A Quantum Parallel Markov Chain Monte Carlo

Andrew J. Holbrook
UCLA Biostatistics, Los Angeles, CA

ABSTRACT
We propose a novel hybrid quantum computing strategy for parallel MCMC algorithms that generate multiple proposals at each step. This strategy makes the rate-limiting step within parallel MCMC amenable to quantum parallelization by using the Gumbel-max trick to turn the generalized accept-reject step into a discrete optimization problem. When combined with new insights from the parallel MCMC literature, such an approach allows us to embed target density evaluations within a well-known extension of Grover’s quantum search algorithm. Letting \( P \) denote the number of proposals in a single MCMC iteration, the combined strategy reduces the number of target evaluations required from \( O(P) \) to \( O(\sqrt{P}) \). In the following, we review the rudiments of quantum computing, quantum search and the Gumbel-max trick in order to elucidate their combination for as wide a readership as possible.

1. Introduction
Parallel MCMC techniques use multiple proposals to obtain efficiency gains over MCMC algorithms such as Metropolis-Hastings (Metropolis et al. 1953; Hastings 1970) and its progeny that use only a single proposal. Neal (2003) first develops efficient MCMC transitions for inferring the states of hidden Markov models by proposing a “pool” of candidate states and using dynamic programming to select among them. Next, Tjelmeland (2004) considers inference in the general setting and shows how to maintain detailed balance for an arbitrary number \( P \) of proposals. Consider a probability distribution \( \pi(d\theta) \) defined on \( \mathbb{R}^D \) that admits a probability density \( \pi(\theta) \) with respect to the Lebesgue measure, that is, \( \pi(d\theta) := \pi(\theta)d\theta \). To generate samples from the target distribution \( \pi \), we craft a kernel \( P(\theta_0, d\theta) \) that satisfies

\[
\pi(A) = \int \pi(d\theta_0)P(\theta_0, A) \tag{1}
\]

for all \( A \subset \mathbb{R}^D \). Letting \( \theta_0 \) denote the current state of the Markov chain, Tjelmeland (2004) proposes sampling from such a kernel \( P(\theta_0, \cdot) \) by drawing \( P \) proposals \( \Theta_{-0} = (\theta_1, \ldots, \theta_P) \) from a joint distribution \( Q(\theta_0, d\Theta_{-0}) := q(\theta_0, \Theta_{-0})d\Theta_{-0} \) and selecting the next Markov chain state from among the current and proposed states with probabilities

\[
\pi_p = \frac{\pi(\theta_p)q(\theta_p, \Theta_{-p})}{\sum_{p' = 0}^P \pi(\theta_{p'})q(\theta_{p'}, \Theta_{-p'})}, \quad p = 0, \ldots, P. \tag{2}
\]

Here, if \( \Theta = (\theta_0, \ldots, \theta_P) \) is the \( D \times (P+1) \) matrix having the current state and all \( P \) proposals as columns, then \( \Theta_{-p} \) is the \( D \times P \) matrix obtained by removing the \( p \)th column. Tjelmeland (2004) shows that the kernel \( P(\theta_0, \cdot) \) constructed in such a manner maintains detailed balance and hence satisfies (1). Others have since built on this work, developing parallel MCMC methods that generate or recycle multiple proposals (Frenkel 2004; Delmas and Jourdain 2009; Calderhead 2014; Yang et al. 2018; Luo and Tjelmeland 2019; Schwedes and Calderhead 2021; Holbrook 2021). Most recently, Glatt-Holtz et al. (2022) place all these developments in their natural measure theoretical context, allowing one to trivially apply (1) and (2) to distributions over discrete-valued random variables.

Taken together, these developments demonstrate the ability of parallel MCMC methods to alleviate inferential challenges such as multimodality and to deliver performance gains over single-proposal competitors as measured by reduced autocorrelation between samples. In the following, we focus on the specification presented in Algorithm 1 but note that the techniques we present may also be effective for generalizations of this basic algorithm.

One need not use parallel computing to implement Algorithm 1, but the real promise and power of parallel MCMC comes from its natural parallelizability (Calderhead 2014). Contemporary hardware design emphasizes architectures that enable execution of multiple mathematical operations simultaneously. Parallel MCMC techniques stand to leverage technological developments that keep modern computation on track with Moore’s Law, which predicts that processing power doubles every two years. For example, the algorithm of Tjelmeland (2004) generates \( P \) conditionally independent proposals and then evaluates the probabilities of (2). One may parallelize the proposal generation step using parallel pseudorandom number generators (PRNG) such as those advanced in Salmon et al. (2011). The computational complexity of the target evaluations \( \pi(\theta_p) \) is linear in the number of proposals. This presents a significant burden when \( \pi(\cdot) \) is
computationally expensive, for example, in big data settings or for Bayesian inversion, but evaluation of the target density over the $P$ proposals is again a naturally parallelizable task. Moreover, widely available machine learning software such as TensorFlow allows users to easily parallelize both random number generation and target evaluations on general purpose graphics processing units (GPU) (Lao et al. 2020). Finally, when generating independent proposals using a proposal distribution of the form $q(\theta_0, \Theta_{-0}) = \prod_{p=1}^{P} q(\theta_0, \theta_p)$, the acceptance probabilities (2) require the $O(P^2)$ evaluation of the $P+1$ terms $q(\theta_p, \theta_p)$, but Holbrook et al. (2021a, 2021b) demonstrate the natural parallelizability of such pairwise operations, obtaining orders-of-magnitude speedups with contemporary GPUs. The proposed method directly addresses the acceptance step of Algorithm 1, while leaving the choice of parallelizing (or not parallelizing) the proposal step to the practitioner.

While parallel MCMC algorithms are increasingly well-suited for developing many-core computational architectures, there are trade-offs that need to be taken into account when choosing how to allocate computational resources. On one end of the spectrum, Gelman and Rubin (1992a, 1992b) demonstrate the usefulness of generating, combining and comparing multiple independent Markov chains that target the same distribution, and one may perform this embarrassingly parallel task by assigning the operations for each individual chain to a separate central processing unit (CPU) core or GPU work-group. In this multi-chain context, simultaneously running multiple parallel MCMC chains could limit resources available for the within-chain parallelization described in the previous paragraph. On the other end of the spectrum, one may find it useful to allocate resources to overcome computational bottlenecks within a single Markov chain that uses a traditional accept-reject step. In big data contexts, Holbrook et al. (2021a, 2021b) and Holbrook, Ji, and Suchard (2022a, 2022b) use multi- and many-core processing to accelerate log-likelihood and log-likelihood gradient calculations within single Metropolis-Hastings and Hamiltonian Monte Carlo (Neal 2011) generated chains. This big data strategy might again limit resources available for parallelization across proposals and target evaluations described above.

In the presence of these tradeoffs, it is worthwhile to develop additional parallel computing tools for parallel MCMC so that future scientists may be better able to flexibly assign sub-routines to different computing resources in a way that is tailored to their specific inference task. In particular, we show that quantum parallelization can be a useful tool for parallel MCMC when evaluation of the target density represents the computational bottleneck.

Quantum computers use quantum mechanics to store information and manipulate data. By leveraging the idiosyncracies of quantum physics, these computers are able to deliver speedups over conventional computing for a relatively small number of computational problems. Some of these speedups are very large. Quantum computers can achieve exponential speedups over conventional computers for some computational tasks. Shor’s quantum algorithm for factoring an integer $N$ (Shor 1994) is polynomial in $\log N$ compared to a super-polynomial classical optimum. The HHL algorithm for solving sparse $N$-dimensional linear systems (Harrow, Hassidim, and Lloyd 2009) is $O(\log N)$ compared to a classical $O(N)$. Other algorithms deliver a still impressive polynomial speedup. For example, the algorithms considered in the following (Section 2.2) achieve quadratic speedups over conventional computing, turning $O(N)$ runtimes into $O(\sqrt{N})$. Both the magnitude of quantum computing’s successes and the relative rarity of those successes mean that there is a general interest in leveraging quantum algorithms for previously unconsidered computational problems. We will show that—with the help of the Gumbel-max trick (Section B)—established quantum optimization techniques are actually useful for sampling from computationally expensive discrete distributions and apply this insight to achieving quadratic speedups for parallel MCMC.

We provide a short introduction to the most basic elements of quantum computing in Appendix A. The interested reader may look to Nielsen and Chuang (2010) for a canonical introduction to quantum algorithms or Lopatnikova and Tran (2021), Wang and Liu (2022) for surveys geared toward statisticians. In Section 2.1, we review and compare three different quantum search algorithms that enjoy quadratic speedups over conventional algorithms. In Section 2.2 we review the quantum minimization algorithm of Durr and Hoyer (1996) and investigate the use of warm-starting therein. We then combine the Gumbel-max trick (Section B) and recent insights in parallel MCMC with the quantum minimization algorithm to create the quantum parallel MCMC algorithm for both continuously-valued (Section 3.2) and discrete-valued (Section 3.3) targets.

## 2. Quantum Search and Quantum Minimization

Grover (1996) demonstrates how use a quantum computer to find a single marked element within a finite set of $N$ items with only $O(\sqrt{N})$ queries, and a result from Bennett et al. (1997) shows that Grover’s algorithm is optimal up to a multiplicative constant. Boyer et al. (1998) extend Grover’s algorithm to multiple marked items or solutions, further extend it to the case when the number of solutions is unknown and provide a rigorous bounds on the algorithms’ error rates. Finally, Durr and Hoyer (1996) use the results of Boyer et al. (1998) to obtain the minimum value within a discrete ordered set. Here, we briefly
Algorithm 2 Quantum search algorithm (Grover 1996)

Data: An oracle \( U_f \) taking \( |x\rangle |y\rangle \rightarrow |x\rangle |y \oplus f(x)\) for a function \( f(x) : \{0, \ldots, N-1\} \rightarrow \{0, 1\} \) that satisfies \( f(x_0) = 1 \) for a single \( x_0 \); \( n + 1 = \log_2(N) + 1 \) quantum states initialized to \( |0\rangle \otimes |1\rangle \); an integer \( R = \left\lfloor \pi \sqrt{N}/4 \right\rfloor \) denoting the number of Grover iterations.

Result: An \( n \)-bit binary string \( x_0 \) satisfying \( f(x_0) = 1 \) with error less than \( 1/N \).

\[ |0\rangle \otimes |1\rangle \rightarrow H^{\otimes n+1} |0\rangle \otimes |1\rangle = |h\rangle |–\rangle; \quad /* |h\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle . \]

\[ |h\rangle |–\rangle \rightarrow \mathcal{G}^R |h\rangle |–\rangle \approx |x_0\rangle |–\rangle; \quad /* \mathcal{G} = \left( 2 |h\rangle \langle h| - I \right) \left( 1 - 2 |x_0\rangle \langle x_0| \right) \]

\[ |x_0\rangle \rightarrow x_0; \text{ return } x_0. \]

review these advances and provide illustrative simulations. In Section B, the Gumbel-max trick allows us to extend these results to the problem of sampling from a discrete distribution.

2.1. Quantum Search

Given a set of \( N \) items and a function \( f : \{0, 1, \ldots, N-1\} \rightarrow \{0, 1\} \) that evaluates to 1 for a single element, Grover (1996) develops an algorithm that uses quantum parallelism to score quadratic speedups over its classical counterparts. After only \( \mathcal{O}(\sqrt{N}) \) evaluations of \( f(\cdot) \), Grover’s algorithm returns the \( x \in \{0, 1, \ldots, N-1\} \) satisfying \( f(x) = 1 \) with high probability. Compare this to \( \mathcal{O}(N) \) requirement for the randomized classical algorithm that must evaluate \( f(\cdot) \) over at least \( N/2 \) items to obtain the same probability of detecting \( x \). The algorithm takes the state \( |0\rangle \otimes |1\rangle \) as input and applies Hadamard gates to each of the individual \( N+1 \) input qubits. The resulting state is

\[ |h\rangle |–\rangle = \left( \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \right) \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |–\rangle . \]

Next, we apply the oracle gate \( U_f : |x\rangle |y\rangle \rightarrow |x\rangle |y \oplus f(x)\) and note that

\[ U_f |x\rangle |–\rangle = U_f |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)
\]
\[ = \frac{1}{\sqrt{2}} \left( |x\rangle |0 \oplus f(x)\rangle - |x\rangle |1 \oplus f(x)\rangle \right)
\]
\[ = -I f(x) |–\rangle . \]

Thus, \( U_f \) flips the sign for the state \( |x_0\rangle \) for which \( f(x_0) = 1 \) but leaves the other states unchanged. If we suppress the ancillary qubit \( |–\rangle \), then \( U_f \) is equivalent to the gate \( U_{x_0} \) defined as \( U_{x_0} |x\rangle = -I^{x_0} |x\rangle \). We may succinctly write this gate as the Householder matrix that reflects vectors about the unique hyperplane through the origin that has \( |x_0\rangle \) for a normal vector:

\[ U_{x_0} = I - 2 |x_0\rangle \langle x_0| . \]

The action of this gate on the state \( |h\rangle \) takes the form

\[ \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} -I^{x_0(x)} |x\rangle . \]

Next, the algorithm reflects the current state about the hyperplane that has \( |h\rangle \) as a normal vector and negates the resulting state:

\[ \left( 2 |h\rangle \langle h| - I \right) \left( 1 - 2 |x_0\rangle \langle x_0| \right) \]
\[ = \frac{1}{\sqrt{N}} \sum_{x} \left( (-1)^{1 - \delta_{x_0(x)}} + \frac{2(N-2)}{N} \right) |x\rangle \]
\[ = \frac{(3N-4)}{N^{3/2}} |x_0\rangle + \sum_{x \neq x_0} \frac{(N-4)}{N^{3/2}} |x\rangle . \]

The scientist who measures the state at this moment would obtain the desired state \( |x_0\rangle \) with a slightly higher probability of \( (3N-4)^2/N^3 \) than the individual probabilities of \( (N-4)^2/N^3 \) for the other states. Each additional application of the Grover iteration

\[ \mathcal{G} := -U_h U_{x_0} := \left( 2 |h\rangle \langle h| - I \right) \left( 1 - 2 |x_0\rangle \langle x_0| \right) \]

increases the probability of obtaining \( |x_0\rangle \) at the time of measurement in the computational basis and \( R = \left\lfloor \pi \sqrt{N}/4 \right\rfloor \) iterations guarantees a probability of success that is greater than \( 1 - 1/N \).

In general, we may use Grover’s search algorithm to find a solution when the number of solutions \( M \) is greater than 1. While the algorithmic details change little, the number of required Grover iterations

\[ R = \left\lfloor \frac{\pi}{4} \sqrt{\frac{N}{M}} \right\rfloor \]

and the probability of success after those \( R \) iterations do change (Boyer et al. 1998). When \( M \) is much smaller than \( N \), the success rate is greater than \( 1 - M/N \), and even for large \( M \) the success rate is more than 1/2. Lower-bounds are useful for establishing mathematical guarantees, but it is also helpful to understand the quality of algorithmic performance as a function of \( M \) and \( R \). Figure 1 shows success curves as a function of the number of Grover iterations (or oracle calls) applied. The search field contains \( 2^{14} \approx 16k \) elements, and the number of solutions \( M \) varies. Each curve represents an individual search task. The algorithm requires more iterations for smaller numbers and fewer iterations for larger numbers of solutions. The upper bound on error \( M/N \) is only an upper bound: the final probability of success for, for example, \( M = 256 \) is 0.997 compared to the bound of 0.984.

While Grover’s algorithm delivers impressive speedups over classical search algorithms, it has a major weakness. Figure 1 hides the fact that the probability of success for Grover’s algorithm is not monatonic in the number of iterations. Running the
algorithm for more than \( R \) iterations can backfire. For example, running the algorithm for \( \sqrt{2N} \) iterations when \( M = 1 \) results in a probability of success less than 0.095 (Boyer et al. 1998). The non-monotonicity of Grover’s algorithm becomes particularly problematic when we do not know the number of solutions \( M \). Taking for example \( N = 2^{20} \), Boyer et al. (1998) point out that 804 iterations provide an extremely high probability of success when \( M = 1 \) but a one-in-a-million chance of success when \( M = 4 \). To solve this problem and develop an effective search algorithm when \( M \) is unknown, those authors adopt the strategy of focusing on the expected number of iterations before success. In particular, they propose the quantum exponential search algorithm (Algorithm 3). When a solution exists, the algorithm returns a solution with expected total number of Grover iterations bounded above by \( \frac{9}{4} \sqrt{N/M} \). Still better, this upper bound reduces to \( \frac{9}{4} \sqrt{N/lM} \) for the special case \( M \ll N \), and simulations presented in Figure 2 show that even this bound is large. Such results come in handy when deciding whether to halt the algorithm’s progress if one believes it possible that no solutions exist. Indeed, this turns out to be useful in the context of quantum minimization (Section 2.2).

**Algorithm 3** is not the only quantum search algorithm that is useful when the number of solutions \( M \) is unknown. Yoder, Low, and Chuang (2014) use generalized Grover iterations that extend (3) to include general phases \((\alpha_j, \beta_j)\):

\[
G(\alpha_j, \beta_j) := -U_h(\alpha_j)U_{x_0}(\beta_j) = \left( 1 - e^{-i\alpha_j} \right) |h\rangle \langle h| - I \left( 1 - e^{i\beta_j} \right) |x_0\rangle \langle x_0|.
\]

This form reduces to the original Grover iteration (3) when \( \alpha = \pm \pi \) and \( \beta = \pm \pi \). To select general phases, the method first fixes an error tolerance \( \delta^2 > 0 \) and a lower bound \( \omega \leq \lambda = M/N \) and then selects an odd upper bound \( L \) on the total number of oracle queries \((L - 1)\) such that

\[
L \geq \frac{\log(2/\delta)}{\sqrt{\omega}}.
\]

Finally, letting \( l = (L - 1)/2 \), one obtains phases \((\alpha_j, \beta_j)\) for \( j = 1, \ldots, l \) that satisfy

\[
\alpha_j = -\beta_{j+1} = 2 \cot^{-1} \left( \frac{\tan(2\pi j/L)}{\sqrt{1 - \gamma^2}} \right),
\]
A. J. HOLBROOK

Minimization with warm-starting (Section 2.2). M underperforms partially due to a miniscule lower bound solutions M for γ (Figure 3).

Algorithm 3 Quantum exponential searching algorithm (Boyer et al. 1998)

Data: An oracle gate Uf taking |x⟩|y⟩ to |x⟩|y ⊕ f(x)⟩ for a function f(x) : {0, . . . , N − 1} → {0, 1} with unknown number of solutions; n = log2(N).

Result: If a solution exists, an n-bit binary string x0 satisfying f(x0) = 1; if no solution exists, the algorithm runs forever.

m ← 1; γ ← 6/5; success ← FALSE; while success ≠ TRUE do

j ← Uniform[0, . . . , m − 1]; |0⟩⊗n |1⟩ → H⊗n+1 |0⟩⊗n |1⟩ = |h⟩|−⟩; |h⟩|−⟩ → Gj|h⟩|−⟩ = |x⟩|−⟩; /* j Grover iterations from Algorithm 2. */

|x⟩ → x; /* Measure and check. */

if f(x) = 1 then

x0 ← x; success ← TRUE;

else

m ← min(γm, √N); /* Increase m in case of failure. */

end

end

return x0.

Figure 3. Total number of oracle evaluations required by fixed-point quantum search (FPQS) (Yoder, Low, and Chuang 2014) minus total required for quantum exponential searching algorithm (QESA) (Algorithm 3) for different numbers of solutions M and search set sizes N from 500 independent simulations each. FPQS underperforms partially due to a miniscule lower bound w = 1/N on λ = M/N; a tuning decision motivated by the potential application within quantum minimization with warm-starting (Section 2.2).

for γ−1 = cos(1 2 cos−1(1 2 )) is the reciprocal of the inverse Lth Chebyshev polynomial of the first kind. Such phases mark the only algorithmic difference between the fixed-point quantum search and the original Grover search (Algorithm 2). The upshot is a search procedure that obtains a guaranteed probability of success 1 − δ2 for any M such that there exists an M0 < M that also obtains the same success threshold (Figure 2). On the one hand, this algorithm avoids the exponential quantum search algorithm's need to perform multiple measurements of the quantum state. On the other hand, the exponential quantum search algorithm requires significantly fewer oracle evaluations when M is small (Figure 3), and it turns out that this is precisely the scenario that interests us.

2.2. Quantum Minimization

Given a function f(·) that maps the discrete set {0, . . . , N − 1} to the integers, we wish to find the minimizer

x0 = arg minx∈{0,...,N−1}f(x).

Durr and Hoyer (1996) propose a quantum algorithm for finding x0 that iterates between updating a running minimum F ∈ f({0, . . . , N − 1}) and applying the quantum exponential search algorithm (Algorithm 3) to find an element x such that f(x) < F. Having run these iterations a set number of times, the algorithm returns the minimizer x0 with high probability. To this end, Durr and Hoyer (1996) show that their algorithm takes an expected total time less than or equal to m0 := 7 log2(N) to find the minimizer, where marking items with values less than the threshold value (Algorithm 4) requires log2(N) time steps and each Grover iteration within the quantum exponential search algorithm requires one time step. From there, Markov’s inequality says

Pr \left( \text{total time to success} \geq \frac{m_0}{\epsilon} \right) \leq \frac{E \left( \text{total time to success} \right)}{m_0/\epsilon} \leq \epsilon,

or that we must scale the minimization procedure’s time steps by a factor of 1/ε to reach a failure rate less than ε. Due to the iterative nature of the algorithm, one might suppose that it is beneficial to start at a value x0 for which f(x0) is lower relative to other values. This turns out to be the case in theory and in practice, and the benefit of warm-starting is particularly useful in the context of parallel MCMC.

Proposition 1 (Warm-starting). Suppose that the quantum minimization algorithm begins with a threshold F0 such that f(x) < F0 for only K − 1 > 0 items. Then the expected total number of time steps to find the minimizer is bounded above by

m0K = \left( \frac{5}{4} - \frac{1}{\sqrt{K - 1}} \right) 9\sqrt{N} + \frac{7}{10} \log_2(K) \log_2(N),

and so the following rule relates the warm-started upper bound to the generic upper bound:

m0K = m0 - 9\sqrt{\frac{N}{K - 1}} + \frac{7}{10} \log_2 \left( \frac{K}{N} \right) \log_2(N).

Proof. The proof follows the exact same form as Lemma 2 of Durr and Hoyer (1996). It relies on a theoretical algorithm called the infinite algorithm that runs until the minimum is found. In this case, Lemma 1 of that paper says that the probability that the rth lowest value is ever selected when searching among K items
Algorithm 4 Quantum sub-routine searching algorithm (Durr and Hoyer 1996)

**Data:** A quantum sub-routine capable of evaluating a function \( f(\cdot) \) over \([0, \ldots, N-1]\) with with unique integer values; a maximum error tolerance \( \epsilon \in (0, 1) \); expected total time to success \( m_0 = \frac{45}{4} \sqrt{N} + \frac{7}{10} \log_2(N) \).

**Result:** A \( \log_2(N) \)-bit binary string \( x_0 \) satisfying \( f(x_0) = \min f \) with probability greater than \( 1 - \epsilon \).

```pseudocode
\begin{align*}
  &\text{Prepare initial state } \frac{1}{\sqrt{N}} \sum_x |x \rangle |x_0 \rangle; \text{ Mark all items } x \text{ satisfying } f(x) < f(x_0); \ s \leftarrow \log_2(N); \text{ Apply quantum exponential searching algorithm (Algorithm 3); } / \ast 1 \text{ time steps} \\
  &\text{for } s < m_0/\epsilon \text{ do} \\
  &\quad \text{ if } f(x') < f(x_0) \text{ then} \\
  &\quad \quad x_0 \leftarrow x' \text{; Obtain } x' \text{ by measuring first register; } \text{if } f(x') < f(x_0) \text{ then} \\
  &\text{end} \\
  &\text{return } x_0.
\end{align*}
```

An upper bound for the expected total number of time steps preparing the initial state and marking items \( f(x) < f(x_0) \) follows in a similar manner.

Proposition 1 shows that, for example, if Algorithm 4 begins at the item with second lowest value, then the expected total time to success is bounded above by \( m_0^2 = \frac{45}{4} \sqrt{N} + \frac{7}{10} \log_2(N) \), reducing the generic upper bound by \( 9 \sqrt{N} - \frac{7}{10} \log_2 \left( \frac{2}{N} \right) \log_2(N) \) time steps. When \( N \) equals 1000, say, the expected total time steps is \( m_0^2 < 78.2 \). Keeping \( N = 1000 \) but letting the algorithm begin at the third lowest value \( (K = 3) \), the expected total time steps before success is \( m_0^3 < 165.6 \). Raising \( N \) to 10,000, the two numbers increase to \( m_0^2 < 234.4 \) and \( m_0^3 < 503.4 \).

In practice, the number of time steps before finding the minimum is surprisingly small. Figure 4 corroborates the intuition that it is beneficial to start at a lower ranked element. To generate these results, we use an early stopping rule for the quantum minimization algorithm’s exponential search sub-routine, halting it after \( \frac{9}{4} \sqrt{N} \) iterations. Even with this stopping rule in place, the error rate of the quantum minimization algorithm is less than 1%. We can increase the early stopping threshold to obtain even lower error rates, but this strategy would seem to be unnecessary in the context of parallel MCMC. The benefits of warm-starting are useful in the same context, when the current state \( \theta^{(s)} \) usually inhabits the high-density region of the target distribution but the majority of proposals do not.

### 3. Quantum Parallel MCMC

With the rudiments of quantum minimization in hand, we present a quantum parallel MCMC (QPMCMC). The general structure of the algorithm the same as Algorithm 1: it constructs a Markov chain by iterating between generating many proposals and randomly selecting new Markov chain states among these proposals. Unlike classical single-proposal MCMC, parallel MCMC proposes many states and chooses one according to the generalized acceptance probabilities of (2). In general MCMC, evaluation of the target density function \( \pi(\cdot) \) is the rate-limiting computational step, becoming particularly onerous in big data scenarios (Holbrook et al. 2021a). While parallel MCMC benefits from improved mixing as a function of MCMC iterations, the increased computational burden of \( P \) target evaluations at each step can lead to less favorable comparisons when accounting for elapsed wall-clock time.

Having successfully generated proposals \( \theta_p, p = 1, \ldots, P \) and evaluated the corresponding proposal densities \( q(\cdot, \cdot) \), we would like to use quantum parallelism and an appropriate oracle gate to efficiently compute the \( \pi(\theta_p) \) but immediately encounter a Catch–22 when we seek to draw a sample \( \theta^{(s+1)} \sim \text{Discrete}(\pi) \) for the vector of probabilities \( \pi(\cdot) \) is the rate-limiting computational step, becoming particularly onerous in big data scenarios (Holbrook et al. 2021a). While parallel MCMC benefits from improved mixing as a function of MCMC iterations, the increased computational burden of \( P \) target evaluations at each step can lead to less favorable comparisons when accounting for elapsed wall-clock time.

In light of this dilemma, we propose to use the Gumbel-max trick (Papandreou and Yuille 2011) to transform the generalized accept-reject step into a discrete optimization procedure (Section B). From there, we use quantum minimization to efficiently sample from \( \text{Discrete}(\pi) \). Crucially, we get away with quantum parallel evaluation of the target \( \pi(\cdot) \) over all superposed states because the Gumbel-max trick does not rely on a normalization step: each superposed state requires no knowledge of any target evaluation other than its own.

Once one has effectively parallelized the target evaluations \( \pi(\theta_p) \), the new computational bottleneck is the calculations required to obtain the \( P + 1 \) proposal density terms \( q(\theta_p, \Theta_{-p}) \) for \( p = 0, \ldots, P \). Under an independent proposal mechanism with a proposal distribution of the form \( q(\theta_0, \Theta_{-0}) = \prod_{p=1}^P q(\theta_0, \theta_p) \), the acceptance probabilities (2) require the
$O(P^2)$ evaluation of the $(P^2+1)$ terms $q(\theta_p, \Theta_{-p})$. To avoid such calculations, we follow Holbrook (2021) and use symmetric proposal distribution for which $q(\theta_p, \Theta_{-p}) = q(\theta_{\tilde{p}}, \Theta_{-\tilde{p}})$ for $p, \tilde{p} = 0, \ldots, P$.

Algorithm 5 The Gumbel-max trick

Data: a vector of unnormalized log-probabilities $\lambda^* = \log \pi + \log c$, for $\pi$ a discrete probability vector with $P + 1$ elements.

Result: A single sample $\hat{p} \sim \text{Discrete}(\pi)$ satisfying $\hat{p} \in \{0, 1, \ldots, P\}$.

for $p \in \{0, 1, \ldots, P\}$ do
  $\; z_p \leftarrow \text{Gumbel}(0, 1); \; \alpha^*_p \leftarrow \lambda^*_p + z_p$;
end

$\hat{p} \leftarrow \arg\max_{p=0,\ldots,P} \alpha^*_p; \; \text{return } \hat{p}.$

3.1. Simplified Acceptance Probabilities

Evaluation of the $P+1$ proposal density terms $q(\theta_p, \Theta_{-p})$ can be computationally burdensome as $P$ grows large. Holbrook (2021) proves that two specific proposal mechanisms enforce equality across all $P + 1$ terms and thus enable the simplified acceptance probabilities

$$\pi_p = \frac{\pi(\theta_p)}{\sum_{p'=0}^P \pi(\theta_{p'})}, \quad p = 0, \ldots, P.$$  \hfill (6)

In Section 3.2, we opt for one of these proposal mechanisms, the centered Gaussian proposal of Tjelmeland (2004). This strategy first generates a Gaussian random variable $\theta$ centered at the current state $\theta_0$ and then generates $P$ proposals centered at $\tilde{\theta}$:

$$\theta_1, \ldots, \theta_P \sim \text{Normal}_D(\tilde{\theta}, \Sigma), \quad \tilde{\theta} \sim \text{Normal}_D(\theta_0, \Sigma).$$  \hfill (7)

Holbrook (2021) shows that this strategy leads to the higher-order proposal symmetry

$$q(\theta_0, \Theta_{-0}) = q(\theta_1, \Theta_{-1}) = \cdots = q(\theta_p, \Theta_{-p})$$  \hfill (8)

and that the simplified acceptance probabilities (6) maintain detailed balance. In fact, other location scale families also suffice in the manner, but here we focus on Gaussian proposals without loss of generality. Finally, the simplicial sampler (Holbrook 2021) accomplishes the same simplified acceptance probabilities but incurs an $O(D^3)$ computational cost.

One may also use a more limited strategy to enforce (8). Glatt-Holtz et al. (2022) show that the sampler using independence proposal $q(\theta_p, \Theta_{-p}) = \prod_{p' \neq p} q(\theta_{p'})$, where $q(\cdot)$ is not a function of $\theta_p$, results in acceptance probabilities

$$\pi_p = \frac{\pi(\theta_p)/q(\theta_p)}{\sum_{p'=0}^P \pi(\theta_{p'p})/q(\theta_{p'})}, \quad p = 0, \ldots, P.$$  \hfill (9)

When $\pi(\cdot)$ and $q(\cdot)$ take continuous values on a topologically compact domain or discrete values on a finite domain, one may specify $q(\cdot)$ to be uniform and let (9) simplify to (6). This strategy proves useful in Section 3.3, in which we consider discrete-valued targets over Ising-type lattice models.

3.2. Continuously Valued Targets

Algorithm 6 presents the details of QPMCMC for a continuously-valued target. The algorithm uses conventional (perhaps parallel) computing almost entirely, excluding two lines that are highlighted. The first of these loads proposals onto the quantum machine, and the second line that calls the quantum minimization algorithm presented in Algorithm 4. This subroutine seeks to find the minimizer of the function

$$f(p) = -(z_p + \log \pi(\theta_p)) \quad \text{over } p = 0, 1, \ldots, P,$$  \hfill (10)

which combines the numerators of (2), the Gumbel-max trick and a trivial negation. As discussed in Section 2.2, the subroutine requires only $O(\sqrt{P})$ oracle evaluations and, therefore, only $O(\sqrt{P})$ evaluations of the target density $\pi(\cdot)$ using a quantum circuit. In theory, a quantum computer can perform the same computations as a classical computer, but the efficiency of the target evaluations would depend on a number of factors related to the structure of the density itself, the availability of fast quantum random access memory (Giovannetti, Lloyd, and Maccone 2008) and the ability of large numbers of quantum gates to act in concert with negligible noise (Kiepinski, Monroe, and Wineland 2002; Erhard et al. 2019).
In general MCMC, one often calibrates the scaling of a proposal kernel to balance between exploring the target’s domain and remaining within high-density regions. Optimal scaling strategies may lead to a large number of rejected proposals (Roberts and Rosenthal 2001). Indeed, Holbrook (2021) shows that parallel MCMC algorithms are no exception. When using the Gumbel-max trick to sample from proposals, this means that the current state is often quite near optimality, representing a warm-start. Figure 5 shows how this warm-starting effects the number of oracle calls (and hence target evaluations) within the quantum minimization sub-routine over the course of an MCMC trajectory. We target multi-dimensional standard normal distributions of differing dimensions using the vector $\{100, \ldots, 100\}$ as starting position. We fix the number of Gaussian proposals to be 2000 and use standard adaptation procedures (Rosenthal 2011) to target a 50% acceptance rate while guaranteeing convergence. Although no theoretical results validate this target acceptance rate, the rate is close to empirically optimal rates from Holbrook (2021). Across iterations, QPMCMC requires relatively few oracle calls compared to the 2000 target evaluations of parallel MCMC. We also witness the expected drop in the number of oracle evaluations as the chain approaches the target’s high-density region. Remarkably, the algorithm succeeds in sampling from the true discrete distribution in 99.5% of the MCMC iterations. An independent simulation obtains similar results, requiring roughly 7% of the usual 4 million target evaluations. Over 99.4% of the 10,000 MCMC iterations across all dimensions successfully sample from the discrete distribution with probabilities of $\{\alpha\}$. Burn-in iterations require moderately more evaluations because the current state occupies a lower density region and represents a "less good" warm-start.

Finally, we compare convergence speed for QPMCMC using 1000, 5000, and 10,000 proposals to target a massively multimodal distribution: a mixture of 1000 two-dimensional, isotropic Gaussians with standard deviations equal to 1 and means equal to $10 \times \{0, 1, \ldots, 999\}$. This target is particularly challenging because the distance between modes is significantly larger than standard deviations. In five independent simulations, we run each algorithm until it achieves and effective sample size of 100. Table 1 contains MCMC iterations and target evaluations required to achieve this effective sample size as well as relative speedups over sequential implementations and relative improvements over the 1000 proposal sampler.

### 3.3. Discrete-Valued Targets

We wish to sample from a target distribution defined over a discrete set $\{\theta_\alpha\}_{\alpha \in \mathcal{A}}$, for $\mathcal{A}$ some finite or countably infinite set of indices. Glatt-Holtz et al. (2022) establish the broader...
Sections 3.3.1 and 3.3.2 consider targets defined over finite sets \( \mathcal{A} \) and make use of the uniform independence proposal scheme described in Section 3.1, thereby facilitating simplified acceptance probabilities (6). This scheme proposes single-flip updates to the current Markov chain state \( \theta_0 \), but it is worth noting that other multiple-flip schemes would also be amenable to QPMCMC.

3.3.1. Ising Model on a Two-Dimensional Lattice

Here, we are interested in an Ising-type lattice model over configurations \( \theta = (\theta_1, \ldots, \theta_D) \) consisting of \( D \) individual spins \( \theta_d \in \{-1, 1\} \). In terms of the preceding section, we have \( \mathcal{A} = \{-1, 1\}^D \) and \( |\mathcal{A}| = 2^D \). In particular, we consider targets of the form

\[
\pi(\theta | \rho) \propto \exp \left( \rho \sum_{(d,d') \in E} \theta_d \theta_{d'} \right),
\]

where \( \rho > 0 \) is the interaction term and \( E \) is the lattice edge set. We specify a two-dimensional 500-by-500 lattice with nearest neighbors connections and fix \( \rho = 1 \). Since this latter setting encourages neighboring spins to equal each other, we begin our QPMCMC trajectories at the lowest-probability “checkerboard” state for an initial configuration. At each iteration, we generate collections of proposal states by uniformly flipping \( P \) individual spins \( \theta_p, p \in \{1, \ldots, P\} \), and obtaining each proposal state \( \theta_p \) by updating the current state \( \theta_0 \) at the single location corresponding to \( \theta_p \). Figure 7 shows results from 10 independent runs using \( P \in \{4, 8, 16, \ldots, 2048\} \) proposals. Trace plots of unnormalized log-probabilities indicate that higher proposal counts enable discovery of higher probability configurations. Interestingly, QPMCMC appears to be particularly beneficial in this large \( P \) context, requiring less than one-tenth the target evaluations required using conventional computing when \( P = 2048 \).

3.3.2. Bayesian Image Analysis

We apply a Bayesian image classification model to an intensity map (Figure 8) of the newly imaged supermassive black hole, Sagittarius A*, located at the Galactic Center of the Milky Way (Akiyama et al. 2022). Whereas one cannot see the black hole itself, one may see the shadow of the black hole cast by the hot, swirling cloud of gas surrounding it. We extract the black hole from the surrounding cloud by modeling the intensity at each of the \( D = 4076^2 = 16,613,776 \) pixels as belonging to a mixture of two truncated normals with values \( y_{d, \ell} \) restricted to the intensity range \([0, 255]\). Namely, we follow Hurn (1997) and specify the latent variable model

\[
y_{d, \ell} | (\mu_{\ell}, \sigma^2, \theta_d) \overset{\text{ind}}{\sim} \text{Normal}(\mu_{\ell}, \sigma^2), \quad y_{d} \in [0, 255],
\]

\[
\theta_d = \ell, \quad d \in \{1, \ldots, D\},
\]

\[
\mu_{\ell} \overset{\text{id}}{\sim} \text{Uniform}(0, 255), \quad \ell \in \{-1, 1\},
\]

\[
\frac{1}{\sigma^2} \sim \text{Gamma} \left( \frac{1}{2}, \frac{1}{2} \right),
\]

where \( \theta = (\theta_1, \ldots, \theta_D) \) share for a prior the Ising model (11) with edges joining neighboring pixels and interaction \( \rho = 1.2 \).

Figure 6. Empirical accuracy of quantum parallel MCMC (QPMCMC) for a 100 dimensional spherical Gaussian target. We generate 100,000 samples using 2000 proposals each iteration and remove the first 2000 samples as burn-in. The QQ (quantile-quantile) plot shows sample quantiles adhering closely to the theoretical quantiles. Similarto the independent simulations shown in Figure 5, here QPMCMC requires less than 7.2% of the usual number of target evaluations.
Table 1. Racing to a minimum (between the two dimensions) of 100 effective samples for a target with 1000 disjoint modes.

| Proposals | MCMC iterations | Target evaluations | Speedup | Efficiency gain |
|-----------|-----------------|--------------------|---------|-----------------|
| 1000      | 249,398 (200,998, 311,998) | 24,988,963 (20,149,132, 31,265,011) | 9.98 (9.98, 9.98) | 1 |
| 5000      | 14,398 (12,998, 16,998) | 3,314,560 (2,989,418, 3,916,281) | 21.72 (21.70, 21.74) | 7.58 (6.25, 9.71) |
| 10,000    | 5998 (4998, 6998) | 1,993,484 (1,662,592, 2,330,842) | 30 (29.96, 30.26) | 12.87 (8.64, 18.80) |

NOTE: “Speedup” is ratio between target evaluations required for sequential and quantum implementations. “Efficiency gain” is ratio between target evaluations required for 1000 proposal and 5000/10,000 proposal implementations. We report means (minima, maxima) across five independent runs.

Figure 7. Convergence of log-posterior for a parallel MCMC sampler targeting an Ising model with uniform interaction $\rho = 1$ and no external field. All chains begin at minimal probability “checkerboard” state. Larger proposal counts allow discovery of higher probability configurations.

We use a QPMCMC-within-Gibbs scheme to infer the join posterior of $\theta$ and the three mixture model parameters. For the former, we use the same QPMCMC scheme as in Section 3.3.1 with 1024 proposals at each iteration. For the latter, we use the closed-form updates presented in Hurn (1997). We run this scheme for 20 million iterations, discarding the first 10 million as burnin. We thin the remaining sample at a ratio of 1 to 40,000 for the latent memberships $\theta$ and 1 to 4000 for the three parameters $\mu_{-1}$, $\mu_1$ and $\sigma^2$. Using the R package CODA (Plummer et al. 2006), we calculate effective sample sizes of the log-posterior (257.1), $\mu_{-1}$ (1,578.7), $\mu_1$ (257.6) and $\sigma^2$ (2500.0), suggesting adequate convergence. Figure 8 shows both the intensity data and the pixelwise posterior mode of the latent membership vector $\theta$. The QPMCMC requires only 1,977,553,608 target evaluations compared to the $1024 \times 20,000,000 = 2.048 \times 10^{10}$ evaluations required for the analogous parallel MCMC scheme implemented on a conventional computer, representing a 10.36-fold speedup.

4. Discussion

We have shown that parallel MCMC enjoys quadratic speedups by combining quantum minimization with the Gumbel-max trick. Within a QPMCMC iteration, the current state represents a warm-start for the sampling-turned-optimization problem, leading to increased efficiencies for the quantum minimization algorithm. Moreover, combining this approach with the Tjelmeland correction (Holbrook 2021) results in a total complexity reduction from $O(P^2)$ to $O(\sqrt{P})$. Preliminary evidence suggests that our strategy may find use when target distributions exhibit extreme multimodality. While the algorithm still must construct long Markov chains to reach equilibrium, generating each individual Markov chain state requires significantly fewer target evaluations.

There are major technical barriers to the practical implementation of QPMCMC. The framework, like other quantum machine learning (QML) schemes, requires on-loading and off-
loading classical data to and from a quantum machine. In the seminal review of QML, Biamonte et al. (2017) discuss what they call the "input problem." Cortese and Braje (2018) present a general purpose quantum circuit for loading \(B\) classical bits into a quantum data structure comprising \(\log_2(B)\) qubits with circuit depth \(O(\log(B))\). For continuous targets, QPMCMC requires reading \(O(P)\) real vectors \(\theta_p \in \mathbb{R}^D\) onto the quantum machine at each MCMC iteration. If \(b\) is the number of bits used to represent a single real value, then reading \(B = O(Pdb)\) classical bits into the quantum machine requires time \(O(\log(Pdb))\). This is true whether one opts for fixed-point (Jordan 2005) or floating-point (Haener et al. 2018) representations for real values. The outlook can be better for discrete distributions. For example, the QPMCMC scheme presented in Section 4 only requires loading the entire configuration state once prior to sampling. A \(D\)-spin Ising model requires \(D\) classical bits to encode, and these bits load onto a quantum machine in time \(O(\log(D))\). Once one has encoded the entire system state, each QPMCMC iteration only requires loading the addresses of the \(O(P)\) proposal states. If one uses \(b\) bits to encode each address, then the total time required to load data onto the quantum machine is \(O(\log(Pb))\) for each QPMCMC iteration. On the other hand, the speedup for discrete targets assumes the ability to hold an entire configuration in QRAM. Conveniently, the "output problem" is less of an issue for QPMCMC, as only a single integer \(\hat{p} \in \{0, \ldots, P\}\) need be extracted within Algorithm 4.

This work leads to three interesting questions. First, what is the status of inference obtained by QPMCMC? The QPMCMC selection step relies on quantum minimization, an algorithm that only achieves success with probability \(1 - \epsilon\). While empirical studies suggest that this error induces little bias, it would be helpful to use this \(\epsilon\) to bound the distance between the target distribution and the distribution generated by QPMCMC. Such theoretical efforts would need to extend recent formalizations of the multiproposal based parallel MCMC paradigm (Glatt-Holtz et al. 2022) to account for biased MCMC kernels.

Second, can QPMCMC be combined with established quantum algorithms that make use of "quantum walks" on graphs to sample from discrete target distributions? Szegedy (2004) presents a quantum analog to classical ergodic reversible Markov chains and shows that such quantum walks sometimes provide quadratic speedups over classical Markov chains. Szegedy (2004) also points out that Grover’s search, a key component within QPMCMC, may be interpreted as performing just such a quantum walk on a complete graph. Wojcan and Abeyesinghe (2008) accelerate the quantum walk by using ancillary Markov chains to improve mixing and apply their method to simulated annealing. Given a quantum algorithm \(A\) for producing a discrete random sample with variance \(\sigma^2\), Montanaro (2015) develops a quantum algorithm for estimating the mean of algorithm \(A\)'s output with error \(\epsilon\) by running algorithm \(A\) a mere \(\tilde{O}(\sigma/\epsilon)\) times, where \(\tilde{O}\) hides polylogarithmic terms. Importantly, this quadratic quantum speedup over classical Monte Carlo applies for quantum algorithms \(A\) that only feature a single measurement such as certain simple quantum walk algorithms. Unfortunately, this assumption fails for quantizations of Metropolis-Hastings, in general, and QPMCMC, in particular. More promising for QPMCMC, Lemieux et al. (2020) develop a quantum circuit that applies Metropolis-Hastings to the Ising model without the need for oracle calls. An interesting question is whether similar non-oracular quantum circuits exist for the basic parallel MCMC backbone to QPMCMC. In general, however, comparison between QPMCMC and other quantum Monte Carlo techniques is challenging because the foregoing literature (a) largely focuses on MCMC as a tool for discrete optimization, with algorithms that only ever return a single Monte Carlo sample or function thereof, and (b) restricts itself to a handful of simple, stylized and discrete target distributions. On the other hand, QPMCMC is a general inferential framework for sampling from general discrete and continuous distributions alike.

Third, there are other models and algorithms in statistics, machine learning and statistical mechanics that require sampling from potentially costly discrete distributions. Can one adapt our quantum Gumbel-max trick to these? Approximate Bayesian computation (Csilléry et al. 2010) extends probabilistic inference to contexts within which one only has access to a complex, perhaps computationally intensive, forward model. Having sampled model parameters from the prior, one accepts or rejects these parameter values based on the discrepancy between the observed and simulated data. If one succeeds in embedding forward model dynamics within a quantum circuit, then one may plausibly select from many parameter values using our quantum Gumbel-max trick. The trick may also find use within sequential Monte Carlo (Doucet, De Freitas, and Gordon 2001). For example, Berzuini and Gilks (2001) present a sequential importance resampling algorithm that uses MCMC-type moves to encourage particle diversity and avoid the need for bootstrap resampling. Multiproposals accelerated by the quantum Gumbel-max trick could add speed and robustness to such MCMC-resampling.

Large-scale, practical quantum computing is still a long way off, but quantum algorithms are ripe for mainstream computational statistics.

Appendix A. Limited Introduction to Quantum Computing

Quantum computers perform operations on unit-length vectors of complex data called quantum bits or qubits. One may write any qubit \(\psi\) as a linear combination of the computational basis states \(|0\rangle\) and \(|1\rangle\). In symbols,

\[
|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad \text{for} \quad \alpha, \beta \in \mathbb{C} \quad \text{and} \quad |\alpha|^2 + |\beta|^2 = 1.
\]

This formula uses Dirac or bra-ket notation and obscures ideas that are commonplace in the realm of applied statistics. We make the unit-vector specification of \(|\psi\rangle\) clear by writing

\[
|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}
\]

or \(|\psi\rangle = \alpha |1\rangle + \beta |0\rangle\).

The full machinery of linear algebra is also available within this notation. The conjugate transpose of \(|\psi\rangle\) is \(\langle \psi |\). The inner product of \(|\psi\rangle\) and \(|\phi\rangle\) is \(\langle \phi | \psi \rangle\). The outer product is \(|\psi\rangle\langle \phi |\). Naturally, we can write \(\psi\) as a linear combination of any other such basis elements. Consider instead the vectors

\[
|+\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \quad \text{and} \quad |-\rangle = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle.
\]

A little algebra shows that \(|+\rangle\) and \(|-\rangle\) are indeed unit-length and orthogonal to each other. A little more algebra reveals that, with respect
to this basis, $\psi$ has coefficients $\alpha'$ and $\beta'$ given by $(\alpha + \beta')/\sqrt{2}$ and $(\alpha - \beta')/\sqrt{2}$, respectively. A last bit of algebra shows that this representation is consistent with $\psi$’s unit length.

But linear algebra is not the only aspect of quantum computing that should come easily to applied statisticians. In addition to thinking of $\psi$ as a vector, it is also useful to think of $\psi$ as a (discrete) probability distribution over the computational basis states $|0\rangle$ and $|1\rangle$. The constraints on coefficients $\alpha$ and $\beta$ mean that we can think of $|\alpha|^2$ and $|\beta|^2$ as probabilities that $\psi$ is in state $|0\rangle$ or $|1\rangle$, respectively. Accordingly, $|+\rangle$ and $|-\rangle$ encode uniform distributions over the computational basis states. In the parlance of quantum mechanics, $|\alpha|^2$ and $|\beta|^2$ are probability amplitudes, and $\psi$, $|+\rangle$ and $|-\rangle$ are all superpositions of the computational basis states. Quantum measurement of $\psi$ results in $|0\rangle$ with probability $|\alpha|^2$, but—in the following—we can safely think of this physical procedure as drawing a single discrete sample from $\psi$’s implied probability distribution.

Quantum logic gates perform linear operations on qubits like $\psi$ and take the form of unitary matrices $U$ satisfying $U^\dagger U = I$ for $U$ the conjugate transpose of $U$. One terrifically important single-qubit quantum gate is the Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$  

One may verify that $H$ is indeed unitary and that its action maps $|0\rangle$ to $|+\rangle$ and $|1\rangle$ to $|-\rangle$. In fact, the reverse is also true on account of the symmetry of $H$. The Hadamard gate thus takes the computational basis states in and out of superposition, facilitating a phenomenon called quantum parallelism. Given a function $f : \{0, 1\} \rightarrow \{0, 1\}$, consider the two-qubit quantum oracle gate $U_f$ which takes $|x\rangle |y\rangle$ as input and returns $|x\rangle |y \oplus f(x)\rangle$ as output, where $\oplus$ denotes addition modulo 2. Importantly, the output simplifies to $|x\rangle |f(x)\rangle$ for $y = 0$. We now consider a quantum circuit that acts on two qubits by first applying the Hadamard transform $H$ to the first qubit and then applying the oracle gate $U_f$ to both. Using the state $|0\rangle |0\rangle$ as input, we have

$$|0\rangle |0\rangle \rightarrow \frac{1}{\sqrt{2}} (|0\rangle |0\rangle + |1\rangle |0\rangle) \rightarrow \frac{1}{\sqrt{2}} (|0\rangle |f(0)\rangle + |1\rangle |f(1)\rangle). $$  

(A.1)

The quantum circuit evaluates $f(\cdot)$ simultaneously over both inputs! Unfortunately, the scientist who implements this circuit cannot directly access $U_f$’s output, and measurement will provide only $|0\rangle |f(0)\rangle$ or $|1\rangle |f(1)\rangle$ with probability 1/2 each. Unlocking the potential of quantum parallelism requires more ingenuity.

Uncountably many single- and two-qubit quantum gates exist, but the real power of quantum computing stems from the development of complex quantum gates that act on multiple qubits simultaneously. To access this power, we need one more tool that also appears in the statistics literature. The Kronecker or tensor product between an $L$-by-$M$ matrix $A$ and an $N$-by-$O$ matrix $B$ is the $LN$-by-$MO$ matrix

$$A \otimes B = \begin{bmatrix} A_{11}B & \ldots & A_{1M}B \\ \vdots & \ddots & \vdots \\ A_{L1}B & \ldots & A_{LM}B \end{bmatrix}. $$  

(A.2)

In statistics, the Kronecker product features in the definition of a matrix normal distribution and is sometimes helpful when specifying the kernel function of a multivariate Gaussian process (Werner, Jansson, and Stoica 2008). Here, the product is equivalent to the parallel action of individual quantum gates on individual qubits. Simple application of Formula (A.2) shows that

$$H^\otimes 2 = H \otimes H = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} $$  

and

$$|0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \end{bmatrix} |0\rangle + \begin{bmatrix} 1 \end{bmatrix} |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}. $$  

(A.3)

We may also denote the left product $H^\otimes 2$ and the right product $|0\rangle^\otimes 2$, $|00\rangle$ or $|0 |0\rangle$. One may therefore express (A.1) as a series of transformations applied to the 4-vector on the very right. Letting $|10\rangle$, $|01\rangle$ and $|11\rangle$ take on analogous meanings to $|00\rangle$, an immediate result of (A.3) is that

$$H^\otimes 2 |00\rangle = \frac{1}{2} \left( |00\rangle + |01\rangle + |10\rangle + |11\rangle \right). $$  

(A.4)

The action of $H^\otimes 2$ transforms $|00\rangle$ into a superposition of the states $|00\rangle$, $|10\rangle$, $|01\rangle$ and $|11\rangle$, where the probability of selecting each is a uniform $1/(2^2) = 1/4$. Writing so many 0s and 1s is tedious, so an alternative notation becomes preferable. Exchanging $|00\rangle$ for $|00\rangle$, $|11\rangle$ for $|01\rangle$, $|2\rangle$ for $|10\rangle$, and $|3\rangle$ for $|11\rangle$, (A.4) becomes the more succinct

$$H^\otimes 2 |00\rangle = \frac{1}{2} \left( |0 + |1 + |2 + |3 \rangle \right). $$  

This formula extends generally to operations over $n$ qubits. Now letting $N = 2^n$, we have

$$H^\otimes n |0\rangle^\otimes n = \frac{1}{\sqrt{N}} \left( |0\rangle + |1\rangle + \ldots + |N - 1\rangle \right) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle =: |h\rangle, $$  

and we call $|h\rangle$ a uniform superposition over the states $|0\rangle, \ldots, |N - 1\rangle$. The many-qubit analogue for the quantum parallelism of (A.1) is then

$$|0\rangle^\otimes n \rightarrow \left( \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \right) |0\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle. $$

Appendix B. Gumbel-max

We wish to randomly select a single element from the set $\{0, 1, \ldots, P\}$ with probability proportional to the unnormalized probabilities $\pi^* = (\pi_0^*, \pi_1^*, \ldots, \pi_P^*)$. That is, there exists a $c > 0$ such that $\pi^* = c \pi$, for $\pi$ a valid probability vector, but we only have access to $\pi^*$. Define $\lambda_\pi := \log \pi$ and $\lambda^* := \log \pi^* = \log \pi + \log c$, and assume that $z_0, \ldots, z_P \sim \text{Gumbel}(0, 1)$. Then, the probability density function $g(\cdot)$ and cumulative distribution function $G(\cdot)$ for each individual $z_p$ are

$$g(z_p) = \exp \left( -z_p - \exp(-z_p) \right) \quad \text{and} \quad G(z_p) = \exp \left( - \exp(-z_p) \right). $$

Now, defining the random variables $\alpha^*_p := \lambda^*_p + z_p$, $\alpha_p := \lambda_p + z_p$ and

$$\hat{p} = \arg \max_{p=0, \ldots, P} \alpha^*_p, $$

we have the result

$$\Pr(\hat{p} = p) = \pi_p. $$

In words, the procedure of adding Gumbel noise to unnormalized log-probabilities and taking the index of the maximum produces a random...
variable that follows the discrete distribution over \( \pi \). Moving from left to right:

\[
Pr(\hat{p} = p) = Pr(\alpha^*_p > \alpha^*_{p'}, \forall p' \neq p)
\]

\[
= Pr(\alpha_p + \log c > \alpha_{p'}, \forall p' \neq p)
\]

\[
= Pr(\alpha_p > \alpha_{p'}, \forall p' \neq p)
\]

\[
= \int_{-\infty}^{\infty} \prod_{p' \neq p} Pr(\alpha_p > \alpha_{p'} | \alpha_p) g(\alpha_p - \lambda_p) d\alpha_p
\]

\[
= \int_{-\infty}^{\infty} \prod_{p' \neq p} G(\alpha_p - \lambda_{p'}) g(\alpha_p - \lambda_p) d\alpha_p
\]

\[
= \int_{-\infty}^{\infty} \prod_{p' \neq p} \exp\left(-\exp(\lambda_{p'} - \alpha_{p'})\right) \exp\left(-\alpha_{p'} + \lambda_{p'} - \exp(-\alpha_{p'} + \lambda_{p'})\right) d\alpha_p.
\]

Recalling that \( \lambda_{p'} = \log \pi_{p'} \), we exponentiate the logarithms, and the integral becomes

\[
\pi_p \int_{-\infty}^{\infty} \prod_{p' \neq p} \exp\left(-\pi_{p'} \exp(-\alpha_{p'})\right) \exp\left(-\alpha_{p'} - \pi_p \exp(-\alpha_{p'})\right) d\alpha_p
\]

\[
= \pi_p \int_{-\infty}^{\infty} \exp(-\alpha_{p'}) \exp\left(-\sum_{p' = 0}^{p} \pi_{p'} \exp(-\alpha_{p'})\right) d\alpha_p
\]

\[
= \pi_p \int_{-\infty}^{\infty} \exp(-\alpha_{p'}) \exp\left(-\exp(-\alpha_{p'})\right) d\alpha_p = \pi_p,
\]

where the final equality follows easily from a change of variables.

**Appendix C. Mixing of Parallel MCMC and QPMC M**

To ascertain whether QPMC MCMC mixes differently compared to conventional parallel MCMC, we run both algorithms for a range of proposal counts to sample from a 10-dimensional standard normal distribution. For each algorithm and proposal setting, we run 100 independent chains for 10,000 iterations and obtain effective sample sizes ESS\(_p\) for \( d \in \{1, \ldots, 10\} \). We then calculate the relative differences between the means and minima of one chain generated using parallel MCMC and one chain generated using QPMC MCMC; for example:

Relative difference between means ESS\(_p\):

\[
\frac{|\text{ESS}_{pMCMC} - \text{ESS}_{QPMC MCMC}|}{\text{ESS}_{pMCMC}}
\]

Figure B.1 shows results. In general, the majority relative differences are small. For both statistics, mean relative differences are less than 0.05, regardless of proposal count. Again for both statistics, more than 75% of the independent runs result in relative differences below 0.1. We note that relative differences between means (blue) appear to decrease with the number of proposals, but the same does not hold for relative differences between minima (red).

**Appendix D. Note on Simulations**

We use R (R Core Team 2021), Python (van Rossum 1995), TensorFlow (Abadi et al. 2016) and TensorFlow Probability MCMC (Lao et al. 2020) in our simulations and the ggplot2 package to generate all figures (Wickham 2016). In R, we use the package CODA (Plummer et al. 2006) to calculate effective sample sizes. In Python, we use a built-in function from TensorFlow Probability MCMC. The primary color palette comes from Ram and Wickham (2018).

All simulations rely on the fact that the Grover iterations of (3) manipulate the probability amplitudes in a deterministic manner. For example, the following R code specifies \( N \) uniform probability amplitudes (sqrtProbs), performs \( I \) Grover iterations and measures a single state according to the resulting probabilities.

```r
sqrtProbs <- rep(1/sqrt(N),N); i <- 1
while (i <= I) {
  sqrtProbs <- (1-2*marks)*sqrtProbs
  sqrtProbs <- -sqrtProbs + 2*mean
  i <- i + 1
}
measurement <- sample(size=1, x=1:N, prob=sqrtProbs^2)
```

Of course, simulating these iterations on a classical computer requires precomputing the values of marks beforehand. All code is available online at [https://github.com/andrewjholbrook/qPMCMC](https://github.com/andrewjholbrook/qPMCMC).

**Disclosure Statement**

There are no competing interests to declare.

**Funding**

This work was supported by grants NIH K25 AI153816, NSF DMS 2152774 and NSF DMS 2236854.

**References**

Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., Devin, M., Ghemawat, S., Irving, G., Isard, M., et al. (2016), “TensorFlow: A System for [Large-Scale] Machine Learning,” in 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16), pp. 265–283. [1414]

Akiyama, K., Alberdi, A., Alef, W., Algaba, J. C., Anantua, R., Asada, K., Azulay, R., Bach, U., Bachzko, A.-K., Ball, D., et al. (2022), "First Sagittarius A* Event Horizon Telescope Results. I. The Shadow of the Supermassive Black Hole in the Center of the Milky Way," The Astrophysical Journal Letters, 930, L12. [1410,1411]

Bennett, C. H., Bernstein, E., Brassard, G., and Vazirani, U. (1997), "Strengths and Weaknesses of Quantum Computing," SIAM Journal on Computing, 26, 1510–1523. [1403]

Berzuini, C., and Gilks, W. (2001), "Resample-Move Filtering with Cross-Model Jumps," in Sequential Monte Carlo Methods in Practice, eds. A. Doucet, N. Freitas, and N. Gordon, pp. 117–138, New York: Springer. [1412]

Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., and Lloyd, S. (2017), "Quantum Machine Learning," Nature, 549, 195–202. [1412]

Boyer, M., Brassard, G., Heyer, P., and Tapp, A. (1998), "Tight Bounds on Quantum Searching," Fortschritte der Physik: Progress of Physics, 46, 493–505. [1403,1404,1405,1406]

---

Figure B.1. Relative differences between effective sample sizes (ESS) for parallel MCMC (pMCMC) and quantum parallel MCMC (QPMC MCMC) across a range of proposal counts. We target a 10-dimensional standard normal distribution. For each algorithm and proposal setting, we generate 100 independent chains of length 10,000 and calculate the mean and minimum ESS across dimensions.
