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

Florian Meier [1,2,*] and Lídia del Rio [1,†]
[1]*Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*
[2]*Atominstitut, TU Wien, 1020 Vienna, Austria*

(Received 27 April 2022; accepted 29 November 2022; published 20 December 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.

DOI: 10.1103/PhysRevA.106.062426

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 (Fig. 1). 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 [1]. As heat dissipation in a quantum computer threatens coherence, reducing the work cost of erasure may be of critical importance.

We consider algorithms that use a *main register* of n qubits and an *auxiliary register* of m qubits (Fig. 1); 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 (Fig. 2) 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 [2–4], which coherently copies the output register to an external system, and then uncomputes the algorithm's circuit on the original qubits reversibly (Fig. 3). 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 [5]. Probabilistic quantum algorithms are made (approximately) deterministic by repeating them many times, and applying classical postprocessing 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) postprocessing as a large reversible quantum circuit, so that the final postprocessed quantum output is approximately decoupled from the rest of the memory.[1] 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.

We will work in the quantum resource theory of thermal operations [7–9]. 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 [10]. 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 [10]. This, together with recent erasure experiments that approach Landauer's limit [11–13], have led us to speculate that energies of the order $k_B T$ may eventually become relevant to quantum computing. Overall, thermodynamic optimization of quantum

*florian.meier@tuwien.ac.at
†lidia@phys.ethz.ch

[1]For example, majority votes can be implemented reversibly [6].

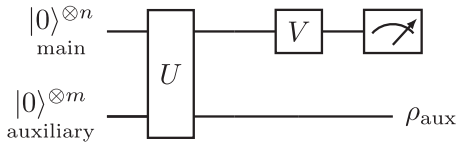

FIG. 1. Class of algorithms considered. We consider quantum algorithms where a main register is used until the final measurement, but there can be auxiliary registers, which are needed for only part of the algorithm, for example, the period-finding algorithm and more generally algorithms for hidden subgroup problems are of this form.

computation entails at least three independent components: (1) cost of unitary gates, (2) cost of erasure of fully mixed qubits, and (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 Sec. IV.

A. Contribution of this paper

Making use of entanglement between the main and auxiliary register as a thermodynamic resource [7–9,14,18,19], we introduce an erasure scheme (Fig. 4). 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.

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 possible only if we already know the solution to the problem, i.e., the hidden subgroup (Theorem 2).

(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 3).

(3) As an alternative to erasure, we can use that same partial information to simplify the algorithm, so that it uses fewer qubits (Theorem 4). We provide explicit protocols for the cases of black-box oracles and open circuit access to oracles (Figs. 7 and 8).

(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.

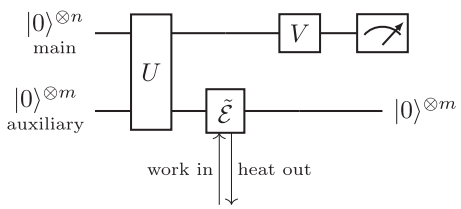

FIG. 2. On-the-go brute-force erasure. In order to free up memory space, the auxiliary register can be erased on the go. A brute-force erasure at temperature T will have work cost $k_B T \ln 2$ per qubit due to Landauer's principle.

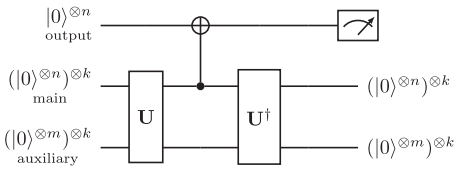

FIG. 3. Bennett's uncomputing erasure. For Bennett's uncomputing, the original probabilistic algorithm is made essentially deterministic by running many copies of $(V \otimes \mathbb{1}) \circ U$ in parallel together with a quantum implementation of the classical postprocessing, summarized as **U**. The result of this calculation is coherently copied to an output register and **U** is uncomputed.

In Sec. 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 Sec. III. By the example of the period finding algorithm in Sec. III C 1, we illustrate the key concepts of our optimized on-the-go erasure scheme and in Sec. III A, we generalize the example to the Abelian hidden subgroup problem. There we state the main theorems 1–4 together with a qualitative sketch of the proofs. Discussions and open questions can be found in Sec. IV. The full proofs of the main theorems and further generalizations are explored in the Appendixes: in Appendix A an explicit erasure protocol [20] is reviewed, and Appendixes B and C contain the proofs for our results.

II. SETTING AND 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

Landauer's principle [1,21] demonstrates the intricate relation between information theory and thermodynamics. It states that logically irreversible operations come with an

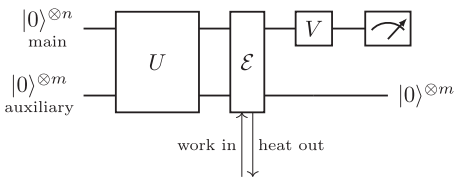

FIG. 4. Optimized on-the-go erasure. We propose an optimized on-the-go erasure scheme which takes advantage of the entanglement between main and auxiliary register to reduce the work cost of erasure of the latter.

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 ρ_S, the average work cost of erasing this system at a temperature T (that is setting $\rho_S \mapsto |0\rangle\langle 0|_S$ using a thermal bath at temperature T) scales with the entropy of the initial state,

$$W(S) = H(S) k_B T \ln 2, \tag{1}$$

where k_B is the Boltzmann constant and $H(\rho) = -\operatorname{Tr}(\rho \log_2 \rho)$ is the von Neumann entropy [14]. In the setting of Fig. 2, 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 ρ_S. The average work cost of this map corresponds to the worst-case scenario of erasing a fully mixed state $\rho_S = (\mathbb{1}/2)^{\otimes m}$, that is $mk_BT \ln 2$ 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,

$$\rho_{RGS} \overset{\mathcal{E}}{\mapsto} \rho_{RG} \otimes |0\rangle\langle 0|_S, \text{ where } \rho_{RG} = \operatorname{Tr}_S(\rho_{RGS}), \tag{2}$$

which does not exceed an average work cost (and heat dissipation) of

$$W(S|G)_\rho = H(S|G)_\rho \, k_B T \ln 2, \tag{3}$$

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 GS: there exists a process that achieves the transformation $\rho_G \otimes |0\rangle\langle 0|_S \mapsto \rho_{GS}$ 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 Sec. IV). In the following G will be the main register and S will be the auxiliary register.[2] The reference system R includes the nonaccessible degrees of freedom that may be correlated with our quantum registers, e.g., the rest of the quantum computer.

1. Example: Erasure of half of a Bell pair

This is the simplest application of Lemma 1, which will be useful to understand the general procedure later [18]. 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,

$$\rho_{GS} = \rho_{G_1} \otimes |\chi\rangle\langle\chi|_{G_2 S}, \tag{4}$$

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 $\rho_G \otimes |0\rangle\langle 0|_S = \rho_{G_1} \otimes \frac{\mathbb{1}_{G_2}}{2} \otimes |0\rangle\langle 0|_S$. We achieve that with the following protocol:

(1) Unitarily rotate the pure state of G_2S from $|\chi\rangle$ to $|00\rangle$ for free,

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

This erasure map, decomposed in the following two steps:

$$\rho_{G_1} \otimes |\chi\rangle\langle\chi| \overset{U}{\underset{\text{free}}{\longmapsto}} \rho_{G_1} \otimes |0\rangle\langle 0|_{G_2} |0\rangle\langle 0|_S \tag{5}$$

$$\overset{\mathcal{E}^\dagger}{\underset{\text{gain } k_BT \ln 2}{\longmapsto}} \rho_{G_1} \otimes \frac{\mathbb{1}_{G_2}}{2} \otimes |0\rangle\langle 0|_S, \tag{6}$$

does not affect the reduced state of the G register:

$$\rho_G = \operatorname{Tr}_S(\rho_{GS}) = \rho_{G_1} \otimes \frac{\mathbb{1}_{G_2}}{2} \tag{7}$$

$$= \operatorname{Tr}_S\left(\rho_{G_1} \otimes \frac{\mathbb{1}_{G_2}}{2} \otimes |0\rangle\langle 0|_S\right). \tag{8}$$

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

$$W(S|G) = -k_BT \ln 2 = H(S|G) k_BT \ln 2 \tag{9}$$

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 1 (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[3] 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

[2]The notation G for the main register is chosen because later the main register will encode a group G.

[3]That is, polynomial time complexity under the assumption that f can be implemented efficiently.

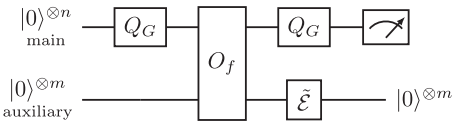

FIG. 5. Abelian hidden subgroup algorithm [22,23]. The quantum circuit above solves the Abelian hidden subgroup problem. Since it is of the same form as Fig. 4, we can use it as a candidate for optimizing the on-the-go erasure. The main register $\mathcal{H}_G$ encodes the group G and the auxiliary register $\mathcal{H}_S$ encodes S. The function oracle acts on states of the joint register via $O_f|g,s\rangle = |g, s \oplus f(g)\rangle$, with $\oplus$ denoting the bitwise XOR operation. The algorithm performs the following sequence: (1) Generalized quantum Fourier transform $Q_G \otimes \mathbb{1}$ on G register creates a superposition $\frac{1}{|G|}\sum_{g\in G}|g,0\rangle$. (2) Global oracle operation O_f on both registers. At any later point we can erase S with a map $\tilde{\mathcal{E}}$. (3) Quantum Fourier transform Q_G on G register. (4) Measurement of the G register. (5) Classical postprocessing of the result.

the HSP (Fig. 5). In Appendix B 1 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 Fig. 1. After a unitary $U = O_f \circ (Q_G \otimes \mathbb{1})$ operation on main and auxiliary register the latter is no longer needed and can be erased by using a Landauer erasure $\tilde{\mathcal{E}}$. 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 Fig. 4 corresponds to the composition $O_f \circ (Q_G \otimes \mathbb{1}) = U$ from Fig. 5. By ρ_{GS} we denote the state of GS right after U. To apply the result from Lemma 1 we have to determine *where* in ρ_{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, ℓ Bell pairs $|\chi\rangle$,

$$\rho_{GS} \overset{U_G\otimes U_S}{\longmapsto} \rho_{G^{(1)}S^{(1)}} \otimes (|\chi\rangle\langle\chi|_{G^{(2)}S^{(2)}})^{\otimes \ell}. \tag{11}$$

In our erasure algorithm, the entanglement is always compressed into fully entangled pairs of qubits.[4] In Sec. III A we establish bounds on the number of Bell pairs ℓ 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 $\rho_{G^{(1)}} \otimes (\mathbb{1}_{G^{(2)}}/2)^{\otimes \ell}$. Before one can continue the computation with $V = Q_G$, the local transformation U_G

[4]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).

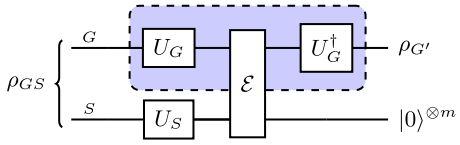

FIG. 6. The erasure process acting on an initial state ρ_{GS} must leave the reduced state of the main register invariant, i.e., we require $\mathrm{Tr}_S(\rho_{GS}) = \rho_{G'}$ (the violet box in the circuit must act locally as the identity on G). This requirement is necessary to ensure that our on-the-go erasure procedure does not affect the outcome of the algorithm to which it is applied.

has to be undone,

$$\rho_{G^{(1)}} \otimes \left(\frac{\mathbb{1}_{G^{(2)}}}{2}\right)^{\otimes \ell} \overset{U_G^\dagger}{\longmapsto} \rho'_G, \tag{12}$$

where the reduced state on G is unaffected by the erasure $\rho'_G = \mathrm{Tr}_S(\rho_{GS})$ (Fig. 6). 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 Sec. II C there is an upper bound on how well one can optimize the thermodynamics of the algorithm:

Theorem 1 (Entanglement upper bound). For an Abelian group G with hidden subgroup H and indicator function $f : G \to S$ as in Problem 1, solved by the algorithm from the circuit in Fig. 5 the maximal number $\ell_{\max}$ of Bell pairs between main and auxiliary registers that can be obtained via local unitary operations is

$$\ell_{\max} = \log_2 \frac{|G|}{|H|} = -H(S|G)_{\rho_{GS}}, \tag{13}$$

where ρ_{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 [28–30]. 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 $|[g]\rangle_{G/H} \otimes |f([g])\rangle_{S^{(2)}}$. They originate the state right after the function

oracle

$$\rho_{GS} = \frac{1}{|G|} \sum_{[g],[g']\in G/H} \sum_{h,h'\in H} |g+h, f(g)\rangle\langle g'+h', f(g')|_{GS}. \tag{14}$$

The sum over the cosets can be factored out via a local transformation, given by a choice of representative for each coset, that is, $U_G|g+h\rangle_G = |[g]\rangle_{G/H} \otimes |h\rangle_H$. Furthermore reordering the computational basis of $\mathcal{H}_S$ such that $|f([g])\rangle_{S^{(2)}}$ has the same computational representation as $|[g]\rangle_{G/H}$, we find

$$\rho_{\text{rest}} \otimes \sum_{[g]\in G/H} |[g], f([g])\rangle\langle[g], f([g])|_{G/H,S^{(2)}} \tag{15}$$

$$= \rho_{\text{rest}} \otimes (|\chi\rangle\langle\chi|)^{\otimes \log_2 |G/H|}_{G/H,S^{(2)}}. \tag{16}$$

This results in a contribution of $\ell_{\max} = \log_2 |G/H|$ Bell pairs. The remaining terms in the sum are not entangled. Along the same lines we show that such a factorization can indeed be realized by unitary operations.

Lemma 2 (Existence of transformations saturating the bound). There exist local unitaries U_G and U_S which saturate the upper bound $\ell_{\max}$ of Bell pairs which can be factored from the state after the function oracle O_f.

There is a caveat to the transformations U_G and U_S saturating this upper bound as in Theorem 1. In fact, finding the transformations must be at least as difficult as solving the problem for which we run the algorithm in the first place.

Theorem 2 (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 1 can be used to solve the HSP.

The underlying reason is that the transformation U_G required for this factorizes the main register $\mathcal{H}_G$ into parts belonging to H and G/H,

$$U_G : \mathcal{H}_G \to \mathcal{H}_H \otimes \mathcal{H}_{G/H}. \tag{17}$$

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 about the solution of our problem. In a next step we explore how Theorem 2 generalizes to instances where $\ell_{\max}$ is not reached. What type of partial information is required to factor $\ell \leqslant \ell_{\max}$ Bell pairs, and how do we quantify it?

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

1. Optimized on-the-go erasure

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 $\ell \leqslant \ell_{\max}$ Bell pairs after the function oracle O_f. We start with the promise of *knowing where* ℓ Bell pairs are, that is, we have access to transformations U_G and U_S on $\mathcal{H}_G$ and $\mathcal{H}_S$ which factor out ℓ Bell pairs after the function oracle. The Bell pairs we consider are fully correlated qubits which tells us that the oracle O_f maps some part of $\mathcal{H}_G$ one to one on $\mathcal{H}_S$. Formally, this corresponds to a factorization $\mathcal{H}_G \cong \mathcal{H}_G^{(1)} \otimes \mathcal{H}_G^{(2)}$ and $\mathcal{H}_S \cong \mathcal{H}_S^{(1)} \otimes \mathcal{H}_S^{(2)}$ with O_f fully correlating the spaces $\mathcal{H}_G^{(2)}$ and $\mathcal{H}_S^{(2)}$. This translates into a promise about algebraic properties of f which characterizes what we need to know about f to factor out ℓ Bell pairs (Promise 1).

Promise 1 (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 B 3, Definition 2 and Theorem 9, together with a proof that Promise 1 is sufficient and necessary for factoring ℓ 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 B 3 for detailed prescriptions of the transformations). In particular, the specific form in Eq. (19) allows factoring out Bell pairs as outlined in our strategy (Sec. II C) in Eq. (11).

Promise 2 (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

$$U_G : \mathcal{H}_G \to \mathcal{H}_K \otimes \mathcal{H}_{G/K}. \tag{18}$$

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

$$U_G \otimes U_S|g, f(g)\rangle = |k_g, [k]\rangle \otimes |\tilde{f}(k_g), [k]\rangle. \tag{19}$$

The circuit in Fig. 7 implements the modifications due to the transformations U_G and U_S from Promise 2. This brings a reduction of the work cost of erasure which we quantify in Theorem 3.

Theorem 3 (Work cost of erasure with partial information). Given the transformations U_G and U_S from Promise 2, 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

$$W = (m - 2\ell)k_B T \ln 2, \tag{20}$$

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 1. The only change in the circuit of Fig. 7 is that the transformations U_G and U_S have to be replaced by their generalized versions. In Appendix B 3, Theorem 10 generalizes Theorem 3. For a proof, the reader is referred there.

2. Oracle simplification with partial information

In Sec. III B we derived a no-go result (Theorem 2) for the factorization $\mathcal{H}_G \to \mathcal{H}_H \otimes \mathcal{H}_{G/H}$ 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 2), 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

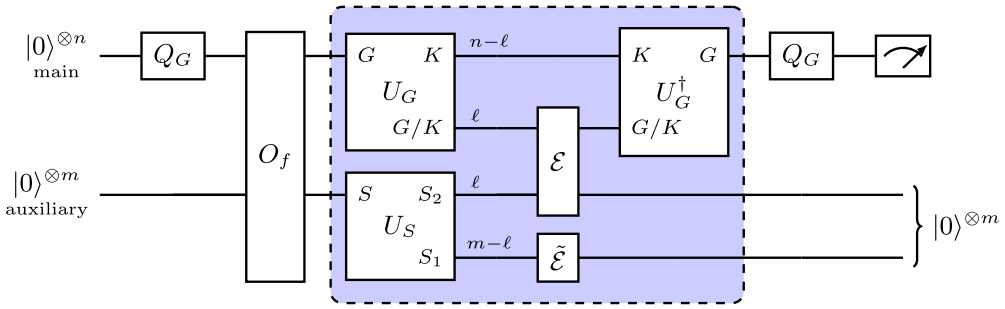

FIG. 7. Optimized on-the-go erasure. The above circuit is a modified version of Fig. 5 implementing the optimized on-the-go erasure of ℓ qubits (see shaded part of the diagram). Here we know unitaries U_G and U_S which factor out part of the entanglement between the main and auxiliary register in the form of ℓ Bell pairs. The ℓ qubits belonging to the auxiliary register are then erased at temperature T with $\tilde{\mathcal{E}}$ at a total average work cost of $-\ell k_B T \ln 2$. In the list below, the first steps 1–2 and last steps 3–5 of the modified algorithm displayed above are unchanged from the original. 1-2. Generalized quantum Fourier transform and oracle operation. 2a. Unitary transformation $U_G \otimes U_S \otimes \mathbb{1}_B$. 2b. Side information erasure $\mathcal{E}$ of ℓ qubits, standard erasure $\tilde{\mathcal{E}}$ of remaining $m-\ell$ qubits. 2c. Reverse transformation $U_G^\dagger \otimes U_S^\dagger \otimes \mathbb{1}_B$. 3-5. Quantum Fourier transform, measurement, and classical postprocessing.

information required for the transformations U_G and U_S? The following result answers this question.

Theorem 4 (Partial information correspondence). The unitaries U_G and U_S from Promise 2 can be used to formally construct a new function oracle $\tilde{O}_f$ which requires 2ℓ 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 2ℓ fewer qubits than with O_f. Both the main and auxiliary qubits can be reduced by ℓ and in comparison to the circuit in Fig. 7, the quantum Fourier transform on the main register is now implemented for the group K instead of G. Details for the proof of Theorem 4 are in Appendix C. The two constructions we made are thermodynamically equivalent: For the circuit in Fig. 7 we have an average work cost of erasure equal $(m-2\ell)k_B T \ln 2$ due to an erasure of ℓ auxiliary qubits which were fully entangled to the main register. In the simplified algorithm using modified oracle from Fig. 8, 2ℓ 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 4, given in the circuit of Fig. 8 is sufficient for finding the hidden subgroup H. The simplification due to the modified oracle $\tilde{O}_f$ (see Fig. 8) 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 2ℓ 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 2 (Period finding problem). Given a function $f : \mathbb{Z}_N \to \mathbb{Z}_M$ which is r-periodic and injective on each period of length r, the goal is to find r.

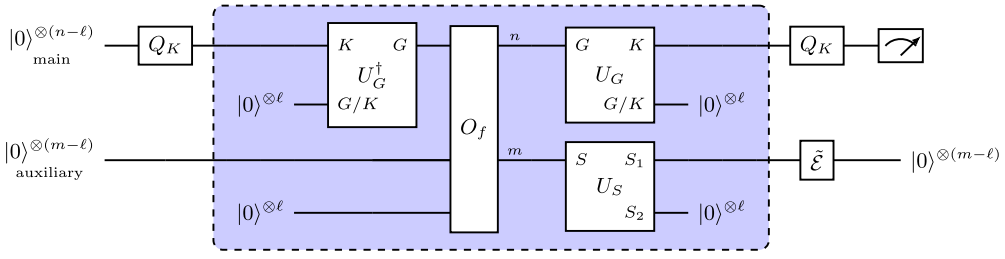

FIG. 8. Oracle simplification. If we have access to partial information about a subgroup K, the modified oracle $\tilde{O}_f$ (violet box in the circuit) can be used instead of the original oracle O_f. The 2ℓ qubits inside the violet box are in the $|0\rangle$ state regardless of the input of the main and auxiliary qubits. All in all, the oracle $\tilde{O}_f$ has 2ℓ 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 2ℓ qubits. In comparison to the standard algorithm (Fig. 5) 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 Fig. 5; in the following enumeration they are steps 1 and 3–4, while steps 2a′–2c′ are encapsulated by $\tilde{O}_f$ in the above circuit: 1. Generalized quantum Fourier transform Q_K on $\mathcal{H}_K$, 2a′. Inverse transformation $U_G^\dagger$ on $\mathcal{H}_K \otimes \mathcal{H}_{G/K}$, 2b′. Original oracle operation O_f, 2c′. Transformations $U_G \otimes U_S$, 3–4. Generalized quantum Fourier transform Q_K on $\mathcal{H}_K$, and measurement of K register.

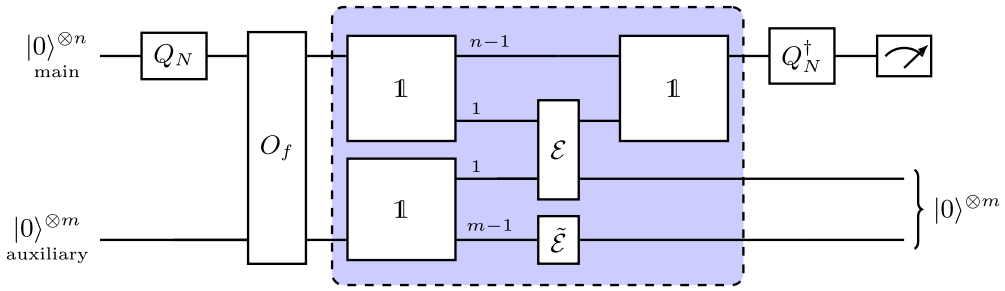

FIG. 9. Two-qubit on-the-go erasure for the period finding algorithm. Here the circuit describing the optimized on-the-go erasure of the least significant qubits in the period finding algorithm is shown. Given the Promise 3, the oracle O_f fully entangles the least significant qubits of main and auxiliary register. The auxiliary qubit of this pair can then be erased at a negative average work cost of $-k_BT\ln 2$ if the erasure is performed at temperature T.

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

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

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

Promise 3. The function f can be written in the form $f(2x(+1)) = 2\tilde{f}(x)(+1)$, for some other function $\tilde{f}$: $\mathbb{Z}_{N/2} \to \mathbb{Z}_{M/2}$. 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 2; here, we go through the calculations of the optimized on-the-go erasure (Fig. 9) and provide an explicit simplification of the function oracle (Fig. 10). 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

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

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

$$= \rho_{G^{(1)}S^{(1)}} \otimes |\chi\rangle\langle\chi|_{G^{(2)}S^{(2)}}, \tag{24}$$

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 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, $U_G = \mathbb{1}_G$ and $U_S = \mathbb{1}_S$ (Fig. 9). 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 3 in terms of computational complexity? An alternative usage of the partial information is to run the PFA not for the function $f : \mathbb{Z}_N \to \mathbb{Z}_M$ but rather $\tilde{f} : \mathbb{Z}_{N/2} \to \mathbb{Z}_{M/2}$ with $\tilde{f}(x) = f(2x)/2$. This algorithm requires two fewer qubits to run. Operationally, we simply do not 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 (Fig. 10).

2. Discrete logarithm problems

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

Problem 3 (Discrete logarithm problem). Given the cyclic group $S = \{1, \gamma, \ldots, \gamma^{N-1}\}$ of order N with generator γ 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 pedadogical derivation) by introducing the group $G = \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ and a function

$$f : G \to S;\ (i, j) \mapsto \gamma^i A^{-j}. \tag{25}$$

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

$$f((i, j) + (k, \ell)) = f(i + k, j + \ell) \tag{26}$$

$$= \gamma^{i+k}A^{-j-\ell} = \gamma^i\gamma^k A^{-j}A^{-\ell} \tag{27}$$

$$= f(i, j)f(k, \ell). \tag{28}$$

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 2 is available. This could again be the case in form of an intermediate subgroup $H \subseteq K \subseteq G$.

IV. DISCUSSION

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

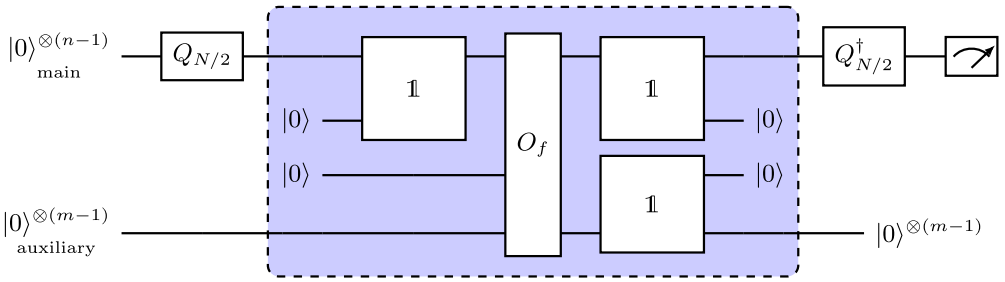

FIG. 10. Two-qubit oracle simplification for the period finding algorithm. At equivalent thermodynamic costs as the on-the-go erasure in Fig. 9, the period finding algorithm can alternatively be simplified to an algorithm which uses two qubits fewer by keeping the least significant qubits of main and auxiliary register constantly in the ground state $|0\rangle$.

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 ℓ qubits for application, the following costs have to be weighted against each other: on-the-go erasure versus the following:

(1) *Straightforward erasure:* Given the architecture of the quantum computer, does the work cost reduction by $2\ell k_B T \ln 2$ 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 postprocessing and a reversible majority vote compared to the gain of $(m-2\ell)k_B T \ln 2$? 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 2ℓ 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 ℓ fewer qubits. At the level of thermodynamic costs, both options are equivalent.

A. 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 3 (together with Promise 2) 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 $\mathcal{H}_K = \mathrm{span}_{\mathbb{C}}\{|k\rangle : k \in K\}$ 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 $O(n2^n)$ [31], 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 (Sec. III C 1), and for the discrete logarithm for all subgroups of $G = \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ of the form $\langle\langle 2^k\rangle\rangle \times \mathbb{Z}/N\mathbb{Z}$ (Sec. III C 2). 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 B 4.

B. 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 [7,32–34]. The battery consists of *fueled* qubits in state $|0\rangle$ and *depleted* qubits in the fully mixed state $\mathbb{1}/2$; 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. In 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 A 2.

A related topic is algorithmic cooling which is about the process of producing cold (that is, approximately pure) qubits [35]. There are approaches that extract entropy from a target system by coupling it to thermal baths in an approach called

heat-bath algorithmic cooling [36–38]. 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 A 2), one could apply algorithmic cooling there to produce pure battery states.

C. 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 [18,39]. If the rest Hamiltonian of the qubits is not fully degenerate, one needs to employ single-shot versions of the free energy [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 [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.

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 [43,44], without affecting the state of the main register.

ACKNOWLEDGMENTS

We thank Marcus Huber for discussions and feedback. F.M. acknowledges the SEMP scholarship from Movetia for his research stay abroad and the stipend from the QUIT group at TU Vienna. L.d.R 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 F.M.'s semester project as a master's student. The technical contributions (including proofs and algorithm proposals) and first draft of the paper are his. L.d.R. 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 $\mathbb{1}/2 \mapsto |0\rangle\langle 0|$ comes with diverging resource costs by the third law of thermodynamics [45–47] 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 setup for the erasure consists of three quantum systems.

(1) *Qubit.* The system of the qubit is described by the two dimensional Hilbert space $\mathcal{H}_S = \mathbb{C}^2$ with basis $\{|0\rangle_S, |1\rangle_S\}$. Furthermore, it is assumed that the energy levels of this system are degenerate, this is achieved with the Hamiltonian $H_S = 0$.

(2) *Work storage.* In an idealized scenario the work storage consists of an infinite number of evenly spaced, nondegenerate energy eigenstates $\mathcal{H}_W = \{|E_k\rangle : k \in \mathbb{Z}\}$. The Hamiltonian in given by $H_W = \sum_{k\in\mathbb{Z}} k\Delta |E_k\rangle\langle E_k|$ with Δ the energy spacing between two neighboring levels $|E_k\rangle$, $|E_{k+1}\rangle$. An experimental realization will only be able approximate this system with energy levels bounded from below. Because the explicit implementation of the qubit erasure is not relevant for the remaining treatment of the online erasure, we will not investigate this any further.

(3) *Heat bath.* The heat bath is an ensemble of N qubits thermalized at a temperature $\beta = 1/k_B T$ where each qubit has a different energy spacing. The Hilbert space is $\mathcal{H}_{\text{bath}} = (\mathbb{C}^2)^{\otimes N}$, with basis $\{|0\rangle_\ell, |1\rangle_\ell\}$ for the ℓth factor. The Hamiltonian governing the dynamics of the system is $H_{\text{bath}} = \sum_{\ell=1}^{N} \ell\Delta |1\rangle\langle 1|_\ell \otimes \mathbb{1}_{i\neq\ell}$. The energy Δ is the same as for the work storage. Requiring that the qubits of the heat bath are at a temperature β gives the thermal state of $\mathcal{H}_{\text{bath}}$ to be

$$\tau(\beta) = \frac{e^{-\beta H_{\text{bath}}}}{Z}, \quad Z = \text{Tr}(e^{-\beta H_{\text{bath}}}).$$

In a first example we consider the erasure of one fully mixed qubit $\rho = \mathbb{1}/2$ in $\mathcal{H}_S$. For a heat bath consisting of N qubits an erasure is performed in N steps. In step ℓ ($1 \leqslant \ell \leqslant N$) the qubit from $\mathcal{H}_S$ is swapped with the ℓth qubit from the heat bath $\mathcal{H}_{\text{bath}}$ and simultaneously the energy level of the work storage is lowered by ℓ steps to preserve energy. The unitary operation implementing this step is

$$\begin{aligned} U^{(\ell)} = \sum_{k\in\mathbb{Z}} &\{|E_{k+\ell}, 1_S, 0_\ell\rangle\langle E_k, 0_S, 1_\ell| \\ &+ |E_k, 0_S, 1_\ell\rangle\langle E_{k+\ell}, 1_S, 0_\ell|\} \otimes \mathbb{1}_{i\neq\ell} \qquad \text{(A1)} \\ &+ \mathbb{1}_B \otimes (|0_S, 0_\ell\rangle\langle 0_S, 0_\ell| + |1_S, 1_\ell\rangle\langle 1_S, 1_\ell|) \otimes \mathbb{1}_{i\neq\ell}, \qquad \text{(A2)} \end{aligned}$$

and it commutes with the Hamiltonian of the joint system of the work storage, qubit and heat bath. The energy level diagram in Fig. 11 (adapted from [20]) visualizes this unitary operation for $\ell = 3$.

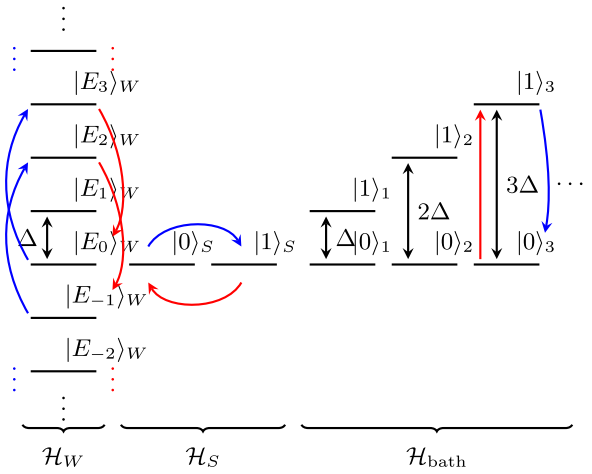

FIG. 11. Qubit erasure energy diagram. Energy level diagram for the erasure setup of one qubit. From left to right are work storage, qubit system, and heat bath. The curved arrows visualize the swapping operation done by the unitary $U^{(3)}$ from Eq. (A1).

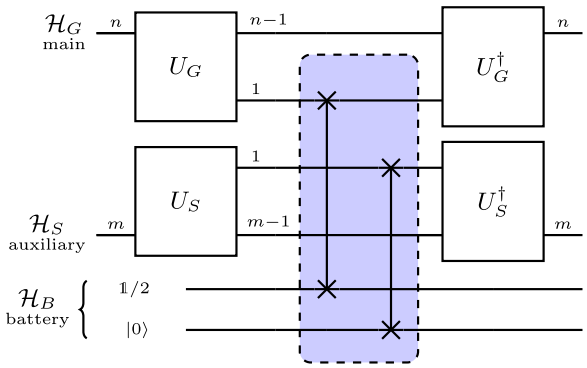

FIG. 12. The first transformation brings the state $\rho_{GS} \otimes (\mathbb{1}/2) \otimes |0\rangle\langle 0|$ into a factorized form $\rho_{G'S'} \otimes |\chi\rangle\langle\chi| \otimes (\mathbb{1}/2) \otimes |0\rangle\langle 0|$, in which the Bell pair $|\chi\rangle\langle\chi|$ is swapped with the partially erased state $(\mathbb{1}/2) \otimes |0\rangle\langle 0|$. After uncomputing U_G and U_S, that is, $\rho_{G'S'} \otimes (\mathbb{1}/2) \otimes |0\rangle\langle 0| \otimes |\chi\rangle\langle\chi|$ is mapped to $\tilde{\rho}_{GS} \otimes |\chi\rangle\langle\chi|$, the reduced states of the main register $\tilde{\rho}_G = \text{Tr}_S(\tilde{\rho}_{GS})$ is the same as before the operation, $\rho_G = \tilde{\rho}_G$, where $\rho_G = \text{Tr}_S(\rho_{GS})$.

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

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

the erasure U acts on ρ_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 $\mathbb{1}_S/2$ 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. For many qubits this process can be performed on each qubit individually.

2. Using an information battery inside the quantum computer

For the purpose of this work it suffices to consider two types of battery registers: One register $\mathcal{H}_B^{(\text{depleted})}$, containing only fully mixed qubits

$$\rho_B^{(\text{depleted})} = \left(\frac{\mathbb{1}}{2}\right)^{\otimes \dim B^{(\text{depleted})}}, \tag{A3}$$

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,

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

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.

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.

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 the entanglement between the registers can be compressed into Bell pairs (see Appendix B 3). Instead of using these unitaries to prepare the registers for being erased as in Fig. 7, they can be used to swap the entangled states with states from the battery. In Fig. 12 the situation is presented for a single Bell pair swap. It generalizes to many Bell pairs without any complications.

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, and finally 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* (HSP).

Problem 1 (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 $g, g' \in G$

$$f(g) = f(g') \iff gH = g'H, \quad (10)$$

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 [23]. 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 $\bar{g} = g + H \in G/H$. 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 5 (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

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

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

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

$$\rho_k : \ell \in \mathbb{Z}/a\mathbb{Z} \mapsto \omega_a^{k\ell} \in \mathbb{C}^* \quad (B2)$$

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 2 ([53]). The characters of $G \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_m\mathbb{Z}$ (c.f. Theorem 5) are given by

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

where the factors are as in Proposition 1 and elements $g, h \in G$ are understood as in the decomposition of G into cyclic factors. The irreducible representation ρ_g having χ_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 χ_g as introduced in Proposition 2: 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 true only for characters of one-dimensional irreducible representations and does not hold in general.

Theorem 6 (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

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

The characters are defined as in Proposition 2.

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

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

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

Definition 1 (Quantum Fourier transform of a group register [23]). Let G be a finite Abelian group with decomposition as in Theorem 5. For any $g \in G$ the character state $|\chi_g\rangle$ is declared by

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

the functions χ_g, $g \in G$ as in Proposition 2.

In the algorithm solving the HSP from Fig. 5, states will be transformed according to the rule in Eq. (B6) and certain summands will cancel out according to Theorem 6. The following subgroup will be of particular interest to us:

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

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 erasure 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 Fig. 5.

Step 1. Denote by ρ_ℓ the density matrix of the joint G and S register after iteration step ℓ in the HSP algorithm, in particular $\rho_0 = |0\rangle\langle 0| \otimes |e\rangle\langle e|$. The first steps of the algorithm

$$\rho_0 \overset{(1)}{\mapsto} |\chi_0\rangle\langle\chi_0| \otimes |0\rangle\langle 0| \quad (B8)$$

$$= \frac{1}{|G|} \sum_{g,g' \in G} |g\rangle\langle g'| \otimes |0\rangle\langle 0| = \rho_1, \quad (B9)$$

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

Step 2. Oracle Operation:

$$\rho_1 \overset{(2)}{\mapsto} \frac{1}{|G|}\sum_{g,g'\in G} |g\rangle\langle g'| \otimes |f(g)\rangle\langle f(g')| \tag{B10}$$

$$= \frac{1}{|G|}\sum_{\bar{g},\bar{g}'\in G/H}\left\{\sum_{h,h'\in H}|g+h\rangle\langle g'+h'|\right\} \tag{B11}$$

$$\otimes\ |f(g)\rangle\langle f(g')| = \rho_2. \tag{B12}$$

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

$$\rho_2' = \mathrm{Tr}_S\,\rho_2 = \frac{1}{|G|}\sum_{\bar{g}\in G/H}\left\{\sum_{h,h'\in H}|g+h\rangle\langle g+h'|\right\}. \tag{B13}$$

Steps 3–4. The remaining two steps are performed on the reduced G register. The states will be denoted by a dash ρ_ℓ':

$$\rho_2' \overset{(3)}{\mapsto} \frac{1}{|G|}\sum_{\tilde{g}\in G/H}\left\{\sum_{h,h'\in H}|\chi_{g+h}\rangle\langle\chi_{g+h'}|\right\} \tag{B14}$$

$$= \left(\frac{|H|}{|G|}\right)^2 \sum_{\tilde{g}\in G/H}\left\{\sum_{\tilde{g},\tilde{g}'\in H^\perp}\chi_g(\tilde{g})\chi_g(\tilde{g}')|\tilde{g}\rangle\langle\tilde{g}'|\right\} = \rho_3'. \tag{B15}$$

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

3. Proofs

Theorem 1 (Entanglement upper bound). For an Abelian group G with hidden subgroup H and indicator function $f : G \to S$ as in Problem 4, solved by the algorithm from the circuit in Fig. 5 the maximal number $\ell_{\max}$ of Bell pairs between main and auxiliary registers that can be obtained via local unitary operations is

$$\ell_{\max} = \log_2\frac{|G|}{|H|} = -H(S|G)_{\rho_{GS}}, \tag{13}$$

where ρ_{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

$$H(S|G) = H(\rho_{GS}) - H(\rho_G), \tag{B16}$$

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 ρ_{GS} and $\rho_G = \mathrm{Tr}_S\,\rho_{GS}$ is the reduced state of the G register. Observe the following two facts: First, up until the erasure of the S register which takes place after step 2 in the HSP algorithm, the joint state ρ_{GS} is a pure state. Second, we have $\rho_{GS} = \rho_G \otimes \rho_S$ before step 2 where the function oracle is applied, where ρ_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 nonzero is after O_f but before the $\mathcal{H}_S$ is traced out. The corresponding state from Eq. (B12) is

$$\rho_{GS} = \frac{1}{|G|}\sum_{\substack{\bar{g},\bar{g}'\in\\ G/H}}\left\{\sum_{\substack{h,h'\in\\ H}}|g+h\rangle\langle g'+h'|\right\}\otimes|f(g)\rangle\langle f(g')|, \tag{B17}$$

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

$$H(S|G) = H(\rho_{GS}) - H(\rho_G) \tag{B18}$$

$$= 0 + \mathrm{Tr}(\rho_G\log_2\rho_G), \tag{B19}$$

with $\rho_G = \rho_2'$ the reduced G register state; cf. Eq. (B13). The entropy measure is invariant under unitary transformations of ρ_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 ρ_2 can be factored $\rho_2 \cong \rho_H \otimes \rho_{G/H}$:

$$\frac{1}{|G|}\sum_{\bar{g}\in G/H}\left\{\sum_{h,h'\in H}|g+h\rangle\langle g+h'|\right\} \tag{B20}$$

$$\cong \underbrace{\frac{1}{|H|}\sum_{h,h'\in H}|h\rangle\langle h'|}_{=\rho_H} \otimes \underbrace{\frac{|H|}{|G|}\sum_{\bar{g}\in G/H}|g\rangle\langle g|}_{=\rho_{G/H}}. \tag{B21}$$

The factor ρ_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 its diagonal basis with eigenvalues $|H|/|G|$. The entropy of $\rho_G = \rho_2$ therefore is

$$H(\rho_G) = -\mathrm{Tr}_H(\rho_H\log_2\rho_H) - \mathrm{Tr}_{G/H}(\rho_{G/H}\log_2\rho_{G/H}) \tag{B22}$$

$$= -\sum_{G/H}\frac{|H|}{|G|}\log_2\left(\frac{|H|}{|G|}\right) \tag{B23}$$

$$= +\log_2\left(\frac{|G|}{|H|}\right), \tag{B24}$$

which gives the entropy of the S register conditioned on G

$$H(S|G) = -\log_2\left(\frac{|G|}{|H|}\right). \tag{B25}$$

Up to the negative sign this is equal the maximal number $k := \log_2(|G|/|H|)$ of Bell pairs formed by qubits from the G and S register which can possibly be extracted from the HSP algorithm. ■

Lemma 2 (Existence of transformations saturating the bound). There exist local unitaries U_G and U_S which saturate the upper bound $\ell_{\max}$ of Bell pairs which can be factored from the state after the function oracle O_f.

Proof. We argue why operations U_G and U_S exist such that the result from Eq. (11) can be achieved. First, consider the G

register: If a choice of representative is made for each coset $\bar{g} \in G/H$, any element $g' \in G$ can be split as $g' = g + h$ with g the representative of $\bar{g}'$ and $h \in H$. Thus, there exists an invertible map on $\mathcal{H}_G$ such that $|g'\rangle \mapsto |h\rangle \otimes |g\rangle \in \mathcal{H}_H \otimes \mathcal{H}_{G/H}$. The states $\{|g\rangle\}_{g\in G}$ are orthonormal, thus, this map is unitary, we shall denote it by U_G. In comparison to the notation in step (3) from the paragraph about the classification of all qubit extraction procedures, we have $\mathcal{H}_{G/H} = \mathcal{H}_{B_1}$, $\mathcal{H}_H = \mathcal{H}_G^{(1)}$ and

$$U_G : \mathcal{H}_G \longrightarrow \mathcal{H}_H \otimes \mathcal{H}_{G/H}, \tag{B26}$$

$$|g'\rangle = |g + h\rangle \longmapsto |h\rangle \otimes |g\rangle. \tag{B27}$$

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 $\mathcal{H}_S$ may have more qubits than are actually needed to represent $\mathrm{im} f \subseteq S$. This overhead of qubits can be factored out by reordering the computational basis of $\mathcal{H}_S$ such that $|f(g)\rangle \mapsto |0\rangle \otimes |\tilde{f}(g)\rangle \in \mathcal{H}_S^{(1)} \otimes \mathcal{H}_{B_2}$. This operation is unitary and can be chosen such that for all representatives g, the states $|\tilde{f}(g)\rangle \in \mathcal{H}_{B_2}$ and $|g\rangle \in \mathcal{H}_{G/H}$ have the same computational representation. This transformation will be denoted by U_S. ■

Theorem 2 (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 1 can be used to solve the HSP.

Proof. Any local unitary U_G factoring the main register register $\mathcal{H}_G$ into $\mathcal{H}_H \otimes \mathcal{H}_{G/H}$ 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 $\mathcal{H}_H \otimes \mathcal{H}_{G/H}$. Pick some $g \in G$, then U_G factors the state $|g\rangle$ into two parts:

$$U_G|g\rangle = |h_g\rangle \otimes |[g]\rangle. \tag{B28}$$

Despite our ignorance about how the group structure is binarily encoded in the quantum registers $\mathcal{H}_H$ and $\mathcal{H}_{G/H}$, 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 $|[0]\rangle \in \mathcal{H}_{G/H}$ by computing $U_G|0\rangle = |h_0\rangle \otimes |[0]\rangle$.

(2) Pick any $|h\rangle_H \in \mathcal{H}_H$ and deduce $|h\rangle_G \in \mathcal{H}_G$ via

$$U_G^\dagger |h\rangle \otimes |[0]\rangle = |h\rangle \in \mathcal{H}_G. \tag{B29}$$

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 $\mathcal{H}_G$, we have access to an encoding $g \in G \mapsto |g\rangle \in \mathcal{H}_G$ while for $\mathcal{H}_H$ 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 $\chi_{\tilde{g}}$ from the standard algorithm solving the HSP in Appendix B 2, 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 2 is 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 2 (General local transformations of G and S). Define local transformations

$$U_G : \mathcal{H}_G \to \mathcal{H}_G^{(1)} \otimes \mathcal{H}_G^{(2)}, \tag{B30}$$

$$U_S : \mathcal{H}_S \to \mathcal{H}_S^{(1)} \otimes \mathcal{H}_S^{(2)}, \tag{B31}$$

which factor quantum states encoding elements in $g \in G$ and $s \in S$ according to

$$U_G|g\rangle = |g^{(1)}, g^{(2)}\rangle, \tag{B32}$$

$$U_S|s\rangle = |s^{(1)}, s^{(2)}\rangle. \tag{B33}$$

Similarly to the notation introduced in Eq. (B33), let us write for some state $|f(g)\rangle \in \mathcal{H}_S$, $U_S|f(g)\rangle = |f^{(1)}(g), f^{(2)}(g)\rangle$. Using this notation we can formulate two general conditions on transformations U_G and U_S:

Theorem 9 (General characterization of partial erasure transformations). If and only if the transformations U_G and U_S satisfy the two requirements

(1) For all $g, \tilde{g} \in G : f(g) = f(\tilde{g}) \to g^{(2)} = \tilde{g}^{(2)}$,

(2) The function $f^{(1)}(g)$ depends only on $g^{(1)}$ and $f^{(2)}(g) = g^{(2)}$ in the binary computational representation in $\mathcal{H}_S^{(2)} = (\mathbb{C}^2)^{\otimes k} = \mathcal{H}_G^{(2)}$,

they can factor out the entanglement in the form of ℓ 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

$$\rho_{GS} \mapsto \rho_{\tilde{G}\tilde{S}} \otimes (|\chi\rangle\langle\chi|)^{\otimes \ell}. \tag{B34}$$

We allow that U_G may only factor part of the register $\mathcal{H}_{G/H}$, say $k \leqslant |G|/|H|$ qubits. The transformations need not necessarily respect the group structure of G; hence, we refrain from using an intermediate subgroup K as in the main part of the paper but rather work with the factorization from Definition 2. Starting with the state ρ_2 after step 2 of the standard HSP algorithm (see Fig. 5 and Appendix B 2), we find a new state ρ_{2a}:

$$\rho_{2a} = (U_G \otimes U_S)\rho_2(U_G^\dagger \otimes U_S^\dagger) \tag{B35}$$

$$= \frac{1}{|G|} \sum_{g,\tilde{g}\in G} |g^{(1)}, g^{(2)}\rangle\langle\tilde{g}^{(1)}, \tilde{g}^{(2)}| \otimes |f^{(1)}(g), f^{(2)}(g)\rangle \times \langle f^{(1)}(\tilde{g}), f^{(2)}(\tilde{g})| \tag{B36}$$

$$\overset{\heartsuit}{=} \frac{1}{|G|} \left\{ \sum_{g^{(1)},\tilde{g}^{(1)}} |g^{(1)}\rangle\langle\tilde{g}^{(1)}| \otimes |f^{(1)}(g^{(1)})\rangle\langle f^{(1)}(\tilde{g}^{(1)})| \right\} \tag{B37}$$

$$\otimes \left\{ \sum_{g^{(2)},\tilde{g}^{(2)}} |g^{(2)}\rangle\langle\tilde{g}^{(2)}| \otimes |f^{(2)}(g^{(2)})\rangle\langle f^{(2)}(\tilde{g}^{(2)})| \right\} \tag{B38}$$

$$= \frac{1}{\dim \mathcal{H}_G^{(1)}} \left\{ \sum_{g^{(1)},\tilde{g}^{(1)}} |g^{(1)}\rangle\langle\tilde{g}^{(1)}| \otimes |f^{(1)}(g^{(1)})\rangle\langle f^{(1)}(\tilde{g}^{(1)})| \right\} \otimes (|\chi\rangle\langle\chi|)^{\otimes k}. \tag{B39}$$

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

Remark. The transformations U_G and U_S from Promise 2 where one has partial information on an intermediate subgroup $H \subseteq K \subseteq G$ are a special case of the transformations from Theorem 9 with

$$\mathcal{H}_G^{(1)} = \mathcal{H}_K, \text{ and } \mathcal{H}_G^{(2)} = \mathcal{H}_{G/K}, \tag{B40}$$

as this decomposition satisfies all two assumptions from Theorem 7.

Theorem 10 (Work cost of erasure with partial information, general version). Given the transformations U_G and U_S from Definition 2 and Theorem 9, 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

$$W = (m - 2\ell)k_B T \ln 2, \tag{B41}$$

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 of state of the circuit from Fig. 7 is reproduced here in order to show it coincides with the one from the standard HSP algorithm in Fig. 5.

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

$$\rho_2 = \frac{1}{|G|} \sum_{\substack{\tilde{g},\tilde{g}' \in \\ G/H}} \left\{ \sum_{\substack{h,h' \in \\ H}} |g+h\rangle\langle g'+h'| \right\} \otimes |f(g)\rangle\langle f(g')|. \tag{B42}$$

Steps 2a–2c. Applying the operation $U_G \otimes U_S$ to the state ρ_2 gives (see calculation in proof of Theorem 9)

$$\begin{aligned} \rho_{2a} &= (U_G \otimes U_S)\rho_2(U_G^\dagger \otimes U_S^\dagger) \\ &= \frac{1}{\dim \mathcal{H}_G^{(1)}} \left\{ \sum_{g^{(1)},\tilde{g}^{(1)}} |g^{(1)}\rangle\langle\tilde{g}^{(1)}| \right. \\ &\quad \left. \otimes |f^{(1)}(g^{(1)})\rangle\langle f^{(1)}(\tilde{g}^{(1)})| \right\} \otimes (|\chi\rangle\langle\chi|)^{\otimes k}. \end{aligned} \tag{B43}$$

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

$$W^{(1)} = \dim\left(\mathcal{H}_S^{(1)}\right) k_B T \ln 2 = (m-\ell) k_B T \ln 2. \tag{B44}$$

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

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

which amounts to a total average work cost of erasure

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

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

$$\rho'_{2c} = \frac{1}{|G|} \sum_{\tilde{g} \in G/H} \left\{ \sum_{h,h' \in H} |g+h\rangle\langle g+h'| \right\}, \tag{B47}$$

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 2 which are used in Theorem 9 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, Sec. III C 1). 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 2). There, the transformations U_G and U_S act on a state $|g, f(g)\rangle$ as

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

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, $\mathcal{H}_K = \text{span}_{\mathbb{C}}\{|k\rangle : k \in K\}$ 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 Sec. III C 1.

APPENDIX C: PROOFS: ORACLE SIMPLIFICATION IN THE HIDDEN SUBGROUP PROBLEM

This Appendix is dedicated to proving Theorem 4 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 Fig. 8 with the simplified algorithm.

Theorem 4 (Partial information correspondence). The unitaries U_G and U_S from Promise 2 can be used to formally construct a new function oracle $\tilde{O}_f$ which requires 2ℓ 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 ρ_i for the algorithm in the circuit of Fig. 8 is performed, with $1 \leqslant i \leqslant 6$ indexing the steps defined there.

Steps 1–2. The sum $\sum_k$ is implicitly over the range of the first factor in $\{|k,t\rangle = U_G|g\rangle : g \in G\} \subseteq \mathcal{H}_K \otimes \mathcal{H}_{G/K}$. Then

$$\rho_1 = \frac{1}{|K|}\sum_{k,\tilde{k}} |k,0\rangle\langle\tilde{k},0| \otimes |0\rangle\langle 0| \tag{C1}$$

$$\xmapsto{U_G^\dagger \otimes \mathbb{1}_S} \frac{1}{|K|}\sum_{k,\tilde{k}} \underbrace{U_G^\dagger|k,0\rangle}_{=:|g(k,0)\rangle}\langle\tilde{k},0|U_G \otimes |0\rangle\langle 0| = \rho_2. \tag{C2}$$

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

$$\rho_2 \xmapsto{O_f} \frac{1}{|K|}\sum_{k,\tilde{k}} U_G^\dagger|k,0\rangle\langle\tilde{k},0|U_G \otimes |f(g(k,0))\rangle\langle f(g(\tilde{k},0))| \tag{C3}$$

$$\xmapsto{U_G \otimes U_S} \frac{1}{|K|}\sum_{k,\tilde{k}} |k,0\rangle\langle\tilde{k},0| \otimes |f^{(1)}(k),0\rangle\langle f^{(1)}(\tilde{k}),0| = \rho_4. \tag{C4}$$

For the last equality we used property 2 imposed in Theorem 9. At this stage we see that $\tilde{O}_f$ acts trivially on the registers $\mathcal{H}_G^{(2)} = \mathcal{H}_{G/K}$ and $\mathcal{H}_S^{(2)}$, saving 2ℓ 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

$$\rho_4' = \mathrm{Tr}_{\mathcal{H}_{G/K}\otimes\mathcal{H}_S}\,\rho_4 \tag{C5}$$

$$= \frac{1}{|K|}\sum_{\bar{k}\in K/H}\left\{\sum_{h,h'\in H}|k+h\rangle\langle k+h'|\right\} \tag{C6}$$

be the reduced state of ρ_4 where all registers but $\mathcal{H}_K$ have been traced out. Observing $H \subseteq K$, the quantum Fourier transform Q_K acts on ρ_4' as

$$\rho_4' \xmapsto{Q_K} \frac{1}{|K|}\sum_{\bar{k}\in K/H}\left\{\sum_{h,h'\in H}|\chi_{k+h}\rangle\langle\chi_{k+h'}|\right\} \tag{C7}$$

$$= \left(\frac{|H|}{|K|}\right)^2 \sum_{\bar{k}\in K/H}\left\{\sum_{g,g'\in H_K^\perp}\chi_k(g)\chi_k(g')|g\rangle\langle g'|\right\}, \tag{C8}$$

where $H_{K^\perp} = \{g \in K : \forall h \in H : \chi_g(h) = 1\}$ is the analog of $H^\perp$ 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. ■

[1] R. Landauer, Irreversibility and heat generation in the computing process, IBM J. Res. Dev. **5**, 183 (1961).

[2] C. H. Bennett, The thermodynamics of computation—A review, Int. J. Theor. Phys. **21**, 905 (1982).

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

[4] A. Baumeler and S. Wolf, Free energy of a general computation, Phys. Rev. E **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 (London) **476**, 476 (2011).

[6] M. A. Nashiry and J. E. Rice, A reversible majority voter circuit and applications, in *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), Victoria, BC, Canada* (IEEE, 2017).

[7] M. Lostaglio, An introductory review of the resource theory approach to thermodynamics, Rep. Prog. Phys. **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, Phys. Rev. Lett. **111**, 250404 (2013).

[9] Z.-W. Liu, K. Bu, and R. Takagi, One-Shot Operational Quantum Resource Theory, Phys. Rev. Lett. **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. Boechler, and G. L. Snider, Experimental test of Landauer's principle at the sub-k_BT level, Jpn. J. Appl. Phys. **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, Proc. Natl. Acad. Sci. U. S. A. **111**, 13786 (2014).

[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, J. Phys. A: Math. Theor. **49**, 143001 (2016).

[15] F. Binder, L. A. Correa, C. Gogolin, J. Anders, and G. Adesso (eds.), *Thermodynamics in the Quantum Regime*, Fundamental Theories of Physics Vol. 195 (Springer International Publishing, Cham, 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?, arXiv:2106.05151 [quant-ph].

[17] A. Auffèves, Quantum Technologies need a quantum energy initiative, PRX Quantum **3**, 020101 (2022).

[18] L. d. Rio, J. Åberg, R. Renner, O. Dahlsten, and V. Vedral, The thermodynamic meaning of negative entropy, Nature (London) **474**, 61 (2011).

[19] F. G. S. L. Brandão and G. Gour, Reversible Framework for Quantum Resource Theories, Phys. Rev. Lett. **115**, 070503 (2015).
[20] P. Skrzypczyk, A. J. Short, and S. Popescu, Work extraction and thermodynamics for individual quantum systems, Nat. Commun. **5**, 4185 (2014).
[21] C. H. Bennett, Notes on Landauer's principle, reversible computation, and Maxwell's Demon, Stud. Hist. Philos. Sci. B **34**, 501 (2003).
[22] M. Mosca and A. Ekert, The hidden subgroup problem and eigenvalue estimation on a quantum computer, in *Quantum Computing and Quantum Communications*, edited by C. P. Williams (Springer, Berlin, 1999), pp. 174–188.
[23] R. de Wolf, Quantum computing: Lecture notes, arXiv:1907.09415 [quant-ph].
[24] M. Mosca, Abelian Hidden subgroup problem, in *Encyclopedia of Algorithms*, edited by M.-Y. Kao (Springer US, Boston, 2008), pp. 1–4.
[25] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. **26**, 1484 (1997).
[26] A. Y. Kitaev, Quantum measurements and the Abelian Stabilizer Problem, arXiv:quant-ph/9511026 [quant-ph].
[27] M. Ettinger, P. Høyer, and E. Knill, The quantum query complexity of the hidden subgroup problem is polynomial, Inf. Proc. Lett. **91**, 43 (2004).
[28] N. J. Cerf and C. Adami, Negative entropy in quantum information theory, in *New Developments on Fundamental Problems in Quantum Physics*, edited by M. Ferrero and A. van der Merwe (Springer Netherlands, Dordrecht, 1997), pp. 77–84.
[29] N. J. Cerf and C. Adami, Negative Entropy and Information in Quantum Mechanics, Phys. Rev. Lett. **79**, 5194 (1997).
[30] N. Friis, S. Bulusu, and R. A. Bertlmann, Geometry of two-qubit states with negative conditional entropy, J. Phys. A: Math. Theor. **50**, 125301 (2017).
[31] V. Shende, A. Prasad, I. Markov, and J. Hayes, Synthesis of reversible logic circuits, IEEE Trans. Comput-Aided Design Integrat. Circuits Syst. **22**, 710 (2003).
[32] M. Horodecki and J. Oppenheim, Fundamental limitations for quantum and nanoscale thermodynamics, Nat. Commun. **4**, 2059 (2013).
[33] G. M. Andolina, M. Keck, A. Mari, M. Campisi, V. Giovannetti, and M. Polini, Extractable Work, the Role of Correlations, and Asymptotic Freedom in Quantum Batteries, Phys. Rev. Lett. **122**, 047702 (2019).
[34] P. Lipka-Bartosik, P. Mazurek, and M. Horodecki, Second law of thermodynamics for batteries with vacuum state, Quantum **5**, 408 (2021).
[35] D. K. Park, N. A. Rodriguez-Briones, G. Feng, R. Rahimi, J. Baugh, and R. Laflamme, Heat bath algorithmic cooling with spins: Review and prospects, in *Electron Spin Resonance (ESR) Based Quantum Computing*, edited by T. Takui, L. Berliner, and G. Hanson (Springer New York, New York, 2016), pp. 227–255.
[36] Á. M. Alhambra, M. Lostaglio, and C. Perry, Heat-bath algorithmic cooling with optimal thermalization strategies, Quantum **3**, 188 (2019).
[37] R. Soldati, D. B. R. Dasari, J. Wrachtrup, and E. Lutz, Thermodynamics of a Minimal Algorithmic Cooling Refrigerator, Phys. Rev. Lett. **129**, 030601 (2022).
[38] A. Serafini, M. Lostaglio, S. Longden, U. Shackerley-Bennett, C.-Y. Hsieh, and G. Adesso, Gaussian Thermal Operations and the Limits of Algorithmic Cooling, Phys. Rev. Lett. **124**, 010602 (2020).
[39] D. Egloff, O. C. O. Dahlsten, R. Renner, and V. Vedral, A measure of majorization emerging from single-shot statistical mechanics, New J. Phys. **17**, 073001 (2015).
[40] J. Åberg, Truly work-like work extraction via a single-shot analysis, Nat. Commun. **4**, 1925 (2013).
[41] D. Reeb and M. M. Wolf, An improved Landauer principle with finite-size corrections, New J. Phys. **16**, 103011 (2014).
[42] J. G. Richens, A. M. Alhambra, and L. Masanes, Finite-bath corrections to the second law of thermodynamics, Phys. Rev. E **97**, 062132 (2018).
[43] O. Gühne and G. Tóth, Entanglement detection, Phys. Rep. **474**, 1 (2009).
[44] C. Li, B.-H. Wang, B. Wu, and X. Yuan, Detecting entanglement of quantum channels, Commun. Theor. Phys. **73**, 115101 (2021).
[45] W. Nernst, Ueber die Berechnung chemischer Gleichgewichte aus thermischen Messungen, Nachr. Ges. Wiss. Göttingen, Math.-Phys. Klasse **1906**, 1 (1906).
[46] W. Nernst, Über die Beziehung zwischen Wärmeentwicklung und maximaler Arbeit bei kondensierten Systemen, Ber. Kgl. Pr. Akad. Wiss. **52**, 933 (1906).
[47] H. Wilming and R. Gallego, Third Law of Thermodynamics as a Single Inequality, Phys. Rev. X **7**, 041033 (2017).
[48] N. Freitas, R. Gallego, L. Masanes, and J. P. Paz, Cooling to absolute zero: The unattainability principle, in *Thermodynamics in the Quantum Regime*, edited by F. Binder, L. Correa, C. Gogolin, J. Anders, and G. Adesso, Fundamental Theories of Physics Vol. 195 (Springer, Cham, 2018), p. 597.
[49] F. Clivaz, R. Silva, G. Haack, J. B. Brask, N. Brunner, and M. Huber, Unifying paradigms of quantum refrigeration: Fundamental limits of cooling and associated work costs, Phys. Rev. E **100**, 042130 (2019).
[50] W. Pusz and S. L. Woronowicz, Passive states and KMS states for general quantum systems, Commun. Math. Phys. **58**, 273 (1978).
[51] P. Skrzypczyk, R. Silva, and N. Brunner, Passivity, complete passivity, and virtual temperatures, Phys. Rev. E **91**, 052133 (2015).
[52] J. J. Rotman, *Advanced Modern Algebra, Part I*, 3rd ed. (American Mathematical Society, Providence, RI, 2015).
[53] W. Fulton and J. Harris, *Representation Theory: A First Course*, Graduate Texts in Mathematics (Springer, New York, 2004).