Thermodynamic optimization of quantum algorithms: On-the-go erasure of qubit registers

Florian Meier\textsuperscript{1,2} and L\'{a}dia del Rio\textsuperscript{1} \textsuperscript{*}

\textsuperscript{1}Institute for Theoretical Physics, ETH Z"urich, 8093 Z"urich, Switzerland
\textsuperscript{2}Atominstiut, Technische Universit"at Wien, 1020 Vienna, Austria

(Dated: December 23, 2022)

We consider two bottlenecks in quantum computing: limited memory size and noise caused by heat dissipation. Trying to optimize both, we investigate “on-the-go erasure” of quantum registers that are no longer needed for a given algorithm: freeing up auxiliary qubits as they stop being useful would facilitate the parallelization of computations. We study the minimal thermodynamic cost of erasure in these scenarios, applying results on the Landauer erasure of entangled quantum registers. For the class of algorithms solving the Abelian hidden subgroup problem, we find optimal on-the-go erasure protocols. We conclude that there is a trade-off: if we have enough partial information about a problem to build efficient on-the-go erasure, we can use it to instead simplify the algorithm, so that fewer qubits are needed to run the computation in the first place. We provide explicit protocols for these two approaches.

I. INTRODUCTION

When is the best time to reset qubit registers? A default option is to run a whole algorithm and reset all registers to $|0\rangle$ at the end, after the final measurements. However, if the total number of qubits is a limitation and we need to run several algorithms concurrently, we may want to free up some registers as they stop being useful: for example, in the period-finding algorithm, the auxiliary register can be discarded after applying the oracle (Figure 1a). Another critical factor may be heat dissipation: Landauer’s principle tells us that the erasure of every single qubit from a fully mixed state to $|0\rangle$ has a fundamental work cost of $k_B T \ln 2$ if performed at temperature $T$, releasing the same amount of heat to the environment \cite{landauer1961}. As heat dissipation in a quantum computer threatens coherence, reducing the work cost of erasure may be of critical importance.

Previous erasure schemes. We consider algorithms that use a main register of $n$ qubits and an auxiliary register of $m$ qubits (Figure 1a); the latter can be discarded at some halfway point in the algorithm. For example, the period-finding algorithm is of this form. To optimize memory space, we may want to erase it as soon as possible: a brute-force erasure procedure of those $m$ qubits (Figure 1b) would dissipate heat $m k_B T \ln 2$ with a simple fixed map, independent of the algorithm. On the other extreme, if we only want to optimize the heat cost, we can apply Bennett’s reversible erasure procedure \cite{bennett1997}, which coherently copies the output register to an external system, and then uncomputes the algorithm’s circuit on the original qubits reversibly (Figure 1c). The main drawback of this procedure emerges when it is applied to probabilistic quantum algorithms like period-finding: Bennett’s uncomputing only works when the output register is decoupled from the rest of the quantum computer — in other words, when the algorithm outputs a deterministic result \cite{delrio2022}. Probabilistic quantum algorithms are made (approximately) deterministic by repeating them many times, and applying classical post-processing to the probabilistic outputs, including for example a majority vote. To apply Bennett’s uncomputing to a probabilistic algorithm like period-finding, we would have to implement all these runs of the algorithm and the (usually classical) post-processing as a large reversible quantum circuit, so that the final post-processed quantum output is approximately decoupled from the rest of the memory \cite{delrio2022}. This process has a large complexity cost both in terms of memory size and circuit length; while it may be worth pursuing in a distant future when our computers work flawlessly and reversibly at the quantum level, in this work we focus on a NISQ regime, and try to optimize both thermodynamic and computational complexity costs of algorithms.

Thermodynamic considerations. We will work in the quantum resource theory of thermal operations \cite{chiribella2010,gu2012,uffmann2012}. In this framework, unitary operations on degenerate systems are given for free, and irreversible operations like erasure have associated work costs. Contemporary quantum computers are of course still far from this ideal scenario; nonetheless, the fundamental limits for the energy cost of implementing single-qubit unitaries are comparable to that of erasure \cite{gross2014}. Moreover, note that the energy requirements to implement common unitary operations (which depend on the quantum control mechanisms) scale sublinearly on the number of qubits, while erasure scales linearly \cite{gross2014}. This, together with recent erasure experiments that approach Landauer’s limit \cite{helsen2013,delrio2022}, have us speculate that energies of the order $k_B T$ may eventually become relevant to quantum computing. Overall, thermodynamic optimization of quantum com-

\footnote{1 For example, majority votes can be implemented reversibly \cite{bennett1997}.}
putation entails at least three independent components: (1) cost of unitary gates, (2) cost of erasure of fully mixed qubits, (3) optimizing number of fully mixed qubits that must be erased (see [14–17] for reviews on the thermodynamics of quantum computation). Our work addresses the third component, and can be applied in conjunction with restrictions or improvements on the former two. This is further discussed in Section IV.

A. Contribution of this paper

Optimized on-the-go erasure. Making use of entanglement between the main and auxiliary register as a thermodynamic resource [7–9, 14, 18, 19], we introduce a new erasure scheme (Figure 1d). It entails a strictly lower heat dissipation than brute-force erasure; in contrast to Bennett’s uncomputing, the auxiliary register is reset on-the-go without needing additional qubits. However, these improvements do not come for free: the main cost of our scheme will arise from the information to access the entanglement.

List of results. In the setting of the Abelian hidden subgroup problem, we use partial information about entanglement to optimize the erasure of auxiliary registers. In particular:

1. We find that optimal erasure (where all the entanglement between registers is exploited) is only possible if we already know the solution to the problem, i.e. the hidden subgroup (Theorem 5).
2. Given partial information about the problem, we provide an optimal on-the-go erasure protocol of auxiliary registers and compute its work cost (Theorem 8).
3. As an alternative to erasure, we can use that same partial information to simplify the algorithm, so that it uses fewer qubits (Theorem 9). We provide explicit protocols for the cases of black-box oracles and open circuit access to oracles (Figure 4 and 5).
4. There is a precise trade-off between the thermodynamic cost of erasure and algorithm simplification. The optimal choice of implementation (in terms of computational complexity) depends on the oracle: if we have open circuit access to the oracle, it is more efficient to simplify the circuit; if the oracle is given as a black box it is roughly equivalent to perform on-the-go erasure or to simplify the circuit.

Structure. In Section II we review the mathematical tools and notions of quantum thermodynamics along with the algorithm solving the Abelian hidden subgroup problem. These are the main ingredients on which our results are based which will be shown in Section III. By the example of the period finding algorithm in Section III C 1, we illustrate the key concepts of our optimized on-the-go
erasure scheme and in Section III A we generalize the example to the Abelian hidden subgroup problem. There, we state the main theorems 3 - 9 together with a qualitative sketch of the proofs. Discussions and open questions can be found in Section IV. The full proofs of the main theorems and further generalizations are explored in the appendix: in appendix A an explicit erasure protocol 20 is reviewed, and appendices B and C contain the proofs for our results.

II. SETTING & BUILDING BLOCKS

In this section we briefly review the results obtained in 18 regarding optimal bounds for the thermodynamic costs of erasing a memory with quantum side information — this will be useful as a building block for our erasure schemes. Then we recall the algorithm solving the Abelian hidden subgroup problem, and lastly, we devise a strategy for how to optimize the erasure of the auxiliary register of said algorithm.

A. Erasure with quantum side information

Work cost of erasure. Landauer’s principle 1, 21 demonstrates the intricate relation between information theory and thermodynamics. It states that logically irreversible operations come with an intrinsic work cost, related to the temperature of the environment where the computation is carried out. If we are looking at a system $S$ initially in a state $\rho_S$, the average work cost of erasing this system at a temperature $T$ (that is setting $\rho_S \rightarrow |0\rangle \langle 0|_S$ using a thermal bath at temperature $T$) scales with the entropy of the initial state,

$$W(S) = H(S)k_B T \ln 2,$$

where $k_B$ is the Boltzmann constant and $H(\rho) = -\text{Tr}(\rho \log \rho)$ is the von-Neumann entropy 14. In the setting of Figure 1 being ignorant about the state of the $m$-qubit auxiliary system, one has to apply a fixed erasure map and not the optimal map designed for the actual state $\rho_S$. The average work cost of this map corresponds to the worst-case scenario of erasing a fully mixed state $\rho_S = (1/2)^\otimes m$, that is $m k_B T \ln 2$ for erasure at temperature $T$. This energy is then dissipated into the rest of the quantum computer, causing it to heat up, which may increase noise and decoherence. Using side information, available as entanglement between the main and auxiliary registers, we attempt to improve this work cost by using the following result.

**Lemma 1** (Erasure with quantum side information 18). Given two degenerate quantum registers $G$ and $S$ and any reference system $R$, then there exists a process $\mathcal{E}$ acting on $G$, $S$ and an environment at temperature $T$ that erases $S$ while preserving $G$ and $R$, that is,

$$\rho_{RGS} \xrightarrow{\mathcal{E}} \rho_{RG} \otimes |0\rangle \langle 0|_S,$$

where $\rho_{RG} = \text{Tr}_S(\rho_{RGS})$, which does not exceed an average work cost (and heat dissipation) of

$$W(S|G)_\rho = H(S|G)_\rho k_B T \ln 2,$$

with $H(S|G)_\rho = H(GS)_\rho - H(G)_\rho$ the conditional von-Neumann entropy of $S$ conditioned on $G$. This procedure is reversible on $G$: there exists a process that achieves the transformation $\rho_G \otimes |0\rangle \langle 0|_S \rightarrow \rho_{GS}$ for the symmetric work cost $-W(S|G)_\rho$. The key insight of Lemma 1 is that quantum correlations (and in particular entanglement) can be used as additional resources to reduce the work cost of erasure of the auxiliary system. The average work cost is meant with respect to the thermodynamic limit of many independent copies of the systems $GS$ (for a brief discussion of single-shot and finite-size effects, see Section IV). In the following $G$ will be the main register and $S$ will be the auxiliary register. The reference system $R$ includes the non-accessible degrees of freedom that may be correlated with our quantum registers, e.g. the rest of the quantum computer.

**Example: erasure of half of a Bell pair 18.** This is the simplest application of Lemma 1 which will be useful to understand the general procedure later. Take system $S$ to be a single qubit with Hilbert space $\mathcal{H}_S = \mathbb{C}^2$ and $G$ to be two qubits with $\mathcal{H}_G = \mathcal{H}_{G_1} \otimes \mathcal{H}_{G_2} = \mathbb{C}^2 \otimes \mathbb{C}^2$. Suppose that initially, $G_2$ and $S$ are entangled,

$$\rho_{GS} = \rho_G \otimes |\chi\rangle \langle \chi|_{G_2} S,$$

where $|\chi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ is a fully entangled Bell state. The goal is to erase $S$ while preserving $G$ — that is, the final state should be $\rho_G \otimes |0\rangle \langle 0|_S = \rho_G \otimes \frac{1}{2} \otimes |0\rangle \langle 0|_S$. We achieve that with the following protocol:

1. Unitarily rotate the pure state of $G_2 S$ from $|\chi\rangle$ to $|00\rangle$ for free,

2. Perform reverse erasure on $G_2$, to end up in state $\rho_{G_1} \otimes \frac{1}{2} \otimes |0\rangle \langle 0|_S$, gaining $k_B T \ln 2$ work.

This erase map, decomposed in the following two steps, does not affect the reduced state of the $G$ register:

$$\rho_G = \text{Tr}_S (\rho_{GS}) = \rho_G \otimes \frac{1}{2}$$

$$\rho_G = \text{Tr}_S \left( \rho_{G_1} \otimes \frac{1}{2} \otimes |0\rangle \langle 0|_S \right).$$

\footnote{The notation $G$ for the main register is chosen because later the main register will encode a group $G.$}
FIG. 2. Abelian hidden subgroup algorithm [22, 23]. The quantum circuit above solves the Abelian hidden subgroup problem. Since it is of the same form as Figure 1d we can use it as a candidate for optimizing the on-the-go erasure. The main register \( H_G \) encodes the group \( G \) and the auxiliary register \( H_S \) encodes \( S \). The function oracle acts on states of the joint register via \( O_f|g,s⟩ = |g, s ⊕ f(g)⟩ \), with \( ⊕ \) denoting the bitwise XOR operation. The algorithm performs the following sequence:

1. Generalized quantum Fourier transform \( Q_{G} \otimes I \) on \( G \) register creates a superposition \( \frac{1}{|G|} \sum_{g \in G} |g, 0⟩ \).
2. Global oracle operation \( O_f \) on both registers. At any later point we can erase \( S \) with a map \( \mathcal{E} \).
3. Quantum Fourier transform \( Q_{G} \) on \( G \) register.
4. Measurement of the \( G \) register.
5. Classical post-processing of the result.

At the end, the total average work cost of erasure for this toy example is

\[
W(S|G) = -k_B T \ln 2 = H(S|G)k_B T \ln 2. \tag{9}
\]

in accordance with Eq. (3).

B. Hidden subgroup problem

Several computational problems can be phrased in terms of the hidden subgroup problem (HSP) [24], most famously period finding, which finds its application in Shor’s integer factorization algorithm, and the discrete logarithm problem [25]. We will first state the general problem and how our erasure algorithm applies, before looking at those particular instances.

Problem 2 (Hidden Subgroup Problem [22]). Let \( G \) be a finite group, \( S \) some finite set and \( f : G \to S \) a function. Given the existence of a subgroup \( H \subseteq G \) such that for all \( g, g' \in G \)

\[
f(g) = f(g') \iff gH = g'H, \tag{10}
\]

the goal is to determine \( H \).

The HSP can be solved by an efficient quantum algorithm originally found by [26], under the assumption that the group \( G \) is Abelian (the group operation is commutative). We will from now on be using the addition symbol \( + \) for group operations in \( G \) to highlight its Abelian property, that is \( g + h \) instead of \( gh \). Unless stated otherwise, whenever we refer to the HSP, the Abelian HSP is meant. For the general non-Abelian HSP, there are algorithms efficient in terms of oracle complexity [23, 27], but to the authors’ knowledge, no general algorithm exists that is efficient in gate complexity. Here we follow [22, 23] for the quantum algorithm solving the HSP (Figure 2). In Appendix B the computational steps are derived and explained in detail. At this point, the key observation we make is that the circuit solving the HSP is precisely of the form as required, e.g. the circuit in Figure 1d. After a unitary \( U = O_f \circ (Q_{G} \otimes I) \) operation on main and auxiliary register the latter is no longer needed and can be erased by using a Landauer erasure \( \mathcal{E} \). The computation on the main register can be continued independently.

C. Strategy towards on-the-go erasure

So far we have identified the point at which we optimize the erasure of the auxiliary register: Right after these qubits are not needed anymore but before the computation on the main register is finished. The global unitary \( U \) from Figure 1d corresponds to the composition \( O_f \circ (Q_{G} \otimes I) = U \) from Figure 2. By \( \rho_{GS} \) we denote the state of \( GS \) right after \( U \). To apply the result from Lemma 1 we have to determine where in \( \rho_{GS} \) the entanglement between \( G \) and \( S \) is. Operationally, this means we need to find local operations \( U_G \) and \( U_S \) on the main and auxiliary register respectively such that the entanglement between these registers is compressed in well-defined qubits, for example \( \ell \) Bell pairs \( |χ⟩ \),

\[
\rho_{GS} \xrightarrow{U_G \otimes U_S} \rho_{G^{(1)}S^{(1)}} \otimes (|χ⟩⟨χ|_{G^{(2)}S^{(2)}})^{\otimes \ell}. \tag{11}
\]

That is, polynomial time complexity under the assumption that \( f \) can be implemented efficiently.
In our erasure algorithm, the entanglement is always compressed into fully entangled pairs of qubits\(^4\). In Section III.A we establish bounds on the number of Bell pairs \(\ell\) for which the transformation in Eq. (11) can be achieved. After an optimized erasure of \(S\) according to Lemma 1 the reduced state of the main register is 
\[
\rho_G(\ell) \otimes \left( \frac{1}{2} 1_G^{\otimes \ell} \right) \xrightarrow{U_G^\dagger} \rho'_G,
\]
where the reduced state on \(G\) is unaffected by the erasure \(\rho'_G = \text{Tr}_S(\rho_{GS})\) (Figure 3). This ensures that the algorithm still produces the same outcome, regardless of the manipulations due to the on-the-go erasure. An important question we will answer in the next section is about the costs of the unitaries \(U_G\) and \(U_S\). While in the thermal operations resource theory they are for free, we have to quantify their cost from a computational standpoint.

### III. RESULTS

Here, we introduce the optimized on-the-go erasure protocols, starting with general bounds for the HSP. Then, we will define a class of modifications realizing these optimizations whose costs we will quantify in terms of the algorithm’s width. This section is concluded by a toy example for the period finding algorithm which is a special case of the HSP.

#### A. General bounds for on-the-go erasure in the HSP

For general unitary transformations \(U_G\) and \(U_S\) as sketched in the strategy from Section II.C there is an upper bound on how well one can optimize the thermodynamics of the algorithm:

**Theorem 3** (Entanglement upper bound). For an Abelian group \(G\) with hidden subgroup \(H\) and indicator function \(f : G \rightarrow S\) as in Problem 2, solved by the algorithm from the circuit in Figure 2 the maximal number \(\ell_{\max}\) of Bell pairs between main and auxiliary registers that can be obtained by local unitary operations is 
\[
\ell_{\max} = \log_2 \frac{|G|}{|H|} = -H(S|G)_{\rho_{GS}},
\]
where \(\rho_{GS}\) is the state of the computational registers after the oracle operation \(O_f\).

The formal proof of this statement is outsourced to Appendix B.3. Here we sketch it: The key insight is to quantify the entanglement between \(G\) and \(S\) using the conditional von-Neumann entropy \(\text{Ent}_{G/S}\). As the function \(f\) from the HSP is constant on cosets \(g + H \in G/H\), the only entanglement that is generated by the function oracle \(O_f\) comes from a sum over the different cosets in \(G/H\). Each coset \([g] \in G/H\) contributes to the entanglement by terms of the form \([g]_G/H \otimes f([g])_S\).

Theorem 5 (No-go for saturating the bound). Any on-the-go erasure protocol applying local unitaries \(U_G\) and \(U_S\) to factorize the maximum amount \(\ell_{\max}\) of Bell pairs from Theorem 3 can be used to solve the HSP.

The underlying reason is that the transformation \(U_G\) required for this factorizes the main register \(H_G\) into parts belonging to \(H\) and \(G/H\),
\[
U_G : H_G \rightarrow H_H \otimes H_{G/H}\).
\]

Essentially this means we have operational access to the elements of \(H \subseteq G\) via the inverse operation \(U_G^\dagger\). This hints at a relation between the number of Bell pairs we can factorize and the amount of information we have

\(^2\) Alternatively, one could weaken this assumption and consider partially mixed qubits, for which the relative entropy is greater, and therefore (by Lemma 1), the work cost of erasure is lower. To be applied optimally, this may require more fine-tuned control of the physical interface in the “information battery” part of the quantum computer (see Appendix A.2).
about the solution of our problem. In a next step we explore how Theorem 5 generalizes to instances where \( \ell_{\text{max}} \) is not reached. What type of partial information is required to factor \( \ell \leq \ell_{\text{max}} \) Bell pairs, and how do we quantify it?

B. On-the-go erasure and limits with partial information

**Partial information.** In a first step we characterize the partial information we need to know about the indicator function \( f : G \to S \) such that we are able to factor \( \ell \leq \ell_{\text{max}} \) Bell pairs after the function oracle \( O_f \). We start with the promise of knowing where \( \ell \) Bell pairs are, that is, we have access to transformations \( U_G \) and \( U_S \) on \( H_G \) and \( H_S \) which factor out \( \ell \) Bell pairs after the function oracle. The Bell pairs we consider are fully correlated which characterizes what we need to know about \( f \) to factor out \( \ell \) Bell pairs (Promise 6).

**Promise 6** (General partial information characterization, informal version). We need to know a factorization \( G \cong G^{(1)} \times G^{(2)} \) and \( S \cong S^{(1)} \times S^{(2)} \) with \( |G^{(2)}| = |S^{(2)}| = \ell \). Moreover, \( f \) must map \( G^{(2)} \) one-to-one on \( S^{(2)} \).

A formalized version of this promise is given in Appendix B3 Definition 18 and Theorem 19 together with a proof that Promise 6 is sufficient and necessary for factoring \( \ell \) Bell pairs. For the ease of presentation, we will present here a subclass of partial information which respects the group structure of \( G \). Partial information of this type can be understood as narrowing down the search for the subgroup \( H \subseteq G \) to a search for \( H \subseteq K \) with partial information about the function oracle (see Appendix B3 for detailed prescriptions of the transformations). In particular, the specific form in Eq. (19) allows factoring out Bell pairs as outlined in our strategy (Section 11C) in Eq. (11).

**Promise 7** (Partial subgroup information). We assume to have access to partial information about the indicator function \( f : G \to S \). That is, we know

1. an intermediate subgroup \( K \) between \( H \) and \( G \) \((H \subseteq K \subseteq G)\) which operationally means to have access to a unitary operation \( U_G \) which factors the main register according to

\[
U_G : H_G \to H_K \otimes H_{G/K}.
\]

2. where \( f \) maps \( G/K \) in \( S \); operationally that means having access to a unitary \( U_S \) such that

\[
U_G \otimes U_S |g, f(g)\rangle = |k_g, [k]\rangle \otimes |\tilde{f}(k_g), [k]\rangle.
\]

Optimized on-the-go erasure with partial information. The circuit in Figure 4 implements the modifications due to the transformations \( U_G \) and \( U_S \) from Promise 7. This brings a reduction of the work cost of erasure which we quantify in Theorem 8.

**Theorem 8** (Work cost of erasure with partial information). Given the transformations \( U_G \) and \( U_S \) from Promise 7, there exists an on-the-go erasure protocol acting on \( G \), \( S \) and an environment at temperature \( T \), resetting the auxiliary register \( S \) after \( O_f \) while preserving \( G \) which does not exceed an average work cost of erasure of

\[
W = (m - 2\ell)k_B T \ln 2,
\]

where \( \ell = \log_2 |G|/|K| \) and \( m = \log_2 |S| \) is the number of qubits of the auxiliary register.

This result also generalizes to partial information from Promise 6. The only change in the circuit of Figure 4 is that the transformations \( U_G \) and \( U_S \) have to be replaced by their generalized versions. In Appendix B3, Theorem 20 generalizes Theorem 8. For a proof, the reader is referred there.

**Oracle simplification with partial information.** In Section 11B we derived a no-go result (Theorem 5) for the factorization \( H = H_H \otimes H_{G/H} \) by observing that finding such a factorization is as difficult as finding the hidden subgroup \( H \subseteq G \) itself. With the newly introduced partial information erasure (Promise 7), how do we now quantify the difficulty of finding the transformations \( U_G \) and \( U_S ? \) Put differently: What is the operational significance of the partial information required for the transformations \( U_G \) and \( U_S ? \) The following result answers this question.

**Theorem 9** (Partial information correspondence). The unitaries \( U_G \) and \( U_S \) from Promise 7 can be used to formally construct a new function oracle \( \tilde{O_f} \) which requires \( 2\ell \) fewer qubits than \( O_f \) \((\ell = \log_2 |G|/|K|)\). Moreover, this modified oracle \( \tilde{O_f} \) can still be used to solve the HSP.

With the modified oracle \( \tilde{O_f} \) the HSP algorithm can be run on \( 2\ell \) fewer qubits than with \( O_f \). Both the main and auxiliary qubits can be reduced by \( \ell \) and in comparison to the circuit in Figure 4 the quantum Fourier transform on the main register is now implemented for the group \( K \) instead of \( G \). Details for the proof of Theorem 9 are in Appendix C. The two constructions we made are thermodynamically equivalent: For the circuit in Figure 4 we have an average work cost of erasure equal \((m - 2\ell)k_B T \ln 2\) due to an erasure of \( \ell \) auxiliary qubits which were fully entangled to the main register. In the simplified algorithm using modified oracle from Figure 5 \( 2\ell \) fewer qubits are required to run, hence, the average work cost of erasure is also \((m - 2\ell)k_B T \ln 2\). The two constructions also produce the same computational output; in Appendix C it is shown that the construction for Theorem 9 given in the circuit of Figure 5 is sufficient for
finding the hidden subgroup $H$. The simplification due to the modified oracle $\tilde{O}_f$ (see Figure 5) can be categorized in two ways:

1. $O_f$ is given as a black box: The simplification $\tilde{O}_f$ is a formal construction of an existence result.

2. $O_f$ is given with open circuit access: The transformations $U_G$ and $U_S$ can be incorporated into the oracle $O_f$, and the new oracle requires $2\ell$ fewer physical qubits.

C. Special cases of the hidden subgroup problem

1. Toy example with period finding

In this simple example, the on-the-go erasure protocol is straightforward. The period finding algorithm (PFA) is concerned with the following problem, which is a special case of the HSP:

**Problem 10** (Period finding problem). *Given a function $f: \mathbb{Z}_N \rightarrow \mathbb{Z}_M$ which is $r$-periodic and injective on each period of length $r$, the goal is to find $r$.*

The quantum algorithm solving this problem is of the same form as the HSP algorithm, with $G = \mathbb{Z}_N$, $S = \mathbb{Z}_M$ and $Q_G$ replaced by the standard quantum Fourier transform $Q_N$. The main register uses $n = \log_2 N$ and the auxiliary register uses $m = \log_2 M$ qubits. After the first two steps the quantum state of main and auxiliary register equals

$$\rho_{GS} = \frac{1}{N} \sum_{i,j=0}^{N-1} |i, f(i)\rangle \langle j, f(j)|_{GS}. \quad (21)$$

Suppose we were in possession of partial information about the function $f$, in form of a promise.

**Promise 11.** *The function $f$ can be written in the form $f(2x+1) = 2f(x)(+1)$, for some other function $\tilde{f}: \mathbb{Z}_{N/2} \rightarrow \mathbb{Z}_{M/2}$. In particular, it maps even numbers to even numbers and odd to odd.*

This example was first proposed in [18] and it is a special case of Promise 7; here, we go through the calculations of the optimized on-the-go erasure (Figure 6), and provide an explicit simplification of the function oracle (Figure 6b). First of all, if $f$ maps even to even numbers and odd to odd, the least significant qubits of main and auxiliary register in Eq. (21) are always fully entangled. By reordering them, we can write

$$\rho_{GS} = \frac{1}{N/2} \sum_{i,j=0}^{N/2-1} |i, \tilde{f}(i)\rangle \langle j, \tilde{f}(j)|_{G^{(1)}S^{(1)}} \quad (22)$$

$$\otimes \frac{1}{2} \left( \sum_{k,\ell=0}^{M-1} |kk\rangle \langle \ell\ell|_{G^{(2)}S^{(2)}} \right) \quad (23)$$

and apply the result from Lemma 1 to the Bell state $|\chi\rangle$. Since the reduced main register is unaffected by this erasure, the algorithm still works to determine the period.
FIG. 5. If we have access to partial information about a subgroup $K$, the modified oracle $\tilde{O}_f$ (violet box in the circuit above) can be used instead of the original oracle $O_f$. The $2\ell$ qubits inside the violet box are in the $|0\rangle$ state regardless of the input of the main and auxiliary qubits. All in all, the oracle $\tilde{O}_f$ has $2\ell$ fewer (variable) input qubits than $O_f$. If the function oracle $O_f$ is given with open circuit access (in contrast to a black box), the transformations $U_G$ and $U_S$ can be incorporated into $O_f$, giving a physical reduction of $2\ell$ qubits. In comparison to the standard algorithm (Figure 2), the group $G$ has been replaced by $K$, henceforth, also the generalized quantum Fourier transforms $Q_G$ had to be replaced by $Q_K$. The remaining steps are as in Figure 2 in the following enumeration they are grayed out, while steps 2a’ - 2c’ are encapsulated by $\tilde{O}_f$ in the above circuit:

1. Generalized quantum Fourier transform $Q_K$ on $H_K$.
2a’. Inverse transformation $U_G^\dagger$ on $H_K \otimes H_{G/K}$,
2b’. Original oracle operation $O_f$,
2c’. Transformations $U_G \otimes U_S$,
3 - 4. Generalized quantum Fourier transform $Q_K$ on $H_K$, and measurement of $K$ register.

This problem can be rephrased as a HSP (see [23] for a pedagogical derivation) by introducing the group $G = \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ and a function

$$f : G \rightarrow S; (i, j) \mapsto \gamma^i A^{-j}.$$  \hspace{1cm} (25)

The function $f$ is a homomorphism of groups: Let $(i, j), (k, \ell) \in G$, then

$$f((i, j) + (k, \ell)) = f(i + k, j + \ell) = \gamma^i \gamma^k A^{-j-\ell} = \gamma^i \gamma^k A^{-j} A^{-\ell} = f(i, j) f(k, \ell).$$  \hspace{1cm} (27)

The discrete logarithm is now solved by finding the hidden subgroup $H = \langle \langle (a, 1) \rangle \rangle \subseteq G$. In this formulation, the on-the-go erasure protocol is again applicable, given that partial information in the form of Promise 7 is available. This could again be the case in form of an intermediate subgroup $H \subseteq K \subseteq G$.

IV. DISCUSSION

Summary. In the resource theory of thermodynamics we optimized the erasure costs of erasing auxiliary qubits in the algorithms solving the HSP. To achieve this, we applied the result from [15], which states that quantum side-information in the form of entanglement can be used as a resource to reduce the cost of erasing quantum systems. Lastly, we quantified the cost of using said side-information in terms of a trade-off: the side-information

2. Discrete logarithm problems

Another special case of the HSP is the discrete logarithm problem, which has applications in classical public-key cryptography.

Problem 12 (Discrete logarithm problem). Given the cyclic group $S = \{1, \gamma, \ldots, \gamma^{N-1}\}$ of order $N$ with generator $\gamma$ and some element $A \in S$. The question is which $a \in \mathbb{Z}/N\mathbb{Z}$ satisfies $\gamma^a = A$. 

r. In this case, the local unitary operations $U_G$ and $U_S$ with the purpose to compress the entanglement between main and auxiliary register into well defined qubits can be chosen to be trivial, $U_G = 1_G$ and $U_S = 1_S$ (Figure 6a). Ultimately, the reason for this was that (part of) the entanglement was between well-known qubits: the least significant ones. In general, however, this cannot be assumed to be the case.

How much worth is the partial information in Promise 11 in terms of computational complexity? An alternative usage of the partial information is to run the PFA not for the function $f : \mathbb{Z}_N \rightarrow \mathbb{Z}_M$ but rather $\tilde{f} : \mathbb{Z}_{N/2} \rightarrow \mathbb{Z}_{M/2}$ with $\tilde{f}(x) = f(2x)/2$. This algorithm requires 2 fewer qubits to run. Operationally, we simply don’t let the PFA act on the least significant qubits, we replace the quantum Fourier transform $Q_N$ by $Q_{N/2}$ and we let the function oracle act on all but the least significant qubits (Figure 6b).

2. Discrete logarithm problems

Another special case of the HSP is the discrete logarithm problem, which has applications in classical public-key cryptography.

Problem 12 (Discrete logarithm problem). Given the cyclic group $S = \{1, \gamma, \ldots, \gamma^{N-1}\}$ of order $N$ with generator $\gamma$ and some element $A \in S$. The question is which $a \in \mathbb{Z}/N\mathbb{Z}$ satisfies $\gamma^a = A$. 

This problem can be rephrased as a HSP (see [23] for a pedagogical derivation) by introducing the group $G = \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ and a function

$$f : G \rightarrow S; (i, j) \mapsto \gamma^i A^{-j}.$$  \hspace{1cm} (25)

The function $f$ is a homomorphism of groups: Let $(i, j), (k, \ell) \in G$, then

$$f((i, j) + (k, \ell)) = f(i + k, j + \ell) = \gamma^i \gamma^k A^{-j-\ell} = \gamma^i \gamma^k A^{-j} A^{-\ell} = f(i, j) f(k, \ell).$$  \hspace{1cm} (27)
FIG. 6. Two-qubit optimizations to the period finding algorithm. (6a) Here, the circuit describing the optimized on-the-go erasure of the least significant qubits in the period finding algorithm is shown. Given the promise that the function $f$ maps even numbers to even numbers, the oracle $O_f$ fully entangles the least significant qubits of main and auxiliary register. The auxiliary qubit of this pair can then be erased at a negative average work cost of $-k_B T \ln 2$ if the erasure is performed at temperature $T$. (6b) At equivalent thermodynamic costs, the period finding algorithm can alternatively be simplified to an algorithm which uses 2 qubits fewer by keeping the least significant qubits of main and auxiliary register constantly in the ground state $|0\rangle$.

could be used to reduce the algorithm width, at equal thermodynamic costs.

**Applicability.** Our work has treated three possibilities to erase auxiliary qubits in a quantum algorithm. When considering our proposal for an optimized on-the-go erasure of $\ell$ qubits for application, the following costs have to be weighted against each other. On-the-go erasure versus:

1. **Straightforward erasure:** Given the architecture of the quantum computer, does the work cost reduction by $2k_B T \ln 2$ outweigh the gate costs of the local unitaries $U_G$ and $U_S$?

2. **Bennett’s uncomputing:** What restrictions does the quantum computer put on the algorithm’s width and what is the gate cost of implementing many parallel copies of the original circuit together with a quantum version of the classical post-processing and a reversible majority vote compared to the gain of $(m - 2\ell)k_B T \ln 2^2$. Considering current gate costs or even fundamental limits [10], this method is unlikely to yield a thermodynamic advantage in any practical scenario.

The toy example for the PFA demonstrates that there are cases where the local transformations $U_G$ and $U_S$ are trivial, hence they do not add any complexity to the algorithm, giving the optimized on-the-go erasure a strict advantage over approaches (1) and (2). Last but not least, the optimized on-the-go erasure has to be compared to another option:

3. **Oracle simplification:** Is $O_f$ given with open circuit access or is it given as a black box?

If the oracle is available with open circuit access, the simplification comes with a decrease of complexity, making the algorithm use 2 fewer qubits. For a black box, the complexity is roughly the same, with the difference coming from the quantum Fourier transform which has to be performed on $\ell$ fewer qubits. At the level of thermodynamic costs, both options are equivalent.

**Complexity implications.** Depending on the type of partial information available to perform the on-the-go erasure, the complexity of the transformations $U_G$ and $U_S$ can range from being exponential in the input size to being almost trivial. The reason for this is that Theorem 8 (together with Promise 7) is an existence result
and the complexity of the transformations depends on the particular choice of computational basis representation of the states $|g\rangle$ and $|s\rangle$, for $g \in G$ and $s \in S$ respectively. In the scenario, where we have access to side information in the form of an intermediate subgroup $K$, such that $H \subseteq K \subseteq G$, there is no a priori reason for the Hilbert space $\mathcal{H}_K = \text{span}_C\{|k\rangle : k \in K\}$ to be represented by a subregister of qubits of the main register $\mathcal{H}_G$. In the most general case, a unitary transformation is required to permute basis elements and ensure $\mathcal{H}_K$ is encoded on a subset of qubits of the main register. This transformation (which in matrix form only has 0 and 1 elements) has exponential gate complexity $O(n^2k)$ \cite{3}, in the general case. This is not to say that the transformations $U_G$ and $U_S$ cannot be implemented efficiently. There are cases where the computational basis representation for $G$ already ensures that $\mathcal{H}_K$ is implemented on a subset of the main register’s qubits. In these cases, $U_G$ only has to permute qubits and has thus gate complexity bounded by $O(\log |K|)$. For example, in the PFA, this is the case for all subgroups of $G = \mathbb{Z}/N\mathbb{Z}$ generated by powers of 2 (Section 11C1), and for the discrete logarithm for all subgroups of $G = \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ of the form $\langle \langle 2^k \rangle \rangle \times \mathbb{Z}/N\mathbb{Z}$ (Section 11C2). For the transformation $U_S$ to satisfy similar complexity bounds, the target space’s computational representation has to be decomposed analogously to the main register; this is discussed in more detail in Appendix A2.

**Outsourcing thermodynamic processes to an information battery.** In this presentation, all qubit erasure processes take place in the computational registers. It is possible to outsource this thermodynamic task to an external battery register \cite{723}. The battery consists of fueled qubits in state $|0\rangle$ and depleted qubits in the fully mixed state $1/2$; the erasure of depleted qubits takes place there at temperature $T$, with an average work cost of $k_B T \ln 2$ per qubit. The idea is that when we identify pure or fully mixed qubits that need erasure, we exchange them with those in the battery. That way, all thermodynamic processes that require interaction with an environment are take place in the battery, protecting the main registers from dissipation. The price of using a battery is the need for additional SWAP gates between the computational registers and the battery, which depending on the hardware architecture may be costly. Since the information battery does not have an effect on the number of qubits that need to be erased in a quantum computation, further discussion is outsourced to Appendix A2.

**Relation to algorithmic cooling.** Algorithmic cooling is the process of producing cold (that is, approximately pure) qubits \cite{303}. There are approaches that extract entropy from a target system by coupling it to thermal baths in an approach called heat-bath algorithmic cooling \cite{253,313}. Our optimizations in erasure distinguish themselves from algorithmic cooling in that they are not primarily about the production of pure qubits but rather about reducing the thermodynamic cost of said erasure using entanglement as a further resource. When outsourcing the erasure process into an external information battery (see Appendix A2), one could apply algorithmic cooling there to produce pure battery states.

**Single-shot and finite-size effects.** In our analysis, we have simplified the work cost of erasing a single qubit. Using the von Neumann entropy to quantify the work cost of erasure is an approximation valid in the asymptotic i.i.d. limit; for any finite number of rounds smooth entropies are more precise measures of work and heat in erasure \cite{18,39}. If the rest Hamiltonian of the qubits is not fully degenerate, one needs to employ single-shot versions of the free energy \cite{40}; if we want to account for finite-size effects (either on the environment, on thermalizing operations, or energy gaps allowed in intermediate stages of erasure), further corrections are necessary to find the exact work cost as a random variable \cite{41,42}. All these corrections can be applied on top of our results: as mentioned in the introduction, our focus is minimizing the number of qubits that need to be erased through interaction with a thermal environment. The exact cost of that erasure can then be computed in the appropriate regime using some of the corrections above; which ones are relevant depends on the hardware architecture. Similarly, the hardware will determine the actual thermodynamic cost of individual unitary gates, which affects the calculation of whether is better to perform erasure on-the-go or to simplify the circuit.

**Open questions.** A natural follow-up project is to study on-the-go erasure for arbitrary quantum algorithms. Within this setting, one could attempt to generalize the no-go result and the trade-off found in this paper for the HSP algorithm. In that general setting it would also be interesting to explore automatization of the search for optimized erasure (or algorithm simplification) points, for example using entanglement detection \cite{43,44}, without affecting the state of the main register.

**Acknowledgements**

We thank Marcus Huber for discussions and feedback, and we also thank the anonymous referees from PRA for helping us to improve the manuscript. FM acknowledges the SEMP scholarship from Movetia for his research stay abroad and the stipend from the QUIT group at TU Vienna. LdR acknowledges support from the Swiss National Science Foundation through SNSF project No. 200020_165843, from the Quantum Center of ETH Zurich, and from the FQXi large grant RFP-CPW-2009 Consciousness in the Physical World. This paper is the result of FM’s semester project as a masters student. The technical contributions (including proofs and algorithm proposals) and first draft of the paper are his. LdR proposed the original idea, supervised the project, and revised the manuscript.
Appendix A: Physics background: erasure and information battery

This first appendix is dedicated to providing an explicit protocol for erasing a fully mixed qubit at the Landauer limit (Appendix A.1) and to review the basics of an information battery in quantum computing (Appendix A.2).

1. Explicit thermodynamic protocol for erasure of a fully mixed qubit

Erasing a fully mixed qubit, that it mapping $1/2 \mapsto |0\rangle\langle 0|$ comes with diverging resource costs by the third law of thermodynamics [15-17] which has been established in quantum thermodynamics as well, with diverging resource costs being time, energy or control complexity [16, 48, 49]. Here we showcase a protocol [20] which asymptotically implements the erasure of a qubit. The erasure unitary operation implementing this step is

$$U^{(\ell)} = \sum_{k \in \mathbb{Z}} \left\{ |E_{k+\ell}, 1\rangle \langle E_k, 0|_S + |E_k, 0\rangle \langle E_{k+\ell}, 1|_S \right\} \otimes 1_{i\neq \ell}$$

and it commutes with the Hamiltonian of the joint system of the work storage, qubit and heat bath. The energy level diagram in Figure 7 (adapted from [20]) visualizes this unitary operation for $\ell = 3$.

The erasure process is the composition $U = U^{(N)} \cdots U^{(2)} U^{(1)}$. With the initial state

$$\rho_i = |E_0\rangle \langle E_0| \otimes \frac{1_S}{2} \otimes \tau(\beta),$$

the erasure $U$ acts on $\rho_i$ such that after the erasure we are left with the reduced state of the $S$ register

$$\text{Tr}_{B, \text{bath}} (U \rho_i U^\dagger) \propto (|0\rangle \langle 0|_S + e^{-N\beta \Delta} |1\rangle \langle 1|_S).$$

For a large number $N$ of heat bath qubits, this process corresponds to an erasure of the qubit in system $S$: The fully mixed state $1_S/2$ is mapped to $|0\rangle \langle 0|_S$ asymptotically as $N \to \infty$. In this process, the work storage performs a work of $W = k_B T \log 2$ for the erasure which is dissipated as heat into the bath. In the more general case, where the system qubit is not necessarily a fully mixed state but rather $\rho_S = (1-p)|0\rangle \langle 0|_S + p|1\rangle \langle 1|_S$, the erasure unitary $U$ can be truncated which leads to a lower erasure cost of $W(S) = H(S) k_B T \log 2$ with $H(S)$ the von Neumann entropy of the system $S$. This is an explicit realization of the result from [18] for a single qubit.

2. Using an information battery inside the quantum computer

Qubit battery registers. For the purpose of this work it suffices to consider two types of battery registers: One
FIG. 7. Qubit erasure energy diagram. Energy level diagram for the erasure setup of one qubit. From left to right are work storage, qubit system and heat bath. The curved arrows visualize the swapping operation done by the unitary $U^{(3)}$ from Eq. (A1).

The second register $\mathcal{H}_B^{(\text{depleted})}$, containing only fully mixed qubits

$$\rho_B^{(\text{depleted})} = \left(\frac{1}{2}\right)^{\dim B^{(\text{depleted})}},$$

which are completely passive [50, 51], that is, there exists no unitary operation extracting energy from such a state. The second register $\mathcal{H}_B^{(\text{fueled})}$ contains only pure qubits,

$$\rho_B^{(\text{fueled})} = (|0\rangle\langle 0|) \otimes \dim B^{(\text{fueled})}.$$  (A4)

Using a thermal reservoir at temperature $T$ it is at best possible to extract $k_B T \ln 2$ work from a fueled qubit. In our modifications to the HSP algorithm, instead of partially erasing Bell pairs in the computational registers, we swap them with a fully mixed and a pure qubit from the battery $\mathcal{H}_B = \mathcal{H}_B^{(\text{depleted})} \otimes \mathcal{H}_B^{(\text{fueled})}$,

which amounts to a gain of one pure (fueled) qubit in the information battery.

Extraction by Swapping. If the entanglement between the main register $G$ and the auxiliary register $S$ is given by fully entangled qubits, for example in the Bell state $|\chi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, then this state can be replaced by fully mixed qubit for $G$ and a pure qubit for $S$ via a swapping operation. On the reduced $\mathcal{H}_G \otimes \mathcal{H}_S$ register, this is equivalent as a partial erasure of the qubit from $S$, while preserving $G$.

General Bell pair extraction. In general one is not lucky enough for the entanglement between main and auxiliary register to be given in the form of well defined Bell pairs. Since local unitary transformations of $G$ and $S$ respectively preserve the conditional entropy between these two registers, the entanglement can be spread across many qubits. For the class of algorithms solving the HSP, we have shown that there always exist local unitaries $U_G$ and $U_S$ such that $\rho_G \otimes |\chi\rangle$ is mapped to $\rho_G \otimes |\chi\rangle/\sqrt{2}$, the reduced states of the main register $\bar{\rho}_G = Tr_S(\rho_G)$ is the same as before the operation, $\rho_G = \bar{\rho}_G$, where $\rho_G = Tr_S(\rho_G)$.

Appendix B: Proofs: On-the-go erasure in the Hidden Subgroup Problem

In Appendix B.1 we revise the group theoretic basics of the HSP, then in B.2 we go through a step-by-step calculation the unmodified quantum algorithm solving the HSP, lastly in B.3 we deliver the proofs for the theorems of the main body of the paper.

1. Group theory of the Hidden Subgroup Problem

In this section an online erasure protocol is constructed for the quantum algorithm [23] of the Hidden Subgroup Problem (abbr. by HSP).
Problem 2 (Hidden Subgroup Problem [22]). Let $G$ be a finite group, $S$ some finite set and $f : G \to S$ a function. Given the existence of a subgroup $H \subseteq G$ such that for all $g, g' \in G$

$$f(g) = f(g') \iff gH = g'H,$$  \hspace{1cm} (10)

the goal is to determine $H$.

From now on, $G$ shall be an Abelian group. The HSP for general non-Abelian groups does not yet have an efficient quantum algorithm [22]. We diverge from the notation in Eq. (10) and denote by $g + h \in G$ the element in $G$ obtained by the additive group operation on $g$ and $h$ in $G$. The unit element is 0. In particular, the cosets with respect to some subgroup $H \subseteq G$ are from now on denoted by $g + H \in G/H$. We present important definitions and results from group theory [52] and representation theory [53] which will be used in the following discussion (formulation and notation of the results from [52, 53] has been adapted to the specific setting of the HSP at hand).

Theorem 13 (Classification of finite Abelian groups [52]). For any finite Abelian group $G$ there exist positive integers $a_1, \ldots, a_m \in \mathbb{N}$ such that

$$G \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_m\mathbb{Z}$$  \hspace{1cm} (B1)

and $a_1 | a_2 | \cdots | a_m$, where $a_i$ for all $1 \leq i \leq m$ and $m$ are uniquely determined.

Proposition 14 ([53]). For each $0 \leq k \leq a - 1$, the function $\chi_k : \mathbb{Z}/a\mathbb{Z} \to S^1$ declared by $\chi_k(\ell) = e^{2\pi ik\ell/a}$ is a character of the irreducible representation

$$\rho_k : \ell \in \mathbb{Z}/a\mathbb{Z} \mapsto \omega_{a_k}^\ell \in \mathbb{C}^*$$  \hspace{1cm} (B2)

of the cyclic group $\mathbb{Z}/a\mathbb{Z}$. In fact, these are all characters of irreducible representations of $\mathbb{Z}/a\mathbb{Z}$.

Proposition 15 ([53]). The characters of $G \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_m\mathbb{Z}$ (c.f. Theorem 13) are given by

$$\chi_g(h) = \chi_{g_1}^{(a_1)}(h_1) \chi_{g_2}^{(a_2)}(h_2) \cdots \chi_{g_m}^{(a_m)}(h_m),$$  \hspace{1cm} (B3)

where the factors are as in Proposition 14 and elements $g, h \in G$ are understood as in the decomposition of $G$ into cyclic factors. The irreducible representation $\rho_g$ having $\chi_g$ as character is given by the product $\rho_g = \rho_{g_1} \cdots \rho_{g_m}$, with the factors as in Eq. (B2).

Remark. In this special Abelian case the following basic properties are satisfied by the character $\chi_g$ as introduced in Proposition 15. For any $g, h \in G : \chi_g(h) = \chi_h(g)$ and if we take another $g' \in G$ the characters act as group homomorphisms $\chi_h(g + g') = \chi_h(g)\chi_h(g')$. However, this is only true for characters of one-dimensional irreducible representations and does not hold in general.

Theorem 16 (First orthogonality relation of characters (abelian version) [53]). Let $g, g' \in G$ be elements of the Abelian group $G$. In the space of functions $G \to \mathbb{C}$ the two characters $\chi_g, \chi_{g'}$ of irreducible representations of $G$ are orthonormal

$$\langle \chi_g, \chi_{g'} \rangle = \frac{1}{|G|} \sum_{h \in G} \chi_g(h) \chi_{g'}(h) = \delta_{gg'},$$  \hspace{1cm} (B4)

The characters are defined as in Proposition 15.

A reformulation of the quantum Fourier transform for states representing elements of $G$ can be given in terms of characters. Consider again the cyclic group $\mathbb{Z}/a\mathbb{Z}$, pick some $k \in \mathbb{Z}/a\mathbb{Z}$ and define

$$|\chi_k(a)\rangle = \frac{1}{\sqrt{a}} \sum_{\ell=0}^{a-1} \omega_a^{k\ell} |\ell\rangle = \frac{1}{\sqrt{a}} \sum_{\ell=0}^{a-1} \chi_k(\ell) |\ell\rangle.$$  \hspace{1cm} (B5)

Indeed this is the quantum Fourier transform, where we used the abbreviation $\omega_a = e^{2\pi i/a}$ for the $a$-th root of unity. A generalization is given by

Definition 17 (Quantum Fourier transform of a group register [23]). Let $G$ be a finite Abelian group with decomposition as in Theorem 13. For any $g \in G$ the character state $|\chi_g\rangle$ is declared by

$$|\chi_g\rangle = \frac{1}{\sqrt{|G|}} \sum_{h \in G} \chi_g(h) |h\rangle,$$  \hspace{1cm} (B6)

the functions $\chi_g, g \in G$ as in Proposition 15.

In the algorithm solving the HSP from Figure 2, states will be transformed according to the rule in Eq. (B6) and certain summands will cancel out according to Theorem 16. The following subgroup will be of particular interest to us

$$H^\perp = \{ g \in G : \forall h \in H : \chi_g(h) = 1 \}.$$  \hspace{1cm} (B7)

Elements of $H^\perp$ define functions, their characters, which allow us for probing the subgroup $H$.

2. The standard algorithm solving the (Abelian) HSP

Before going into the procedure of how the online era- sure in the algorithm for the HSP works we explain in this section the quantum algorithm which solves the HSP (adapted from [22, 23], originally solved by [26]). We will only work out the case where $|G|$ and $|S|$ are powers of 2 in order to avoid approximations which are needed in the more general case. The $G$ register shall be made up of the first $n = \log_2 |G|$ qubits, the $S$ register consists of the next $m = \log_2 |S|$ qubits. For (later) notational convenience, we refer to the ground state of the $G$ register as $|0\rangle_G$ and as that of the $S$ register as $|0\rangle_S$. If clear from the context, subscripts indicating the register are dropped. We explicitly calculate the protocol from the circuit in Figure 2 from the main part of the paper.
Step 1. Denote by $\rho_\ell$ the density matrix of the joint $G$ and $S$ register after iteration step $\ell$ in the HSP algorithm, in particular $\rho_0 = |0\rangle\langle 0| \otimes |e\rangle\langle e|$. The first steps of the algorithm

$$
\rho_0 \xrightarrow{(1)} \sum_{g,g'\in G} |g\rangle\langle g'| \otimes |0\rangle\langle 0| = \rho_1,
$$

where we used $\chi_0(g) = 1$ for all $g \in G$.

Step 2. Oracle Operation:

$$
\rho_1 \xrightarrow{(2)} \sum_{g,g'\in G} |g\rangle\langle g'| \otimes |f(g)\rangle\langle f(g')|
$$

$$
= \frac{1}{|G|} \sum_{g,g'\in G} \sum_{h,h'\in H} |g+h\rangle\langle g+h'| \otimes |f(g)\rangle\langle f(g')| = \rho_2.
$$

In the Eq. (B12) we used that the choice of representative of $g$ in $\bar{g} = g + h \in G/H$ doesn’t affect the inner summation and that $f(g) = f(g')$ if and only if $\bar{g} = g'$. At this stage the $S$ register is traced out

$$
\rho_2 = \text{Tr}_S \rho_2 = \frac{1}{|G|} \sum_{g,g'\in G/H} \sum_{h,h'\in H} |g+h\rangle\langle g+h'|.
$$

Step 3 - 4. The remaining two steps are performed on the reduced $G$ register. The states will be denoted by a dash $\rho'$. 

$$
\rho_2 \xrightarrow{(3)} \sum_{\bar{g} \in G/H} \sum_{h,h'\in H} \chi_{\bar{g}+h} \chi_{\bar{g}+h'}
$$

$$
= \left( \frac{|H|}{|G|} \right)^2 \sum_{\bar{g} \in G/H} \sum_{\bar{g},\bar{g}' \in H} \chi_{\bar{g}} \chi_{\bar{g}'} = \rho_3
$$

The measurement result of the $G$ register gives an element $\bar{g} \in H^\perp$. This element defines the function $\chi_{\bar{g}} : G \rightarrow S^1$ whose restriction to $H$ is the unit function. For all $h \in H$, $\chi_{\bar{g}}(h) = 1$. Multiple iterations of the HSP algorithm give a set of such functions $\{ \chi_{\bar{g}} \}$ constraining $H \subseteq G$ and thus solving the problem.

3. Proofs

**Theorem 3** (Entanglement upper bound). For an Abelian group $G$ with hidden subgroup $H$ and indicator function $f : G \rightarrow S$ as in Problem 2, solved by the algorithm from the circuit in Figure 2, the maximal number $\ell_{\text{max}}$ of Bell pairs between main and auxiliary registers that can be obtained via local unitary operations is

$$
\ell_{\text{max}} = \log_2 \left| \frac{|G|}{|H|} \right| = -H(S|G)_{\rho_{GS}},
$$

where $\rho_{GS}$ is the state of the computational registers after the oracle operation $O_f$.

**Proof.** The measure we use to quantify the degree of entanglement between the $G$ and $S$ register is the conditional von Neumann entropy

$$
H(S|G) = H(\rho_{GS}) - H(\rho_G),
$$

where $H$ is the standard von Neumann entropy [28, 30]. The number of Bell pairs formed by qubits from $G$ and $S$ will be upper bounded by $-H(S|G)$ as a single bell pair contributes a negative conditional entropy of $-1$. The joint state of $\mathcal{H}_G \otimes \mathcal{H}_S$ is $\rho_{GS}$ and $\rho_G = \text{Tr}_S \rho_{GS}$ is the reduced state of the $G$ register. Observe the following two facts: Firstly, up until the erasure of the $S$ register which takes place after step 2 in the HSP algorithm, the joint state $\rho_{GS}$ is a pure state. Secondly, we have $\rho_{GS} = \rho_G \otimes \rho_S$ before step 2 where the function oracle is applied, where $\rho_G$ and $\rho_S = |0\rangle\langle 0|$ are pure states. Assuming that the function oracle $O_f$ is a black box, the only stage of the HSP algorithm where $H(S|G)$ is non-zero is after $O_f$ but before the $\mathcal{H}_S$ is traced out. The corresponding state from Eq. (B12) is

$$
\rho_{GS} = \frac{1}{|G|} \sum_{\bar{g},\bar{g}' \in G/H} \sum_{h,h' \in H} |g+h\rangle\langle g+h'| \otimes |f(g)\rangle\langle f(g')|,
$$

whose conditional entropy $H(S|G)$ is given by

$$
H(S|G) = H(\rho_{GS}) - H(\rho_G) = 0 + \text{Tr}(\rho_G \log_2 \rho_G),
$$

with $\rho_G = \rho'_2$ the reduced $G$ register state, c.f. Eq. (B13). The entropy measure is invariant under unitary transformations of $\rho_G$. By reordering the computational basis of the $G$ register we can split $\mathcal{H}_G \cong \mathcal{H}_H \otimes \mathcal{H}_{G/H}$. The state $\rho_2$ can be factored $\rho_2 \cong \rho_H \otimes \rho_{G/H} \rho_2$

$$
\frac{1}{|G|} \sum_{\bar{g} \in G/H} \sum_{h,h' \in H} |g+h\rangle\langle g+h'| \cong \frac{1}{|H|} \sum_{h,h' \in H} |h\rangle\langle h'| \otimes \frac{|H|}{|G|} \sum_{\bar{g} \in G/H} |g\rangle\langle g|.
$$

The factor $\rho_H$ is a pure state of $\mathcal{H}_H$, the right one $\rho_{G/H}$ is a mixed state in $\mathcal{H}_{G/H}$, already represented in it’s diagonal basis with eigenvalues $|H|/|G|$. The entropy of
This transformation will be denoted by $U$. This operation is unitary and can be chosen such that $H$ can be factored out by reordering the computational basis for the HSP in Eq. (10), it suffices to restrict to representatives $g$ of cosets $\bar{g} \in G/H$. Generally, the ancillary register $H_S$ may have more qubits than are actually needed to represent im$f \subseteq S$. This overhead of qubits can be factored out by reordering the computational basis of $H_S$ such that $|f(g)\rangle \rightarrow |0\rangle \otimes |\tilde{f}(g)\rangle \in H_S^{(1)} \otimes H_S^{(2)}$. This operation is unitary and can be chosen such that for all representatives $g$, the states $|f(g)\rangle \in H_S^{(1)}$ and $|g\rangle \in H_G$ have the same computational representation. This transformation will be denoted by $U_S$. 

**Theorem 5** (No-go for saturating the bound). Any on-the-go erasure protocol applying local unitaries $U_G$ and $U_S$ to factorize the maximum amount $\ell_{\text{max}}$ of Bell pairs from Theorem 3 can be used to solve the HSP.

**Proof.** Any local unitary $U_G$ factoring the main register register $H_G$ into $H_H \otimes H_G/H$ can in fact be used to determine $H \subseteq G$. Elements in $H$ can be obtained by applying the inverse $U_G^\dagger$ to states in $H_H \otimes H_G/H$. Pick some $g \in G$, then $U_G$ factors the state $|g\rangle$ into two parts

$$U_G|g\rangle = |h_g\rangle \otimes |[g]\rangle.$$  

(B28)

Despite our ignorance about how the group structure is binarily encoded in the quantum registers $H_H$ and $H_G/H$, we know that for any $h \in H$, $|[g]\rangle = |[g + h]\rangle$. Elements from $H$ can then be obtained in two steps

1. Determine $|[0]\rangle \in H_H/H$ by computing $U_G|0\rangle = |h_0\rangle \otimes |[0]\rangle$.  
2. Pick any $|h\rangle \in H_H$ and deduce $|h\rangle_G \in H_G$ via

$$U_G^\dagger|h\rangle \otimes |[0]\rangle = |h\rangle \in H_G.$$  

(B29)

In the second step the register $H$ and $G$ is highlighted for the states $|h\rangle_H$ and $|h\rangle_G$. That is because for $H_H$, we have access to an encoding $g \in G \rightarrow |g\rangle \in H_G$ while for $H_H$ we do not. That is also the reason why one has to use the inverse operation $U_G^\dagger$ to obtain $H$. As with the functions $\chi_S$ from the standard algorithm solving the HSP in Appendix B, this procedure can be used to determine a small number of elements $h \in H$ which then generate the whole subgroup $H$.

In fact one can even go further: Finding an on-the-go erasure procedure in the setting of Theorem 5 is even more difficult than solving the HSP, for that it also requires the transformation $U_S$. For partial information erasure procedures we give a quantitative description of how much information is required to compress the entanglement for an on-the-go erasure.

**Definition 18** (General local transformations of $G$ and $S$). Define local transformations

$$U_G : H_G \rightarrow H_H \otimes H_G/H$$  

(B26)  

$$U_G : H_G \rightarrow H_H \otimes H_G/H.$$  

(B27)

The relevant states in the ancillary register $H_S$ are of the form $|f(g)\rangle$ for $g \in G$. In fact, by the very defining assumption for the HSP in Eq. (10), it suffices to restrict to representatives $g$ of cosets $\bar{g} \in G/H$. Generally, the ancillary register $H_S$ may have more qubits than are actually needed to represent im$f \subseteq S$. This overhead of qubits can be factored out by reordering the computational basis of $H_S$ such that $|f(g)\rangle \rightarrow |0\rangle \otimes |\tilde{f}(g)\rangle \in H_S^{(1)} \otimes H_B$. This operation is unitary and can be chosen such that for all representatives $g$, the states $|f(g)\rangle \in H_B$ and $|g\rangle \in H_G/H$ have the same computational representation. This transformation will be denoted by $U_S$. 

Similarly to the notation introduced in Eq. (B23), let us write for some state $|f(g)\rangle \in H_S$, $U_S|f(g)\rangle = |f^{(1)}(g), f^{(2)}(g)\rangle$. Using this notation we can formulate two general conditions on transformations $U_G$ and $U_S$:

**Theorem 19** (General characterization of partial erasure transformations). If and only if the transformations $U_G$ and $U_S$ satisfy the two requirements

1. For all $g, \bar{g} \in G : f(g) = f(\bar{g}) \rightarrow g^{(2)} = \bar{g}^{(2)}$, 

2. For all $g, \bar{g} \in G : f(g) = f(\bar{g}) \rightarrow g^{(1)} = \bar{g}^{(1)}$, 

3. For all $g, \bar{g} \in G : f(g) = f(\bar{g}) \rightarrow g^{(2)} = \bar{g}^{(2)}$, 

4. For all $g, \bar{g} \in G : f(g) = f(\bar{g}) \rightarrow g^{(1)} = \bar{g}^{(1)}$, 

5. For all $g, \bar{g} \in G : f(g) = f(\bar{g}) \rightarrow g^{(2)} = \bar{g}^{(2)}$, 

6. For all $g, \bar{g} \in G : f(g) = f(\bar{g}) \rightarrow g^{(1)} = \bar{g}^{(1)}$, 

7. For all $g, \bar{g} \in G : f(g) = f(\bar{g}) \rightarrow g^{(2)} = \bar{g}^{(2)}$, 

8. For all $g, \bar{g} \in G : f(g) = f(\bar{g}) \rightarrow g^{(1)} = \bar{g}^{(1)}$.
2. The function $f^{(1)}(g)$ only depends on $g^{(1)}$ and $f^{(2)}(g) = g^{(2)}$ in the binary computational representation in $\mathcal{H}_{G}^{(2)} = (\mathbb{C}^2)^{\otimes k} = \mathcal{H}_{G}^{(2)}$, they can factor out the entanglement in the form of $\ell$ Bell pairs after $O_f$ in the HSP algorithm, where $\ell = \dim \mathcal{H}_{G}^{(2)} = \dim \mathcal{H}_{S}^{(2)}$.

Proof. We obtain conditions on transformations $U_G$ and $U_S$ which allow bringing the joint state of the $G$ and $S$ register into the form
\[
\rho_{GS} \mapsto \rho_{GS} \otimes (|\chi\rangle\langle\chi|)^{\otimes \ell}, \quad (B34)
\]

\[
\rho_{2a} = \left( U_G \otimes U_S \right) \rho_2 \left( U_G \dagger \otimes U_S \dagger \right) = \frac{1}{|G|} \sum_{g,\tilde{g} \in G} |g^{(1)}, g^{(2)}\rangle \langle \tilde{g}^{(1)}, \tilde{g}^{(2)}| \otimes |f^{(1)}(g), f^{(2)}(\tilde{g})\rangle \langle f^{(1)}(g), f^{(2)}(\tilde{g})| \otimes (|\chi\rangle\langle\chi|)^{\otimes \ell}. \quad (B35)
\]

\[
\rho_{2a} = \frac{1}{|G|} \left\{ \sum_{g^{(1)}, \tilde{g}^{(1)}} |g^{(1)}\rangle \langle \tilde{g}^{(1)}| \otimes |f^{(1)}(g^{(1)}), f^{(1)}(\tilde{g}^{(1)})\rangle \langle f^{(1)}(g^{(1)}), f^{(1)}(\tilde{g}^{(1)})| \right\} \otimes (|\chi\rangle\langle\chi|)^{\otimes \ell}. \quad (B36)
\]

\[
\rho_{2a} = \frac{1}{\dim \mathcal{H}_{G}^{(1)}} \left\{ \sum_{g^{(1)}, \tilde{g}^{(1)}} |g^{(1)}\rangle \langle \tilde{g}^{(1)}| \otimes |f^{(1)}(g^{(1)}), f^{(1)}(\tilde{g}^{(1)})\rangle \langle f^{(1)}(g^{(1)}), f^{(1)}(\tilde{g}^{(1)})| \right\} \otimes (|\chi\rangle\langle\chi|)^{\otimes \ell}. \quad (B37)
\]

The necessary and sufficient condition for the transformations $U_G$ and $U_S$ factoring $\ell$ Bell pairs is the equality $\heartsuit$ above.

Remark. The transformations $U_G$ and $U_S$ from Promise [7] where one has partial information on an intermediate subgroup $H \subseteq K \subseteq G$ are a special case of the transformations from Theorem [19] with

\[
\mathcal{H}_{G}^{(1)} = \mathcal{H}_{K}, \quad \text{and} \quad \mathcal{H}_{G}^{(2)} = \mathcal{H}_{G/K}, \quad (B40)
\]

as this decomposition satisfies all two assumptions from Theorem [19].

Theorem 20 (Work cost of erasure with partial information, general version). Given the transformations $U_G$ and $U_S$ from Definition [28] and Theorem [29] there exists an on-the-go erasure protocol acting on $G$, $S$ and an environment at temperature $T$, resetting the auxiliary register $S$ after $O_f$ while preserving $G$ which does not exceed an average work cost of erasure of

\[
W = (m - 2\ell)k_B T \ln 2, \quad (B41)
\]

where $\ell = \log_2(\dim \mathcal{H}_{G}^{(2)})$.

Proof. This result follows from the form of the state in Eq. [B39] and Theorem [1] For completeness, the resulting state of the circuit from Figure [2] is reproduced here in Eq. [B39] and Theorem [4]. For completeness, the resulting state of the circuit from Figure [2] is reproduced here in order to show it coincides with the one from the standard HSP algorithm in Figure [2].

Steps 1 - 2. These steps are the same as for the standard HSP algorithm. The resulting state is

\[
\rho_{2a} = \frac{1}{|G|} \sum_{g,\tilde{g} \in G \setminus H} \left\{ \sum_{h,\bar{h} \in H} |g + h\rangle \langle g + \bar{h}| \otimes |f(g)\rangle \langle f(g')| \right\}. \quad (B42)
\]

Steps 2a - 2c. Applying the operation $U_G \otimes U_S$ to the state $\rho_{2a}$ gives (see calculation in proof of Theorem [19]
\[ \rho_{2a} = \left( U_G \otimes U_S \right) \rho_2 \left( U_G \otimes U_S^\dagger \right) = \frac{1}{\dim \mathcal{H}_G^{(1)}} \left\{ \sum_{g, \tilde{g} \in \mathcal{H}_G^{(1)}} |g(1)\rangle \langle \tilde{g}(1)| \otimes |f(1)(g(1))\rangle \langle f(1)(\tilde{g}(1))| \right\} \otimes (|\chi\rangle \langle \chi|)^\otimes k. \] (B43)

The Bell pairs \(|\chi\rangle\) are formed between qubits from \(\mathcal{H}_G^{(2)}\) and \(\mathcal{H}_S^{(2)}\). The erasure \(\tilde{\mathcal{E}}\) in step 2b of \(\mathcal{H}_S^{(1)}\) is a standard Landauer erasure at temperature \(T\). We are ignorant about the state in \(\mathcal{H}_S^{(1)}\), thus we have to pay the full cost of

\[ W^{(1)} = \dim(\mathcal{H}_S^{(1)}) k_B T \ln 2 = (m - \ell) k_B T \ln 2. \] (B44)

Conversely the erasure \(\mathcal{E}\) is done with quantum side information according to Theorem 1. The average work cost of erasure at temperature \(T\) is given by

\[ W^{(2)} = H(\mathcal{S}^{(2)} | G^{(2)}) k_B T \ln 2 = -\ell k_B T \ln 2, \] (B45)

which amounts to a total average work cost of erasure

\[ W = W^{(1)} + W^{(2)} = (m - 2\ell) k_B T \ln 2. \] (B46)

The erasure leaves the reduced state of the \(G\) register invariant. After uncomputing \(U_G\), we get

\[ \rho_{2e} = \frac{1}{|G|} \sum_{g \in G} \sum_{h, h' \in H} |g + h\rangle \langle g + h'|, \] (B47)

as in Eq. (B13) from the standard HSP algorithm.

Steps 3 - 6. Based on the last observation, these steps go through as for the standard case.

4. Gate complexity of \(U_G\) and \(U_S\)

The transformations \(U_G\) and \(U_S\) from Definition 18 which are used in Theorem 19 are permutations of the basis states \(|g\rangle\) and \(|s\rangle\) for \(g \in G\) and \(s \in S\). These permutations ensure that after the application of the function oracle \(O_f\), the entanglement is compressed into a well-defined subregister of the main and auxiliary register.

In general, a permutation unitary on the computational basis states of \(n\) qubits requires \(O(n2^n)\) CNOT gates [31] and is therefore not efficiently implementable. Nevertheless, depending on the type of partial information available, the complexity of the transformations \(U_G\) and \(U_S\) can be drastically reduced (see for example the PFA, Section III C I). To this end, let us work in the special setting where the partial information is available in the form of an intermediate subgroup \(K\), such that \(H \subseteq K \subseteq G\) (as in Promise 7). There, the transformations \(U_G\) and \(U_S\) act on a state \(|g, f(g)\rangle\) as follows,

\[ U_G \otimes U_S |g, f(g)\rangle = |g, f(g)\rangle \otimes |\tilde{f}(k_g), [k]\rangle, \] (B48)

where \(k_g \in K\) and \([k]\in G/K\) are a decomposition of \(g \in G\) into an element in \(K\) and the quotient group \(G/K\). Consider the special case where \(K\) is already implemented on a subset of qubits of the main register — that is \(\mathcal{H}_K = \text{span}_2\{|k\rangle : k \in K\}\) is the Hilbert space generated by some but not necessarily all qubits that span \(\mathcal{H}_G\). Here the transformation \(U_G\) is only a composition of qubit swaps which can be implemented efficiently with a complexity \(O(\log |K|)\). For the target space an analogous rule holds. If the map \(f : G \to S\) implemented on the level of the function oracle \(O_f\) respects the qubit decomposition of \(\mathcal{H}_G\) into \(\mathcal{H}_K \otimes \mathcal{H}_{G/K}\), that is, these subregisters are mapped to subregisters of the auxiliary space \(\mathcal{H}_S\), then also \(U_S\) has complexity \(O(\log |K|)\). One particular case where this happens is the toy example for the PFA shown in Section III C I.

Appendix C: Proofs: Oracle simplification in the Hidden Subgroup Problem

This appendix is dedicated to proving Theorem 9 and giving more details on the modified HSP algorithm using a simplified oracle. By replacing the function oracle \(O_f\) by \(\tilde{O}_f\) one also has to reconsider what group the main register encodes. In fact, as the transformation \(U_G\) now hidden in \(\tilde{O}_f\) factors \(\mathcal{H}_G\) into registers \(\mathcal{H}_K\) and \(\mathcal{H}_{G/K}\), encoding the groups \(K\) and \(G/K\) respectively, the main register now encodes the subgroup \(K\). This coincides with the statement, that with the partial information, we can narrow down the search for \(H \in G\) to a search of \(H \in K\). Consequently, also the generalized quantum Fourier transform \(Q_G\) has to be replaced by \(Q_K\) as is shown in Figure 3 from the main part of the paper with the simplified algorithm.

Theorem 9 (Partial information correspondence). The unitaries \(U_G\) and \(U_S\) from Promise 7 can be used to formally construct a new function oracle \(\tilde{O}_f\) which requires \(2\ell\) fewer qubits than \(O_f\) \((\ell = \log_2 |G|/|K|)\). Moreover, this modified oracle \(\tilde{O}_f\) can still be used to solve the HSP.

Proof. An explicit calculation of the state \(\rho_i\) for the algorithm in the circuit of Figure 3 is performed, with \(1 \leq i \leq 6\) indexing the steps defined there.

Steps 1 - 2. The sum \(\sum_k\) is implicitly over the range of the first factor in \(\{|k, t\} = U_G|g\rangle : g \in G\} \subseteq \mathcal{H}_K \otimes \mathcal{H}_T\).
\( \mathcal{H}_{G/K} \). Then, \( \rho_1 = \frac{1}{|K|} \sum_{k, \hat{k}} |k, 0\rangle \langle \hat{k}, 0 | \otimes |0\rangle \langle 0 | \) (C1)

\[
U_G^{\dagger} \otimes S \xrightarrow{\rho_1, k, \hat{k}} \frac{1}{|K|} \sum_{k, \hat{k}} U_G^{\dagger} |k, 0\rangle \langle \hat{k}, 0 | U_G \otimes |0\rangle \langle 0 | = \rho_2. \quad (C2)
\]

Steps 3 - 4. Making use of the notation introduced in Eq. (C2) where \( g(k, t) \in G \) is the unique element s.t. \( U_G g(k, t) \) = |k, t\> the next states can be written down,

\[
\begin{align*}
\rho_2 &\xrightarrow{O_f} \frac{1}{|K|} \sum_{k, \hat{k}} U_G^{\dagger} |k, 0\rangle \langle \hat{k}, 0 | U_G \otimes |f(g(k, 0))\rangle \langle f(g(\hat{k}), 0) | \\
U_G \otimes U_S &\xrightarrow{\rho_2} \frac{1}{|K|} \sum_{k, \hat{k}} |k, 0\rangle \langle \hat{k}, 0 | \otimes |f^{(1)}(k), 0\rangle \langle f^{(1)}(\hat{k}), 0 | = \rho_4.
\end{align*}
\]

(C4)

For the last equality we used property\(^2\) imposed in Theorem\(^3\). At this stage we see that \( O_f \) acts trivially on the registers \( \mathcal{H}_{G'}^2 = \mathcal{H}_{G/K} \) and \( \mathcal{H}_{G'}^2 \), saving 2t erasures like the online erasure protocols do.

Steps 5 - 6. Recovering the hidden subgroup. It remains to be shown that the modified algorithm can still be used to determine the hidden subgroup \( H \). Let

\[
\begin{align*}
\rho_4' &= \text{Tr}_{\mathcal{H}_{G/K} \otimes \mathcal{H}_S} \rho_4 \\
&= \frac{1}{|K|} \sum_{k, h, h' \in H} \left\{ \sum_{h, h' \in H} |k + h\rangle \langle k + h'| \right\} \\
&= \frac{1}{|K|} \sum_{k, h, h' \in H} \left\{ \sum_{h, h' \in H} |\chi_k + h\rangle \langle \chi_k + h'| \right\} \\
&= \left( \frac{|H|}{|K|} \right)^2 \sum_{k, h, h' \in H} \sum_{g, g' \in H} |\chi_k (g) \chi_k (g') \rangle \langle g' |.
\end{align*}
\]

(C7)

(C8)

where \( H = \{ g \in K : \forall h \in H : \chi_g (h) = 1 \} \) is the analogue of \( H^+ \) from the standard HSP algorithm with the difference that \( G \) has been replaced by \( K \). This calculation demonstrates that the modified algorithm still recovers the hidden subgroup \( H \).

\[ \square \]

[1] R. Landauer, Irreversibility and Heat Generation in the Computing Process, IBM Journal of Research and Development 5, 183 (1961)

[2] C. H. Bennett, The thermodynamics of computation—a review, International Journal of Theoretical Physics 21, 905 (1982).

[3] J. Watrous, Quantum Computational Complexity, in Encyclopedia of Complexity and Systems Science edited by R. A. Meyers (Springer New York, New York, NY, 2009) pp. 7174–7201.

[4] A. Baumeler and S. Wolf, Free energy of a general computation, PRE 100, 052115 (2019).

[5] L. d. Rio, J. Åberg, R. Renner, O. Dahlsten, and V. Vedral, Addendum to “The thermodynamic meaning of negative entropy” — Supplementary Information —, Nature 476, 476 (2011).

[6] M. A. Nasiriy and J. E. Rice, A reversible majority voter circuit and applications, in IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM) (2017) pp. 1–6.

[7] M. Lostaglio, An introductory review of the resource theory approach to thermodynamics, Reports on Progress in Physics 82, 114001 (2019).

[8] F. G. S. L. Brandão, M. Horodecki, J. Oppenheim, J. M. Renes, and R. W. Spekkens, Resource Theory of Quantum States Out of Thermal Equilibrium, PRL 111, 250404 (2013).

[9] Z.-W. Liu, K. Bu, and R. Takagi, One-Shot Operational Quantum Resource Theory, PRL 123, 020401 (2019).

[10] G. Chiribella, Y. Yang, and R. Renner, Fundamental Energy Requirement of Reversible Quantum Operations, Phys. Rev. X 11, 021014 (2021).

[11] A. O. Orlov, C. S. Lent, C. C. Thorpe, G. P. Boeckler, and G. L. Snider, Experimental Test of Landauer’s Principle at the Sub-\( k_B T \) Level, Japanese Journal of Applied Physics 51, 06FE10 (2012).

[12] J. V. Koski, V. F. Maisi, J. P. Pekola, and D. V. Averin, Experimental realization of a Szilard engine with a single electron, Proceedings of the National Academy of Sciences 111, 13786 (2014). https://www.pnas.org/content/111/38/13786.full.pdf

[13] S. Ciliberto, Landauer’s Bound and Maxwell’s Demon, in Information Theory: Poincaré Seminar 2018, edited by B. Duplantier and V. Rivasseau (Springer International Publishing, Cham, 2021) pp. 87–112.

[14] J. Goold, M. Huber, A. Riera, L. d. Rio, and P. Skrzypczyk, The role of quantum information in thermodynamics—a topical review, Journal of Physics A: Mathematical and Theoretical 49, 143001 (2016).

[15] F. Binder, L. A. Correa, C. Gogolin, J. Anders, and G. Adesso, eds., Thermodynamics in the Quantum Regime, 1st ed., Fundamental Theories of Physics, Vol. 195 (Springer International Publishing, 2018).

[16] P. Taranto, F. Bakhshinezhad, A. Bluhm, R. Silva, N. Friis, M. P. E. Lock, G. Vitagliano, F. C. Binder, T. Debarba, E. Schwarzhans, F. Clivaz, and M. Huber, Landauer vs. Nernst: What is the True Cost of Cooling a Quantum System? (2021), arXiv:2106.05151 [quant-ph].
D. K. Park, N. A. Rodriguez-Briones, G. Feng, P. Lipka-Bartosik, P. Mazurek, and M. Horodecki, Sec-

N. Friis, S. Bulusu, and R. A. Bertlmann, Geometry

G. M. Andolina, M. Keck, A. Mari, M. Campisi, V. Gio-

M. Horodecki and J. Oppenheim, Fundamental limita-

M. Ettinger, P. Høyer, and E. Knill, The quantum query

A. Y. Kitaev, Quantum measurements and the Abelian

P. W. Shor, Polynomial-Time Algorithms for Prime Fac-

L. d. Rio, J. ˚Aberg, R. Renner, O. Dahlsten, and V. Ve-

C. H. Bennett, Notes on Landauer’s principle, reversible
computation, and Maxwell’s Demon, Studies in History
and Philosophy of Science Part B: Studies in History and

M. Mosca and A. Ekert, The Hidden Subgroup Problem

R. de Wolf, Quantum Computing: Lecture Notes (2019),
arXiv:1906.08415 [quant-ph]

M. Mosca, Abelian Hidden Subgroup Problem, in Ency-
clopedia of Algorithms edited by M.-Y. Kao (Springer
US, Boston, MA, 2008) pp. 1–4.

P. W. Shor, Polynomial-Time Algorithms for Prime Factor-
ization and Discrete Logarithms on a Quantum Com-
puter, SIAM Journal on Computing 26, 1484 (1997).
hits://doi.org/10.1137/S0097539795293172

A. Y. Kitaev, Quantum measurements and the Abelian
Stabilizer Problem (1995), arXiv:quant-ph/9510026

M. Ettinger, P. Hoyer, and E. Knill, The quantum query
complexity of the hidden subgroup problem is poly-
nomial, Information Processing Letters 91, 43 (2004).

N. J. Cerf and C. Adami, Negative entropy in quantum
information theory, in [New Developments on Funda-
mental Problems in Quantum Physics], edited by M. Ferrero
and A. van der Merwe (Springer Netherlands, Dordrecht,
1997) pp. 77–84.

N. J. Cerf and C. Adami, Negative Entropy and Infor-
mation in Quantum Mechanics, PRL 79, 5194 (1997)

N. Friis, S. Bulusu, and R. A. Bertlmann, Geometry of
two-qubit states with negative conditional entropy,
Journal of Physics A: Mathematical and Theoretical 50,
125301 (2017)

V. Shende, A. Prasad, I. Markov, and J. Hayes, Syn-
thesis of reversible logic circuits, IEEE Transactions on
Computer-Aided Design of Integrated Circuits and Sys-
tems 22, 710 (2003)

M. Horodecki and J. Oppenheim, Fundamental limita-
tions for quantum and nanoscale thermodynamics, Na-
ture Communications 4, 2059 (2013)

G. M. Andolina, M. Keck, A. Mari, M. Campisi, V. Gio-
vanni, and M. Polini, Extractable Work, the Role of Corre-
lations, and Asymptotic Freedom in Quantum Bat-
teries, Phys. Rev. Lett. 122, 047702 (2019)

P. Lipka-Bartosik, P. Mazurek, and M. Horodecki, Sec-
cond law of thermodynamics for batteries with vacuum
state, Quantum 5, 408 (2021)

D. K. Park, N. A. Rodriguez-Briones, G. Feng, R. Rahimi, J. Baugh, and R. Laflamme, Heat Bath Al-

Algorithmic Cooling with Spins: Review and Prospects, in Electron Spin Resonance (ESR) Based Quantum Com-
puting edited by T. Takui, L. Berliner, and G. Hanson
(Springer New York, New York, NY, 2016) pp. 227–255.

A. M. Alhambra, M. Lostaglio, and C. Perry, Heat-Bath
Algorithmic Cooling with optimal thermalization strate-
gies, Quantum 3, 188 (2019)

R. Soldatì, D. B. R. Dasari, J. Wrachtrup, and E. Lutz, Thermodynamics of a minimal algorithmic cooling refrig-
erator (2021), arXiv:2109.14056 [quant-ph]

A. Serafini, M. Lostaglio, S. Longden, U. Shackerley-
Bennett, C.-Y. Hsieh, and G. Adesso, Gaussian Thermal
Operations and The Limits of Algorithmic Cooling, PRL
124, 010602 (2020)

D. Egloff, O. C. O. Dahlsten, R. Renner, and V. Vedral, A
measure of majorization emerging from single-shot sta-
tistical mechanics, New Journal of Physics 17, 073001
(2015)

J. Aberg, Truly work-like work extraction via a single-
shot analysis, Nature Communications 4, 1925 (2013)

D. Reeb and M. M. Wolf, An improved Landauer prin-
ciple with finite-size corrections, New Journal of Physics
16, 103011 (2014)

J. G. Richens, A. M. Alhambra, and L. Masanes, Finite-
bath corrections to the second law of thermodynamics,
PRE 97, 062132 (2018)

O. Gülme and G. Tóth, Entanglement detection, Physics
Reports 474, 1 (2009)

C. Li, B.-H. Wang, B. Wu, and X. Yuan, Detecting entan-
glement of quantum channels, Communications in Theo-
retical Physics 73, 115101 (2021)

W. Nernst, Über die Berechnung chemischer Glei-
chgewichte aus thermischen Messungen, Nachrichten
von der Gesellschaft der Wissenschaften zu Göttingen,
Mathematisch-Physikalische Klasse 1906, 1 (1906)

W. Nernst, Über die Beziehung zwischen Wärmeentwicklung und maximaler Arbeit bei kon-
densierten Systemen, Ber. Kgl. Pr. Akad. Wiss. 52, 933
(1906)

H. Wilming and R. Gallego, Third Law of Thermody-
namics as a Single Inequality, Phys. Rev. X 7, 041033
(2017)

N. Freitas, R. Gallego, L. Masanes, and J. P. Paz, Cooling
to Absolute Zero: The Unattainability Principle, Ther-
modynamics in the Quantum Regime, 597–622 (2018)

F. Clivaz, R. Silva, G. Haack, J. B. Brask, N. Brun-
er, and M. Huber, Unifying paradigms of quantum re-
frigeration: Fundamental limits of cooling and associ-
ated work costs, Physical Review E 100, 10.1103/phys-
rev.e.100.042130 (2019).

P. Skrzypczyk, R. Silva, and N. Brunner, Passivity, com-
plete passivity, and virtual temperatures, Physical Re-
view E 91, 052133 (2015)

J. J. Rotman, Advanced Modern Algebra: Third Edition,
Part 1, 3rd ed. (American Mathematical Society, Prov-
idence, RI, 2015).

W. Fulton and J. Harris, Representation Theory: A First
Course Graduate Texts in Mathematics (Springer New
York, 2004).