t); u(x))$ and objective $J(y(x, t), u(x))$, one gets a discrete equivalent to (1),

$$\min_{\hat{u}} \hat{J}(\hat{y}, \hat{u}), \quad \text{subject to } \hat{B}(\hat{y}, \hat{u}) = 0,$$ (2)

where $\hat{y} \in \mathbb{R}^\alpha, \hat{u} \in \mathbb{R}^\beta, \hat{J}: \mathbb{R}^\alpha \times \mathbb{R}^\beta \to \mathbb{R}$ and $\hat{B}(\cdot; \hat{u}): \mathbb{R}^\alpha \to \mathbb{R}^\gamma$ are discretizations of the quantities in (1) and the integer values $\alpha, \beta$ and $\gamma$ are discretization dependent.

In this work, we solve the PDE with particle-based Monte Carlo, i.e., we simulate sample trajectories of particles whose distribution density corresponds with a rescaling of the PDE’s solution. The main advantage of Monte Carlo methods lies in their ability to simulate high-dimensional PDEs, without storing their state on a high-dimensional grid. These methods, however, come with the drawback of introducing noise on the computed results, the variance of which scales as $P^{-1}$, with $P$ the number of simulated particle trajectories. Stochastic optimization routines are therefore needed to solve (2). While this work is motivated by its future applicability in the simulation of kinetic models in neutral particle codes for fusion reactor design as used in [10, 25], we consider a simplified setting here, based on the heat equation.

Solving (2) with a gradient-based optimization method, e.g., stochastic gradient descent, requires evaluating both $\hat{J}(\hat{y}', \hat{u}')$ and $\frac{d\hat{J}}{d\hat{u}}(\hat{y}', \hat{u}')$ for a proposed control $\hat{u}'$ and corresponding state $\hat{y}'$, with $\hat{B}(\hat{y}', \hat{u}') = 0$. As the numerical solver $\hat{B}(\cdot; \hat{u}')$ defines an implicit function $\hat{y}' = \hat{y}(\hat{u}')$, one may try to compute the gradient as

$$\frac{d\hat{J}}{d\hat{u}}(\hat{y}(\hat{u}'), \hat{u}') = \frac{\partial \hat{J}}{\partial \hat{u}}(\hat{y}', \hat{u}') + \frac{\partial \hat{J}}{\partial \hat{y}}(\hat{y}', \hat{u}') \frac{d\hat{y}}{d\hat{u}}(\hat{u}')$$.
Evaluating the Jacobian \( \frac{d\hat{J}}{d\hat{u}} \) is often infeasible, given its dimensionality and the implicit definition of \( \hat{y}(\hat{u}) \). We thus consider three alternatives to compute \( \frac{d\hat{J}}{d\hat{u}} \): finite differences, algorithmic differentiation and the adjoint-based approach.

The finite-difference approach is the only one of the three which is a true black-box approach, i.e., not needing knowledge of the solver internals. It is also simple to implement. For each element of \( \frac{d\hat{J}}{d\hat{u}} \), one simply subtracts two solver outputs from each other and performs a division. Its main drawbacks are that it scales poorly with the dimension of \( \hat{u} \), as the PDE needs to be solved \( \beta \) times in addition to the solve for computing \( \hat{y}' \), and that it typically only achieves a relative precision in the order of \( \sqrt{\epsilon_{\text{mach}}} \) due to cancellation errors, with \( \epsilon_{\text{mach}} \) the machine precision.

Algorithmic differentiation \([11]\), while not fully black-box, takes the existing solver code and automatically generates code for calculating its derivative. Conceptually, this approach relies on repeated application of the chain rule. In our case, so-called backward mode is the most advantageous as \( \beta \gg 1 \). This approach computes \( \frac{d\hat{J}}{d\hat{u}}(\hat{y}', \hat{u}') \) to a relative precision in the order of \( \epsilon_{\text{mach}} \), with a theoretical cost upper-bound of four times that of evaluating \( \hat{J}(\hat{y}', \hat{u}') \) \([11]\). However, in the context of Monte Carlo simulations, this approach requires accessing particle states in a time-reversed fashion. Storing these paths in memory is infeasible for all but toy problems. Therefore, one soon needs to apply checkpointing, i.e., storing the simulation state at intermediate moments in time from which partial paths can be recomputed as they are needed \([21]\). This recomputation has at least the cost of the initial constraint simulation and the checkpointing itself often incurs a non-negligible overhead.

The adjoint-based approach \([13]\) uses a solver for \( \hat{B}^*(-; \hat{y}', \hat{u}') \), the adjoint operator to \( \hat{B}(-; \hat{u}') \), derived at \( \hat{y}' \). In this approach, we compute the gradient \( \frac{d\hat{J}}{d\hat{u}}(\hat{y}', \hat{u}') \), through a vector of Lagrange multipliers \( \hat{\lambda} \). The main advantage of this approach is the reduced computational cost. The adjoint PDE for computing \( \hat{\lambda} \) is typically similar to the constraint PDE, so the gradient can be computed at the cost of one additional PDE solve and a small number of matrix-vector products. The main drawback of the adjoint-based approach is the additional work needed in deriving and implementing the adjoint solver. However, as the constraint and adjoint PDE are often similar, existing code can be reused with minimal modifications to develop such a solver.

In the adjoint-based approach one can apply two strategies \([6]\). In the first strategy, called the continuous adjoints or optimize then discretize (OTD), one first derives the adjoint PDE and discretizes each PDE independently. When using Monte Carlo simulation, this strategy has two issues. Often, the adjoint PDE depends on the solution of the constraint PDE, requiring the construction of a solution on the high-dimensional grid that we wish to avoid. Discretizing both PDEs separately also decouples the resulting stochastic simulations, hampering the convergence of stochastic gradient descent, see e.g. \([3, \text{Thm. 4.8}]\). We therefore use discrete adjoints or discretize then optimize (DTO), where we directly derive an adjoint solver from the constraint solver. This derivation results in the same particle paths being used in both discretizations, except for the adjoint simulation running backwards in time.

Note that DTO avoids computing a high-dimensional solution, while introducing a need to store the Monte Carlo paths used in solving the constraint PDE, for use in the
adjoint simulation. Note that this is the same issue as was present in backward-mode algorithmic differentiation, which has conceptual similarities to the adjoint-based approach. While checkpointing can be used to avoid the memory issue, it has the additional drawback that it introduces extra complexity to the adjoint simulation.

The goal of this work is twofold: to present a DTO adjoint approach for Monte Carlo simulations, and to do away with checkpointing by re-computing paths time-reversed during the adjoint simulation. To compute time-reversed paths, we extend the family of permuted congruential pseudorandom number generators (PCG) [23] to make them reversible, i.e., one can request the next and previous random value in the sequence at the same computational cost. While a similarly reversible generator was developed in [30], based on Multiple Recursive Generators [16], we opt for our own implementation based on PCG due to its performance and statistical properties.

The remainder of this paper is structured as follows. In Section 2, we introduce the discrete adjoint approach in the context of Monte Carlo simulations. We then introduce a 1D test problem, based on the heat equation, on which we demonstrate our reversible approach. In Section 3, we introduce the PCG family of random number generators and show how we adapt the generators to make them reversible. We then demonstrate the speedup and memory gains provided by the reversible approach in Section 4. Finally in Section 5, we draw our conclusions and outline our future work.

2 Adjoint Monte Carlo for particle simulations

In the adjoint-based optimization approach, we replace the constrained discrete problem (2) by one of finding stationary points of the discrete Lagrangian

$$\hat{L}(\hat{y}, \hat{u}, \hat{\lambda}) = \hat{J}(\hat{y}, \hat{u}) + \hat{\lambda}^T \hat{B}(\hat{y}, \hat{u}),$$

with $\hat{\lambda} \in \mathbb{R}^\gamma$ a vector of Lagrange multipliers. We now find these fixed points by setting the partial derivatives in $\hat{\lambda}, \hat{y}$ and $\hat{u}$ to zero:

$$\frac{\partial \hat{L}^T}{\partial \hat{\lambda}} (\hat{y}, \hat{u}, \hat{\lambda}) = \hat{B}(\hat{y}, \hat{u}) = 0,$$

Constraint equation; (3)

$$\frac{\partial \hat{L}^T}{\partial \hat{y}} (\hat{y}, \hat{u}, \hat{\lambda}) = \frac{\partial \hat{J}^T}{\partial \hat{y}} (\hat{y}, \hat{u}) + \frac{\partial \hat{B}^T}{\partial \hat{y}} (\hat{y}, \hat{u}) \hat{\lambda} = 0,$$

Adjoint equation; (4)

$$\frac{\partial \hat{L}^T}{\partial \hat{u}} (\hat{y}, \hat{u}, \hat{\lambda}) = \frac{\partial \hat{J}^T}{\partial \hat{u}} (\hat{y}, \hat{u}) + \frac{\partial \hat{B}^T}{\partial \hat{u}} (\hat{y}, \hat{u}) \hat{\lambda} = 0,$$

Design equation. (5)

From (3), we see that the constraining PDE is satisfied for any stationary point of the Lagrangian. Therefore, it holds that, for any $\hat{y}'$, $\hat{u}'$ and $\hat{\lambda}'$ solving the system (3)–(5), $\hat{L}(\hat{y}', \hat{u}', \hat{\lambda}') = \hat{J}(\hat{y}', \hat{u}')$. A fixed point of the Lagrangian is thus also a fixed point of the objective function and a possible solution to the constrained problem (2).

For Monte Carlo, the simulation state $\hat{y}$ consists of an ensemble of $P$ particles.
\[ \{Y_{p, \tau}\}_{p=1}^P, \] 

with \( Y_{p, \tau} \) a vector valued quantity defined at each moment in time \( \tau = 0, \ldots, T \) for each particle with index \( p = 1, \ldots, P \). Assuming independent particles, their time discretized dynamics are described by algebraic expressions

\[
B_{p, \tau+1}(Y_{p, \tau+1}, Y_{p, \tau}; \hat{u}) = 0, \quad \tau = 0, \ldots, T - 1, 
\]

relating particle states at subsequent time steps. We structure the simulation state as

\[
\hat{y} = \left[ \begin{array}{c} Y_{0,0}^T \cdots Y_{0,T}^T \\ \vdots \\ Y_{P,0}^T \cdots Y_{P,T}^T \end{array} \right]^T, 
\]

with the system \( \hat{B}(\hat{y}; \hat{u}) = 0 \) being given by the aggregation of the expressions (7). We now derive a linearization

\[
\hat{B}(\hat{y}; \hat{u}') \approx \frac{\partial \hat{B}}{\partial \hat{y}}(\hat{y}', \hat{u}') (\hat{y} - \hat{y}') 
\]

of the system assuming we have computed a solution \( \hat{y}' \) for a given \( \hat{u}' \) so that \( \hat{B}(\hat{y}'; \hat{u}') = 0 \). We now assume piecewise linearity of \( \hat{B}(\hat{y}; \hat{u}) \) in \( \hat{y} \) making (8) exact for a finite region of values \( \hat{y} \) around \( \hat{y}' \). This approach is also applicable to the non-linear case, under suitable combination with an iterative solver for (3) and (4).

In (8), we see that a Monte Carlo simulation, within a region of the solution space, can be written as a matrix-vector product between a Jacobian and a vector of offset particle states. We also observe that the Jacobian \( \frac{\partial \hat{B}}{\partial \hat{y}}(\hat{y}, \hat{u}) \) is blockwise lower-triangular with a single off-diagonal band of blocks, which is solved for \( \hat{y} \) using forward substitution. We now observe that the same Jacobian appears, transposed, in (4). We can thus solve (4) for \( \hat{\lambda} \) with a similar Monte Carlo simulation to (7). The transposed Jacobian is upper-triangular, meaning the adjoint Monte Carlo simulation corresponds with backward substitution, and thus runs backward in time.

In Section 2.1, we present a test problem, using the heat equation. In Section 2.2, we discuss adjoint simulation time reversal, motivating our reversible approach.

### 2.1 Cooling a 1D rod

We consider the problem of cooling a 1D rod with temperature \( \theta(x, t) \) with \( x \in [0, L] \) and \( t \in \mathbb{R}_{\geq 0} \), cooled by a fluid with a rate \( u(x) \), which we write formally as

\[
\min_{u(x)} J(\theta(x, t), u(x, t)) = \int_0^\infty \int_0^L \frac{1}{2} \theta(x, t)^2 \, dx \, dt + \nu \int_0^L \frac{1}{2} u(x)^2 \, dx, \\
\text{subject to } \mathcal{B}(\theta(x, t); u(x, t)) = \frac{\partial}{\partial t} \theta(x, t) - \frac{\partial^2}{\partial x^2} \theta(x, t) + u(x) \theta(x, t) = 0, \\
\theta(x, 0) = \theta_0(x), \quad \theta(0, t) = \theta(L, t),
\]

where \( \nu \in \mathbb{R}_{\geq 0} \) is a regularization parameter. For simplicity, we consider \( \theta(x, t) \) and \( u(x) \) to be dimensionless.
Given a spatial discretization with cell width $\Delta x$, we perform the approximation

$$ J(\theta(x,t), u(x,t)) \approx \hat{J}(\hat{\theta}, \hat{u}) = \Delta t \sum_{\tau=0}^{T'} \Delta x \frac{1}{2} \hat{\theta}_\tau \hat{\theta}_\tau + \nu \Delta x \frac{1}{2} \hat{u}^\top \hat{u}, \quad (10) $$

where we introduce $\hat{\theta} \in \mathbb{R}^{(T'+1)\times N}$ and $\hat{u} \in \mathbb{R}^N$ as vector valued quantities indexed over time $\tau = 0, \ldots, T$ and space $n = 1, \ldots, N$ so that $N \Delta x = L$, and $T \Delta t$ is sufficiently large that (9) approximates a steady-state solution. Note that $\hat{\theta}_{\tau,n}$ denotes the solution value in the cell $(n - 1) \Delta x \leq x < n \Delta x$ at time $t = \tau \Delta t$. The notation $\sum'$ indicates halving of the first and last terms due to integration with the trapezoid rule.

At the Monte Carlo level, we consider an ensemble of $P$ “heat-transfer” particles

$$ \{Y_{p,\tau}\}_{p=1}^P = \{[X_{p,\tau}, W_{p,\tau}]\}_{p=1}^P, \quad (11) $$

determined by their position $X_{p,\tau}$ and a weight $W_{p,\tau}$ at each time step $\tau$. Given an ensemble (11), one can apply a binning approach to compute a stochastic quantity $\hat{\Theta}$ for which $E[\hat{\Theta}] = \hat{\theta}$, where for each $\tau, n$

$$ \hat{\Theta}_{\tau,n} = \sum_{p=1}^P \frac{1}{\Delta x} I_n(X_{p,\tau}) W_{p,\tau}, \quad \text{with} \quad I_n(x) = \begin{cases} 1, & \text{if } (n - 1) \Delta x \leq x < n \Delta x; \\ 0, & \text{otherwise}. \end{cases} $$

By substituting the stochastic estimate $\hat{\Theta}$ for $\hat{\theta}$ in (10), one then gets a stochastic estimate for $\hat{J}$ for a given ensemble of particles (6).

To initialize the simulation, we sample each particle’s initial position $X_{p,0}$ from the density function $\frac{\theta_0(x)}{\int_L \theta_0(x) dx}$. We then select initial weights $W_{p,0}$, such that $\hat{\Theta}_0 = \hat{\theta}_0$. We then iterate over a particle scheme consisting of two parts for each time step:

- **Diffusion step.** Update the particle’s position following a Brownian motion by sampling a normally distributed value $\xi_{p,\tau}$, i.e.,

$$ X_{p,\tau+1} = X_{p,\tau} + \sqrt{2 \Delta t} \xi_{p,\tau}, \quad \xi_{p,\tau} \sim \mathcal{N}(0, 1). $$

- **Reweighting step.** Reduce the particle’s weight with an exponential decay, i.e.,

$$ W_{p,\tau+1} = W_{p,\tau} \exp \left( -\Delta t \hat{u}(X_{p,\tau+1}) \right), $$

where $\hat{u}(x)$ denotes the value $\hat{u}_n$ with $n$ chosen so that $I_n(x)$ is non-zero.

Each particle trajectory $p$ is thus fully determined by its initial position $X_{p,0}$ and its Brownian increments $\xi_{p,\tau}$.

Rewriting the time-stepping in the form (7), for a given $\hat{u}'$ gives

$$ B_{p,\tau+1}(Y_{p,\tau+1}, Y_{p,\tau}; \hat{u}') = \begin{bmatrix} X_{p,\tau+1} - X_{p,\tau} - \sqrt{2 \Delta t} \xi_{p,\tau} \\ W_{p,\tau+1} - W_{p,\tau} \exp \left( -\Delta t \hat{u}'(X_{p,\tau+1}) \right) \end{bmatrix}, \quad \tau = 0, \ldots, T-1. \quad (12) $$
The Jacobian $\frac{\partial B}{\partial y_p} (y'_p, u'_p)$ is then block-diagonal with blocks $p = 1, \ldots, P$ given by

$$\frac{\partial B_p}{\partial y_p} (y'_p, u'_p) = \begin{bmatrix} \frac{\partial B_{p,1}}{\partial y_{p,1}} & \frac{\partial B_{p,2}}{\partial y_{p,2}} & \cdots & \frac{\partial B_{p,T}}{\partial y_{p,T}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial B_{p,T}}{\partial y_{p,T-1}} & \frac{\partial B_{p,T}}{\partial y_{p,T}} & \cdots & \frac{\partial B_{p,T}}{\partial y_{p,T}} \end{bmatrix},$$

with $\frac{\partial B_{p,T+1}}{\partial y_{p,T}} (y_{p,T+1}, y_{p,T}; u'_p) = \begin{bmatrix} -1 \\ 0 \\ \exp(-\Delta t \hat{u}'(X_{p,T+1})) \end{bmatrix}$, where the bottom-left element of $\frac{\partial B_{p,T+1}}{\partial y_{p,T}}$ is zero by the piecewise constantness of $\hat{u}$.

From (4), we derive a final condition at $\tau = T$ for each particle $p$

$$\hat{\lambda}_{p,T} = \begin{bmatrix} X^*_p \\ W^*_p \end{bmatrix} = -\frac{\partial \hat{J}}{\partial y_{p,T}} = -\begin{bmatrix} 0 \\ \Delta t \Theta(X_{p,T}) \end{bmatrix},$$

introducing $X^*_p$ and $W^*_p$ as adjoint variables, and a recursion for $\tau = T - 1, \ldots, 1$

$$\hat{\lambda}_{p,\tau} = -\frac{\partial B_{p,\tau+1}}{\partial y_{p,\tau}} \hat{\lambda}_{p,\tau+1} - \frac{\partial \hat{J}}{\partial y_{p,\tau}} = \begin{bmatrix} X^*_{p,\tau+1} \\ \exp(-\Delta t \hat{u}'(X_{p,\tau+1})) W^*_p \end{bmatrix} - \begin{bmatrix} 0 \\ \Delta t \Theta(X_{p,\tau}) \end{bmatrix}. \quad (13)$$

Observe that $\forall p, \tau : X^*_{p,\tau} \equiv 0$ meaning (13) defines a Monte Carlo simulation

$$W^*_p = \exp(-\Delta t \hat{u}'(X_{p,\tau+1})) W^*_p - \Delta t \Theta(X_{p,\tau}), \quad (14)$$

running in reverse. For each $p$ and $\tau$, this simulation contributes to (5) as

$$\frac{\partial B_{p,\tau}}{\partial u} (y'_p, u'_p, \hat{\lambda}_{p,\tau}) = \Delta t W_{p,\tau} \exp(-\Delta t \hat{u}'(X_{p,\tau+1})) [I_0(X_{p,\tau+1}) \cdots I_N(X_{p,\tau+1})] W^*_p. \quad (15)$$

The total gradient according to (5) is then

$$\frac{\partial \hat{L}}{\partial u} (y'_p, u'_p, \hat{\lambda}) = v \Delta x \hat{u}' + \sum_{p=0}^P \sum_{\tau=1}^T \frac{\partial B_{p,\tau}}{\partial u} (y'_p, u'_p, \hat{\lambda}_{p,\tau}).$$

### 2.2 Reversing particle trajectories

We observe that the adjoint simulation (14) requires the temperature profile $\Theta$, meaning that the full constraint simulation must be completed before starting the adjoint simulation. The adjoint simulation also requires the particle positions $X_{p,\tau}$ in time-reversed order. When $P \times N$ is small, it is possible to simply store the state of each particle at each time step $\tau$, this approach however becomes infeasible as
the simulation size increases. Large scale simulations will therefore need to resort to checkpointing, i.e., storing the constraint simulation state at a subset of time steps $\tau$. Such a checkpoint consists of the state vector $\hat{y}_\tau$ and the state of the random number generator at the end of the given time step. During the adjoint simulation, one loads these checkpoints in reverse order and re-computes the required path segments. For information on checkpointing see, e.g., [21, Sec. 5.2] and references therein.

While checkpointing avoids an uncontrolled increase in memory usage, it introduces an additional computational cost, which is at least that of simulating the constraint equation, on top of the cost of the adjoint simulation. We aim to avoid the need for checkpointing by re-computing the paths in time reversed order in the adjoint simulation, based on the final state of the constraint simulation. As we can re-write (12) as an explicit expression for $\hat{y}_\tau$, path generation is reversible if we know the random values involved. To compute these random values we introduce the concept of a reversible random number generator in the next section.

3 Reversible random number generators

In this section, we present one of the main contributions of this work, the reversal of the PCG family of pseudorandom number generators [23]. Although we specifically cover PCGs here, we remark that it is typical for the state-transition function of a pseudorandom generator to be a bijection, and thus reversible. This property follows from the fact that a non-bijective state-transition function makes some states more likely than others, thus reducing uniformity. It is however not necessarily the case that the reversal can be done at the same computational cost. Some examples of other candidate reversible generators are (those based on) linear congruential generators [5]; counter based generators such as SplitMix [27] and Random123 [26]; linear feedback shift register based generators such as the Mersenne Twister [20] and Xoshiro/Xoroshiro [1]; and chaotic generators such as SFC [9]. We first introduce PCGs in Section 3.1 and motivate their use as random bit generators. Next in Section 3.2, we reverse PCGs, so that we can request the previous value in a generator’s pseudorandom sequence at the same cost as requesting the next value. In Section 3.3, we then describe how we use the reversed generator to sample arbitrary distributions.

3.1 Permuted congruential generators

We choose to reverse the family of permuted congruential generators (PCG) [23]. PCGs make internal use of a linear congruential generator (LCG), i.e., generating pseudorandom integer values $\zeta_k$ in the range $[0, m - 1]$ through a recurrence

$$\zeta_{k+1} = a\zeta_k + c \mod m,$$  

(15)
with \(a\) and \(c\) integers in the range \([0, m - 1]\). However, even for well chosen values \(a, c\) and \(m\), LCGs have poor statistical properties, as demonstrated by benchmark tests such as TestU01 [15]. PCGs improve on the poor statistics of the underlying LCG by applying a 1-way parameterized permutation to its state \(\zeta_k\) to generate an output value. For technical details and an overview of generator variants, we refer to [23].

This combination of a simple internal update function and complex output function makes PCG a good candidate for reversal, while still achieving good statistical properties. While the paper [23] was not published in a peer-reviewed venue we have satisfactorily reproduced their TestU01 benchmark results and a number of our runs can be found together with our code referenced in Section 4. These generators are also widely used in the scientific computing community, being, e.g., the current default generator in NumPy [22]. While they are not suitable as cryptographic generators [4], and some seed pairs have been found that induce measurable correlation between sequences, see the discussion in [24, 29], to our knowledge, no issues have been found in PCGs counterindicating their use in scientific computing.

### 3.2 Reversing PCG

We reverse a PCG by reversing the underlying LCG. That is, we invert the recursion (15) going from state \(\zeta_{k+1}\) to state \(\zeta_k\). The 1-way output function can then be applied to these internal state values just as in the forward sequence generation. The problem of reversing the PCG thus reduces to that of reversing the update function (15), i.e., performing an update

\[
\zeta_k = a^{-1} (\zeta_{k+1} - c) \mod m, \tag{16}
\]

with \(a^{-1}\) the inverse of \(a \mod m\), which is uniquely defined as \(a^{-1} \equiv a^{m-2} \mod m\), if the LCG has a period of length \(m\). This follows from the Hull-Dobell theorem [14, Thm. 1], which states that \(a\) and \(m\) must be co-prime for an LCG to have full period.

One could also compute the previous value by the wraparound of the periodic sequence. However, this computation has a cost equivalent to \(O(\log m)\) generator steps, making reversal very expensive. Instead, we therefore pre-compute the constant \(a^{-1} \equiv a^{m-2} \mod m\) and reply the recursion (16), which has the same computational cost as (15). As previously mentioned, our reversible PCG implementation requires access to the internal state. As such, our C++ implementation directly inherits from the existing PCG class. Our implementation can be found both together with the code for the experiments in Section 4, and in a pull request to the PCG repository\(^1\).

\(^1\) https://github.com/imneme/pcg-cpp/pull/77
3.3 Sampling distributions in reverse

With our reversible PCG, producing sequences of uniformly distributed 64 bit integers in both forward and reverse mode, we want to generate IEEE-754 double precision values from various distributions. We first consider the uniform distribution $\mathcal{U}([0,1])$. Here, it is important to note that it is not possible to define a bijective mapping between 64 bit integers and floating point values that maintains uniformity. This follows from the non-uniformity of floating-point numbers. Here, we take a pragmatic approach, in which we restrict the integers to 53 bits of information, matching the number of floating-point mantissa-bits (52 physical bits and one implicitly defined), thus discarding 11 bits. Discarding these bits ensures that no rounding occurs in the type conversion, thus maintaining uniformity at the cost of additional quantization. In C++ this transformation is given by

```cpp
class float64{
    static inline double float64(std::uint64_t x) {
        return (x >> 11) * 0x1.0p-53;
    }
}
```

If the resulting quantization would be unacceptable, alternative methods exist that can generate all 64-bit floating point values by using more input bits, see e.g. [7].

Once we can sample the uniform distribution, there are two common approaches to sampling other distributions. These are applying analytical transformations through the inverse cumulative density function and using accept-reject sampling. We now discuss reverse sampling in both of these cases. We use the exponential and normal distributions as examples, while remarking that at least one of these approaches can be applied to any commonly used distribution in scientific computing.

3.3.1 Inverse CDF transformations

For some distributions, a simple analytical expression exists for converting uniform values to samples from the desired distribution. The exponential distribution $\mathcal{E}(R)$, describing the time between events in a Poisson point process with event rate $R$, is one such example. Given the cumulative density function for some $\eta \sim \mathcal{E}(R)$, we set

$$\phi = \text{CDF}_{\mathcal{E}}(\eta) = 1 - e^{-R\eta},$$

and observe that $\phi \sim \mathcal{U}([0,1])$. We then know that the inverse function of the CDF

$$\eta = \text{CDF}^{-1}_{\mathcal{E}}(\phi) = -\frac{\ln(1 - \phi)}{R}$$

transforms a value $\phi \sim \mathcal{U}([0,1])$ to a value $\eta \sim \mathcal{E}(R)$. This approach can be applied to any distribution for which a simple expression for the inverse CDF exists and does not rely on the order in which a sequence of values $\phi$ is generated. It however risks introducing quantization effects in low-probability regions [12, Ch. 4].
3.3.2 Accept-reject sampling

When the inverse CDF is too complex for use as a transformation or quantization in, e.g., the tails, is unacceptable, an alternative is to use an accept-reject algorithm. This means that we sample pseudorandom values from a simpler distribution and selectively discard samples so that the non-discarded samples have the desired distribution. Here, we consider the case of sampling the standard normal distribution $\mathcal{N}(0, 1)$ using the Ziggurat algorithm [19].

The Ziggurat algorithm approximates the Bell curve of the normal PDF by a set of $Z$ rectangles with horizontal span $[-\ell_z, \ell_z]$ and vertical span $(h_z, h_z)$, with $z = 0, \ldots, Z - 1$ and $Z$ a power of 2. These rectangles cover the majority of the curve as sketched in Figure 1a and each have the same area as the intersection of the Bell curve and the band $[0, h_{Z-1}]$. Given a value $\zeta_k$ with 64 random bits, the algorithm uses $\log_2(Z)$ of the bits to select an index $z_k \in [0, Z - 1]$. The remaining bits of $\zeta_k$ are used to generate a random value $\phi_k$, according to one of two cases:

- If $z_k \neq Z - 1$, then $\phi_k \sim \mathcal{U}([\ell_{z_k}, \ell_{z_k+1}])$. If $|\phi_k| < \ell_{z_k}$, $\phi_k$ is accepted. Otherwise, we sample an additional value $\psi_k \sim \mathcal{U}((h_{z_k}, h_{z_k+1}))$. If $\psi_k < \exp(-\phi_k^2/2)$ then $\phi_k$ is accepted, otherwise $\phi_k$ is discarded and the algorithm repeats for a new value $\zeta_{k+1}$. We sketch this step in Figure 1b.

- If $z_k = Z - 1$, $\phi_k \sim \mathcal{U}([-\ell_Z, \ell_Z])$. If $|\phi_k| < \ell_{Z-1}$, then $\phi_k$ is returned. Otherwise, we sample the tails beyond the final rectangle with the Marsaglia method [18], which repeatedly converts pairs of uniform values into a proposed normal value from the tails to be accepted or rejected.
The Ziggurat algorithm, follows the “make the common case fast” principle. For example, an implementation with \( Z = 128 \) accepts the initially proposed \( \phi_k \) in 98.78% of cases and performs even better as the number of rectangles increases [19].

Depending on the value of \( \zeta_k \), the Ziggurat algorithm requires either 0, 1 or \( 1 + 2i, i \in \mathbb{N} \), uniform values before sampling a next value \( \zeta_{k+1} \). If all uniform values are drawn from the same sequence, then it is not possible to determine which elements of the sequence correspond with values \( \zeta_k \). We therefore take the approach of only generating the values \( \zeta_k \) from our reversible PCG implementation. If more uniform values are needed to generate a proposal, we then use \( \zeta_k \) to seed a second pseudorandom number generator from which we get these additional values.

In the most common case, i.e., \( z_k \neq Z - 1 \) and \( |\phi_k| < \xi z_k \), no other random values are needed and the performance of our reversible implementation remains unchanged. In other cases, this seeding induces a small amount of extra overhead on top of the Ziggurat algorithm. We deem this small overhead acceptable in the small percentage of cases where such additional values are necessary. To avoid inducing correlations between these additional uniform values and future values of the \( \zeta \) sequence, we refrain from using a PCG to generate these additional values. Instead we use the xoshiro256+ generator [1] for this purpose.

This second generator “trick” makes our accept-reject strategy more general than that proposed in [30], but introduces a potentially biased values. This bias is caused by repeated seeding of the second generator, with fewer possible seed values than can be represented in the generator state. Following the design of the C++ standard library, we separate bit generation from distribution sampling, meaning that we cannot access the PCG’s internal state but only the 64 output bits. Inside xoshiro256+, SplitMix [27] is used to populate its 256 bit state from a 64 bit seed. Additionally, we only use seed values where \( z_k = Z - 1 \) or \( |\phi_k| \geq \xi z_k \). As a consequence, the second generator cannot reach all possible states. Despite these considerations, the values produced don’t consistently fail any tests in TestU01 BigCrush after conversion to uniform values using a CDF transformation. A number of our runs can be found together with our code referenced in Section 4.

Though we only consider the Ziggurat algorithm here, our seeding approach works for any accept-reject algorithm with uncorrelated proposals. Rather than seeding a second generator, one an equally general bias-free approach would be to use a splittable generator such as SplitMix [27] or using multiple streams of same generator. These approaches come at the cost of software modularity. One can also reverse an arbitrary accept-reject algorithm without bias and without breaking modularity by using multiple reversible generators. At most, one needs a generator for each random variable occurring in a branch-condition affecting the number of random variables needed to generate a proposal. The Ziggurat algorithm can, e.g., be reversed with two reversible generators, one providing values \( \zeta_k \) and another providing the values \( \psi_k \) and the pairs used in the Marsaglia algorithm, as the required access pattern of the values from the second sequence is known once \( \zeta_k \) is determined.
4 Simulation results

We now demonstrate the efficacy of our reversible generator approach. First, in Section 4.1, we consider the performance of the reversible generator. Next, in Section 4.2 we consider the problem from Section 2.1. The code for producing our results is available at gitlab.kuleuven.be/numa/public/mcqmc_2022_rrng, together with a Docker configuration with the software dependencies. All timings were produced in a Podman container on a 2021 M1 MacBook Pro with 16GB of RAM.

4.1 Generator efficiency

To test the efficiency of our reversed generator we time how long our C++ implementation needs to generate \( K \) random values in both forward and reverse mode for different seeds, with \( K \) varying between \( 10^3 \) and \( 10^8 \). To produce reliable timings, we perform 55 timings for each \( K \), discarding the first 5 timings and reporting the minimum of the remaining 50. The resulting timings for \(-O3\) are shown in Figure 2.

In Figure 2a, we see that our reverse-mode extension of PCG attains the same performance as the (unaltered) forward implementation. We have thus reversed the uniform generator, at the same computational cost as the forward generation. In addition, Figures 2b and 2c show that both forward and reverse modes for our non-uniform generators attain the same performance. While the cost of sampling the exponential distribution is practically the same as sampling the uniform distribution, sampling the normal distribution values is approximately twice as expensive.

4.2 Cooling a 1D heat equation

We now consider the simulating the 1D heat equation problem from Section 2.1. The periodic domain allows us to focus on reversing the path dynamics themselves, without the additional complexities induced by more complex boundary conditions. As an initial condition, we set \( y(x, 0) = 50 \sin(8\pi x/L) + 90 \) and set the regularization parameter \( \nu = 1 \), the domain length \( L = 10 \) and end time \( T = 1 \). We set the spatial grid size to \( \Delta x = 0.01 \) and the time step size to \( \Delta t = 0.001 \). We show the initial and final conditions, as well as the optimal computed \( \hat{u}(x) \) after convergence in Figure 3.

We now compare a classic implementation of this problem, storing paths in memory, to one where we re-compute the paths in the adjoint simulation using a reversible generator. We compare both approaches for varying batch-sizes, i.e., the number of particles simulated simultaneously, in terms of computational cost and memory usage. In Figure 4a, we see that both implementations perform comparably for smaller batch-sizes. However, once the memory requirements of the algorithm approaches the available 16GB of RAM on the computer, the runtime of the classic implementation increases sharply, while the cost of the reversible implementation continues...
Fig. 2 Comparing forward and reverse mode timings for different random distributions. We see that both modes attain the same performance for all three considered distributions.

Fig. 3 The temperature profile and optimal cooling rate for the 1D heat equation problem.
to grow at an unchanged rate. At this point in the plot, the classic implementation starts writing to disk, causing severe slowdowns in the computation.

While one can avoid this catastrophic blow-up in computational cost through check-pointing, we avoid implementing and fine-tuning a check-pointing code here, as we know that it by definition has a computational cost higher than that of the reversible implementation due to the required recomputation. We however assume that a lower bound for the cost of a checkpointed implementation is given by two reversible constraint simulations and a non-reversible adjoint simulation.

5 Conclusions

We presented a reversible extension to PCG pseudorandom number generators. We also presented strategies for reversing arbitrary distributions using either transformation and accept-reject approaches. We demonstrated that this reversible approach allows us to generate a given sequence of values with the same computational cost both forward from the initial generator state and backwards from the final state.

We then applied this reversible generation to the setting of discrete adjoint-based PDE-constrained optimization with Monte Carlo. We demonstrated on a test problem involving the 1D heat equation that our reversible approach avoids the high memory costs of storing the paths of the constraint equation, while still allowing for a simple implementation of the adjoint solver. We therefore present this approach as an alternative to more complex and more expensive ad-hoc checkpointing approaches.

Although path-reversal is conceptually straightforward, we foresee certain cases were non-injective operations may present challenges in more complex simulations.
Fig. 5 Demonstration of the challenge of reflective boundaries. Both particles $X_p$ and $X_p'$ have the same position at time $\tau + 1$ after moving the same distance to the right, even though they have different positions at time $\tau$.

One such example is reflective boundaries, where, as demonstrated by Figure 5, there are two locations from which a particle can reach a given end-position given a known positional increment. Such issues are often down to implementation, rather than fundamental. The given example can, e.g., be avoided by the introduction of a reflection vector as an additional particle state, which is updated on each reflection. In 1D, this reflection vector based solution, can be interpreted as a simulation on a domain of length $2L$ with periodic boundaries.

In future work, we plan to apply this reversible approach to more complex and higher-dimensional PDEs, where Monte Carlo methods are highly attractive. An example is fusion reactor design with kinetic equations as a constraint [8].

Acknowledgements This paper is based on the master’s theses [2, 17, 28]. We thank the anonymous reviewer for their detailed comments on our discussion of random number generation and Mike Giles for pointing out a mathematical error in the first version of this paper. We thank Michael Mascagni for his input on suitability of different random number generators for this work. We also thank Ignace Bossuyt, Vince Maes and Zhirui Tang for providing feedback on our experiments’ reproducibility. During this work, Emil Løvbak and Andreas Van Barel were funded by the Research Foundation - Flanders (FWO) under, respectively, fellowship numbers 1SB1919N/1SB1921N and 11E1518N. This work has been carried out within the framework of the EUROfusion Consortium, funded by the European Union via the Euratom Research and Training Programme (Grant Agreement No 101052200 — EUROfusion). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for them.

References

1. Blackman, D., Vigna, S.: Scrambled Linear Pseudorandom Number Generators. ACM Transactions on Mathematical Software 47(4), 1–32 (2021)
2. Blondeel, F.: Monte Carlo Adjoint Computation for PDE-Constrained Optimization using Reversible Random Number Generators. Master’s thesis, KU Leuven, Leuven (2022)
3. Bottou, L., Curtis, F.E., Nocedal, J.: Optimization Methods for Large-Scale Machine Learning. SIAM Review 60(2), 223–311 (2018)
4. Bouillaguet, C., Martinez, F., Sauvage, J.: Practical seed-recovery for the PCG Pseudo-Random Number Generator. IACR Transactions on Symmetric Cryptology 2020(3), 175–196 (2020)
5. Brown, F.B.: Random Number Generation with Arbitrary Strides. Transactions of the American Nuclear Society 71, 202–203 (1994)
6. Caflisch, R., Silantyev, D., Yang, Y.: Adjoint DSMC for nonlinear Boltzmann equation constrained optimization. Journal of Computational Physics 439, 110404 (2021)
7. Campbell, T.R.: Uniform random floats: How to generate a double-precision floating-point number in [0, 1] uniformly at random given a uniform random source of bits. nugle.net/~campbell/2014/04/28/uniform-random-float (2014)
8. Dekeyser, W., Blommaert, M., Ghoo, K., Horsten, N., Boerner, P., Samaey, G., Baelmans, M.: Divertor design through adjoint approaches and efficient code simulation strategies. Contributions to Plasma Physics 58(6-8), 643–651 (2018)
9. Gentle, J.E.: Random Number Generation and Monte Carlo Methods. Springer Science & Business Media, New York (2003)
10. Giles, M.B., Pierce, N.A.: An Introduction to the Adjoint Approach to Design. Flow, Turbulence and Combustion 65, 393–415 (2000)
11. Naumann, U., du Toit, J.: Adjoint algorithmic differentiation tools support for typical numerical patterns in computational finance. Journal of Computational Finance 21(4), 23–57 (2018)
12. O’Neill, M.E.: PCG: A Family of Simple Fast Space-Efficient Statistically Good Algorithms for Random Number Generation. Tech. Rep. HMC-CS-2014-0905, Harvey Mudd College, Claremont, CA (2014)
13. O’Neill, M.E.: On Vigna’s PCG Critique. pcg-random.org/posts/on-vigna’s-pcg-critique.html (2018)
14. Reiter, D., Baelmans, M., Börner, P.: The EIRENE and B2-EIRENE Codes. Fusion Science and Technology 47(2), 172–186 (2005)
15. Salmon, J.K., Moraes, M.A., Dror, R.O., Shaw, D.E.: Parallel random numbers: As easy as 1, 2, 3. In: SC ’11: Proceedings of 2011 International Conference for High Performance Computing, Networking, Storage and Analysis, p. 12 (2011)
16. Steele, G.L., Lea, D., Flood, C.H.: Fast splittable pseudorandom number generators. In: Proceedings of the 2014 ACM International Conference on Object Oriented Programming Systems Languages & Applications, pp. 453–472. ACM, Portland Oregon USA (2014)
17. Vigna, S.: The wrap-up on PCG generators. pcg.di.unimi.it/pcg (2018)
18. Yoginath, S.B., Perumalla, K.S.: Efficient reversible uniform and non-uniform random number generation in UNU.RAN. In: Proceedings of the Annual Simulation Symposium, ANSS ‘18, pp. 1–10. Society for Computer Simulation International, San Diego, California (2018)