

Manuscript version: Published Version

The version presented in WRAP is the published version (Version of Record).

Persistent WRAP URL:

<http://wrap.warwick.ac.uk/128163>

How to cite:

The repository item page linked to above, will contain details on accessing citation guidance from the publisher.

Copyright and reuse:

The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions.

Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

Publisher's statement:

Please refer to the repository item page, publisher's statement section, for further information.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk

Fault-tolerant quantum metrology

Theodoros Kapourniotis and Animesh Datta

Department of Physics, University of Warwick, Coventry CV4 7AL, England, United Kingdom

 (Received 13 July 2018; revised manuscript received 9 April 2019; published 27 August 2019)

We introduce the notion of fault-tolerant quantum metrology to overcome noise beyond our control, associated with sensing the parameter, by reducing the noise in operations under our control, associated with preparing and measuring probes and ancillae. To that end, we introduce noise thresholds to quantify the noise resilience of parameter estimation schemes. We demonstrate improved noise thresholds over the non-fault-tolerant schemes. We use quantum Reed-Muller codes to retrieve more information about a single phase parameter being estimated in the presence of full-rank Pauli noise. Using only error detection, as opposed to error correction, allows us to retrieve higher thresholds. We show that better devices, which can be engineered, can enable us to counter larger noise in the field beyond our control. Further improvements in fault-tolerant quantum metrology could be achieved by optimizing in tandem parameter-specific estimation schemes and transversal quantum error correcting codes.

DOI: [10.1103/PhysRevA.100.022335](https://doi.org/10.1103/PhysRevA.100.022335)

I. INTRODUCTION

Like all quantum information processing tasks, noise has an adverse effect on quantum enhancements in precision metrology. Early promises of a quantum-enhanced “Heisenberg scaling” are now tempered by its elusiveness even in the presence of arbitrarily small noise in the sensing process [1,2]. After some early musings [3,4], much effort has been directed towards recovering the Heisenberg scaling using quantum error correction [5–11]. More recent results suggest the impossibility of recovering the Heisenberg scaling in the presence of general Markovian noise if the Hamiltonian lies in the span of the noise operators, even after quantum error correction [12,13]. Studies of error-corrected quantum metrology have focused on either specific experimental systems [9,11,14,15] or specific forms of noise affecting the field [6,9]. Others have assumed instantaneous and perfect correction and control operations [8,9,12,13] or short sensing times to commute noise to the end of the protocol [6,7,10]. These assumptions are unlikely to hold in general.

In this paper, we take a complementary approach by initiating the study of fault-tolerant (FT) quantum metrology. Instead of lower bounds and asymptotic scalings, we focus on the estimation of a phase parameter ϕ associated with the field

$$R_z(\phi) = \exp\left(-i\frac{\phi}{2}Z\right), \quad (1)$$

up to a fixed number of bits, where $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$. We show that ϕ can be estimated to more bits of precision with our FT quantum metrology protocol, in the presence of noise, than without it. This is achieved by introducing the concept of *thresholds* to noisy quantum metrology, providing experimentalists with quantitative targets to aim for. Our illustration uses a specific phase estimation scheme and code switching between Steane and other quantum Reed-Muller codes (QRMCs) to counter locally bounded full-rank noise

beyond our control, associated with the parameter or field being sensed, as well as *under* our control, in preparing, entangling, and measuring probes and ancilla. We call the latter “devices.” We do not assume short sensing times or perfect control operations. We show in Fig. 6 that better devices, which can be engineered, can enable us to counter more noise in the field beyond our control. Our results for fault-tolerant quantum metrology can also be extended to other sensing and estimating applications, such as clock synchronization [16] and systematic error estimation and calibration [17].

In contrast to previous approaches of error-corrected quantum metrology such as Refs. [6,12,13,18], as well as ancilla-assisted quantum metrology schemes [19], our FT quantum metrology framework enables a meaningful quantitative analysis of the noise in devices in addition to that in the field. Recast in terms of noise thresholds, these prior works on quantum metrology with perfect error correction correspond to the dotted blue line in Fig. 6. The dashed blue line shows the depreciating performance of an error-corrected quantum metrology scheme due to noisy devices. Our main result is the solid green/light-gray line in Fig. 6 that shows the possibility of improvement using fault-tolerant quantum metrology.

This paper is organized as follows. In Sec. II, we introduce the notion of fault tolerance in quantum metrology, comparing and contrasting it with the more familiar notion of fault tolerance in quantum computing. Section III presents our main results, culminating in Fig. 6. The subsequent sections provide the technical details and proofs. Section IV provides formal convergence, noise resilience, and resource analysis of a modified estimation scheme [20]. Section V calculates the effect of applying logical $R_z(\phi)$, which is nontransversal for QRMCs in general. Section VI calculates failure probabilities of error detection when devices are perfect. Section VII analyzes the performance of the protocols when devices are not perfect. Finally, Sec. VIII presents the parallel version of our protocols and Sec. IX discusses prospects and open questions in fault-tolerant quantum metrology.

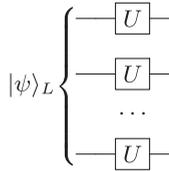


FIG. 1. Single-qubit state $|\psi\rangle$ is encoded into multiqubit state $|\psi\rangle_L$ in order to detect or correct errors on few qubits. Transversal application of unitary gate U means bitwise application of U on physical qubits of $|\psi\rangle_L$. It outputs the encoded state of state $U|\psi\rangle$.

II. FAULT TOLERANCE AND METROLOGY

We treat phase estimation as a quantum circuit, composed of the probe and ancilla state preparations and measurements as well as the application of the $R_z(\phi)$ gate. The central difference between FT quantum metrology and computing is that ϕ is unknown in the former while it is known in the latter. The only way to apply $R_z(\phi)$ is by interrogating the field.

Quantum information can be protected against bounded noise by using a quantum error correcting code (QECC). In order to protect it while it dynamically undergoes computation one can apply the procedures of fault tolerance. Fault tolerance encompasses a set of procedures for preparing encoded states, applying encoded gates, and measuring encoded states. If ϕ is known, as is the case in computing, a fault-tolerant encoding of $R_z(\phi)$ in Eq. (1) can be accomplished. This relies on the existence of a fault-tolerant set of gates from which to build a fault-tolerant circuit. The main property of these procedures is that an error in one component in a FT encoding results in no more than one error in the entire encoded block [21]. As ϕ is unknown in metrology, we cannot undertake its fault-tolerant encoding directly. Fault-tolerant quantum metrology thus operates by performing fault tolerance before and after the field $R_z(\phi)$ is sensed, as in Fig. 3(b).

A desirable design principle in fault tolerance is to limit the proliferation of noise from one part of the circuit to another. This is called transversality and is the requirement that each physical gate employed for the encoded gate acts on at most one physical qubit in each code block [22], as shown in Fig. 1. Since in FT quantum metrology only single qubit gates $R_z(\phi)$ are applied during the interrogation of the field, as shown in Fig. 3, transversality comes naturally. It results in errors on a single physical qubit not propagating to more physical qubits of the same block in a single fault-tolerant gate procedure.

If we restrict ourselves to the well-studied family of stabilizer codes, we cannot hope for a code transversal for $R_z(\phi)$, $\forall \phi \in [0, 2\pi]$. This is because for stabilizer codes all transversal gates reside at a finite level of the Clifford hierarchy [23] (for details see Appendix A). We must therefore move to a digital representation of the phase parameter $\phi = 2\pi \times 0.b_0b_1b_2\dots = b_0\pi + b_1\pi/2 + b_2\pi/4 + \dots$ with $b_n \in \{0, 1\}$. Defining $T_n \equiv \text{diag}(1, e^{i2\pi/2^n})$, Eq. (1) can be reexpressed as $R_z(\phi) = T_1^{b_0} T_2^{b_1} \dots$. Thus, the field interrogation effectively does or does not apply the gate T_n depending on whether $b_n = 0$ or 1, respectively. For n higher than what our transversal code can support, there is a corruption of the logical subspace. We prove in Sec. V that this effect is bounded and that using stabilizer codes can even be benefi-

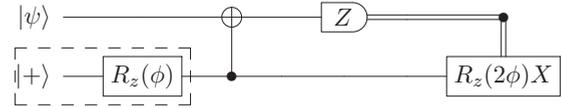


FIG. 2. Gate teleportation: All operations outside the dashed box are protected by a code transversal for $\{cX, H, Z\}$. The unitary correction depends on parameter ϕ and since it is not transversal for the code it requires an extra round of distillation.

cial in our construction. Since any real-world task must use finite resources, we capture the performance of FT quantum metrology in the number of bits of ϕ estimated. Incidentally, digital quantum metrology has been studied for independent reasons [24].

Other design principles of fault-tolerant quantum computing include gate synthesis or approximation to acquire a FT gate set [25], distillation of so-called magic states [26], and state twirling to diagonalize the noise in the magic state basis [27]. In the following, we briefly describe why these cannot be applied to FT quantum metrology in their original form and the modifications we resort to.

Gate synthesis replaces gates that do not belong to the FT set by approximate decompositions of gates of that set. This cannot be applied in FT quantum metrology since we cannot write a decomposition of the gate $R_z(\phi) = T_1^{b_0} T_2^{b_1} \dots$ when the bits b_n are unknown. The only way to apply the gate is by interrogating the field. This results in using a larger block size QECC for retrieving more bits of the unknown parameter in our FT quantum metrology scheme.

The gates involved in the encoding operations [Hadamard and controlled-NOT (CNOT)] and the field $[R_z(\phi) = T_1^{b_0} T_2^{b_1} \dots]$ form a gate set universal for quantum computing. The well-studied family of stabilizer codes is known not to be transversal for a universal set of gates [28]. A solution is to inject external states into the logical circuit in order to apply the corresponding gates. Distillation is a series of operations that gives a high fidelity state out of many low fidelity states and is necessary because the external state is noisy in general. It is accompanied by gate teleportation to apply the corresponding gate at any stage of the circuit, as shown in Fig. 2. This circuit cannot be implemented in our FT quantum metrology scheme, once again because of the unknown ϕ -dependent correction operator in the teleportation step. An alternative solution, which avoids teleportation, is code switching. It switches between codes that are transversal for different subsets of gates. We use this solution (Sec. VII B), which has implications on the noise threshold of our scheme.

State twirling is the application of a randomizing operation that diagonalizes the noise on a state in a basis that is defined by the state. It reduces the types of logical noise that need to be treated in a FT circuit. In our FT quantum metrology scheme, this also cannot be applied because after the first interrogation the state depends on the unknown parameter ϕ . FT quantum metrology thus needs to treat full-rank noise in its entirety.

The culmination of a fault-tolerant approach is the threshold. The noise threshold for FT quantum metrology we define as the strength of noise [29] below which the estimator for the parameter converges. It depends on the type of noise,

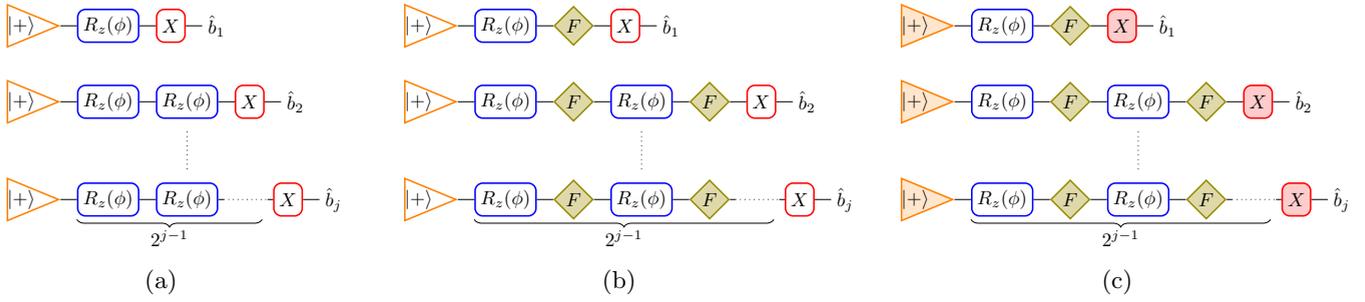


FIG. 3. Three serial quantum metrology protocols for estimating j bits of the phase ϕ : (a) Protocol Ia, (b) Protocol Ib, and (c) Protocol Ic. Blue boxes denote the field to be sensed, with its allied noise beyond our control. Orange triangles are inputs and red boxes are measurements, both under our control. The protocols start with the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ probes. Green rhombuses denote fault tolerance interleaved with sensing the field. Filled shapes denote FT implementations.

the estimation scheme, and the QECC used. Indeed, our FT metrology scheme provides two thresholds—one for the noise in the field which contains the parameter and another for the devices that perform the preparation, encoding, and measurements of the probes and ancilla. One of our main results as shown in Fig. 6 is that if the noise in the devices is below a certain threshold then the threshold for the noise in the field is larger.

In FT quantum computing using gate distillation, a base code transversal only for Clifford gates with high noise threshold such as the surface code [30] can be used. Furthermore, the distillation is based on error detection rather than error correction, which contributes to a higher threshold. In FT quantum metrology where we have to use code switching, estimating bit b_n requires us to employ a code that is transversal for T_n . In this paper, we use QRMCs. The search for QECCs with better performance, in terms of code lengths and thresholds, should be one of the central aims of improving FT quantum metrology in future works.

Encoding

QRMCs are quantum stabilizer codes constructed from classical Reed-Muller codes $\text{RM}(r, m)$. $\text{RM}(r, m)$ have order r and block length 2^m for $0 \leq r \leq m$ [31]. The QRMC $\text{QRM}(1, m)$ has a block size of $2^m - 1$ qubits, encodes one qubit, and has a minimum distance of 3. Transversality of QRMCs enables a logical operation on a logical state by applying transversal gates on the $2^m - 1$ physical qubits. We choose $\text{RM}(1, n + 1)$ as the basis for the QRMCs, which are transversal for T_j , $j \leq n$ [32]. However, these QRMCs are not transversal for T_j for $j > n$. The effect of these post-transversal rotations is subtle and needs to be counteracted in FT metrology. Applying T_n transversally on $\text{QRM}(1, n + 1)$ applies the logical T_n^\dagger gate.

III. RESULTS

Quantum phase estimation can be performed in series. It can also be performed in parallel where multiple qubits in an entangled state interrogate the field simultaneously. They perform similarly to serial strategies where a single qubit interrogates the field multiple times coherently. See Sec. VIII.

We introduce fault tolerance into quantum metrology in three stages. The first, Protocol Ia [Fig. 3(a)], is affected by

noise everywhere but uses no fault tolerance. It serves as our benchmark. The second, Protocol Ib [Fig. 3(b)], comes in two types—with noiseless and noisy devices—but uses fault tolerance to counteract noise in the field only. The third, Protocol Ic [Fig. 3(c)], is affected by noise in both the field and devices and uses fault tolerance to counteract them both. These protocols can be applied to any phase estimation scheme. Since different phase estimation schemes perform differently under noise, their FT threshold improvements and resource requirements will be different.

We illustrate the above methodology for a phase estimation scheme due to Rudolph and Grover (RG) [20], which we choose for its operational simplicity. The RG protocol performs bitwise phase estimation, is nonadaptive, and requires only a Pauli X measurement. The original RG protocol cannot estimate all possible phases—it has an excluded region [33] captured by a parameter γ . We now present our main results.

A. No fault tolerance

For any bit b_j , we denote its estimate as \hat{b}_j . The RG scheme assumes $0 \leq \phi < \pi$, from which we have that $\hat{b}_0 = 0$. We use it to estimate the unknown phase ϕ to t bits. This phase estimation protocol, labeled Protocol Ia, is presented below and depicted in Fig. 3(a). The protocol converges if it outputs the first t bits of ϕ with confidence ϵ .

Protocol Ia

For $j = 1, \dots, t$

1. Repeat M times.
 - (i) Prepare $|+\rangle$.
 - (ii) Interrogate field 2^{j-1} times.
 - (iii) Measure X .
2. Calculate \hat{p}_j as the fraction of the $+1$ measurement outcomes out of M . If $\hat{b}_{j-1} = 0$ set $\hat{\phi}_j = \cos^{-1}(2\hat{p}_j - 1)$ in $[0, \pi]$, or else in $[\pi, 2\pi]$.
 - (i) If $\hat{b}_{j-1}\pi \leq \hat{\phi}_j < \hat{b}_{j-1}\pi + (\pi/2 - \gamma)$, set $\hat{b}_j = 0$.
 - (ii) If $\hat{b}_{j-1}\pi + (\pi/2 + \gamma) \leq \hat{\phi}_j \leq \hat{b}_{j-1}\pi + \pi$, set $\hat{b}_j = 1$. Otherwise output estimate up to bit $j - 1$ and exit.
3. If $j \neq t$ increase j by one and go to step 1, otherwise exit and output

$$\hat{\phi} = \hat{b}_1 \frac{\pi}{2} + \hat{b}_2 \frac{\pi}{4} + \dots + \hat{b}_t \frac{\pi}{2^t}.$$

In the noiseless case, this protocol converges everywhere except for ϕ in between the decision boundaries—called the

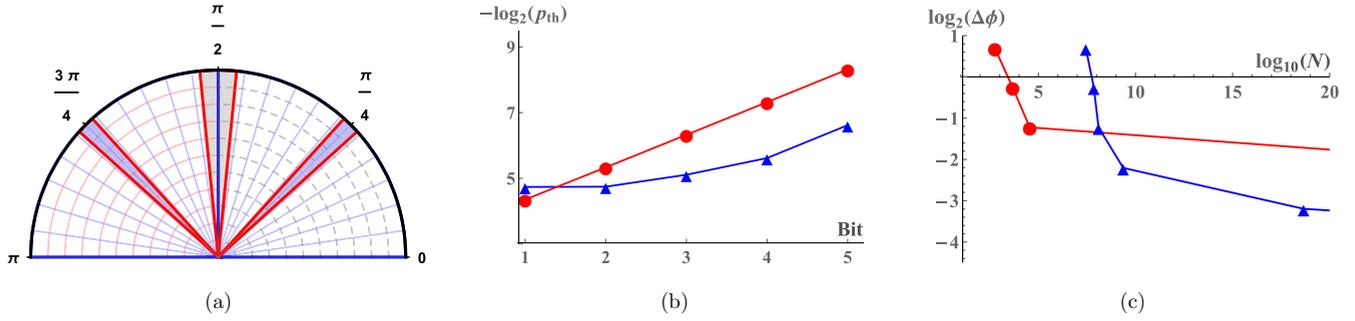


FIG. 4. (a) Scheme with $\gamma = \pi/32$. The allowed region for ϕ is divided into $[0, \pi/2]$ and $[\pi/2, \pi)$. The decision boundaries are the red lines. For $j = 1$ the excluded region (gray) is centered around $\pi/2$. For $j = 2$, the excluded region (blue) is centered either around $\pi/4$ if $b_1 = 0$ or around $3\pi/4$ if $b_1 = 1$. This pattern continues for $j > 2$. (b) Noise thresholds for $\gamma = \pi/32$. Red circles, Protocol Ia; blue triangles, Protocol Ib. That the blue line is below the red demonstrates the benefits of FT phase estimation for higher bits. (c) Standard deviation vs resources for $\gamma = \pi/32$, $p = 0.63\%$. Red circles, Protocol Ia; blue triangles, Protocol Ib; markers denote bits starting from 1 and increasing left to right. Improvement from fault tolerance appears in estimating higher bits. See Appendix C for other values of γ .

excluded region—which depend on γ [Fig. 4(a)]. In the latter case, we abort the protocol. The total range of the excluded angles in the worst case, when there are no overlapping excluded regions, is $2t\gamma$. This and the convergence of Protocol Ia are proven in Sec. IV.

In the noisy case, we define the noise threshold as the probability p below which Protocol Ia converges. We consider full-rank noise, which can occur at any point before, during, or after the interaction of the probe with the field, of the form

$$\mathcal{E}(\rho) = (1 - p)\rho + p(p_x X\rho X + p_y XZ\rho ZX + p_z Z\rho Z), \quad (2)$$

where $1 \geq p$, $p_{x,y,z} \geq 0$ and add up to 1. This incorporates parallel noise ($p_x = p_y = 0$), perpendicular noise ($p_z = p_y = 0$), and combinations thereof.

Several recent works have studied the effect of noise of various ranks on the scaling of precision of phase estimation [15,34–36]. All our results are valid for all allowed values of $p_{x,y,z}$.

Mathematically, Protocol Ia converges for $p < p_{\text{th}}$, where the threshold for the noise affecting the field p_{th} is the solution of (see Sec. IV B)

$$1 - (1 - p)^{2^{t-1}} = \delta(\gamma) = |\sin \gamma|/2. \quad (3)$$

The robustness of Protocol Ia against noise depends on γ . A larger γ excludes more angles but makes the protocol more robust against noise. Our FT protocols overcome this tradeoff. The threshold p_{th} obtained from Eq. (3) and presented in Fig. 4(b) sets the benchmark against which we compare our next two FT protocols. A larger p_{th} denotes a greater resilience to noise.

The number of field interrogations, our resource, required for Protocol Ia to converge is (see Sec. IV B)

$$N = (2^t - 1) \frac{1}{2[\delta(\gamma) - p_f]^2} \ln \left(\frac{2t}{\epsilon} \right), \quad (4)$$

where $p_f = 1 - (1 - p)^{2^{t-1}}$. We plot the standard deviation of our estimate $\Delta\phi$ against the resources required for this protocol for a fixed p and γ in Fig. 4(c). If $p \ll p_{\text{th}}$ for a given t , $\Delta\phi = O(\log N/N)$, where the logarithmic term appears due to bitwise estimation [20] and the $1/N$ term represents the Heisenberg scaling in very low noise.

B. Error detection against field noise

First we assume noiseless devices. Protocol Ib begins by creating a Bell state between the probe and an ancilla. The probe is then encoded using QRMCs. The encoded subsystem interrogates the field transversally and is measured in the logical X basis. This, along with appropriate local correction, teleports information of ϕ onto the ancillae at the physical level. This process, represented by the green rhombuses and blue boxes in Fig. 3(b), is repeated 2^{j-1} times, using the output of one step as the input to the next to estimate b_j . Protocol Ib combats noise of the form of Eq. (2) in the field using error detection.

Protocol Ib

For $j = 1, \dots, t$

1. Repeat M times.
 - (i) Prepare probe $|+\rangle$. Set $k = 1$.
 - (ii) Prepare ancilla $|0\rangle$. Apply CNOT between probe and ancilla. Encode probe by QRM(1, $j + 2$).
 - (iii) Interrogate field transversally with probe. Apply error detection on probe. Restart (i) if syndrome measurements reject.
 - (iv) Teleport by measuring probe in logical X and adapting Pauli frame accordingly (see Fig. (5)).
 - (v) If $k < 2^{j-1}$, increase k by one, use ancilla as new probe, and return to (ii).
 - (vi) Measure X .
2. Step 2 of Protocol Ia with γ replaced by γ' .
3. If $j \neq t$ increase j by one and go to step 1, otherwise exit and output

$$\hat{\phi} = \hat{b}_1 \frac{\pi}{2} + \hat{b}_2 \frac{\pi}{4} + \dots + \hat{b}_t \frac{\pi}{2^t}.$$

The decision boundaries of Protocol Ib are defined by parameter γ' —the “logical” version of γ . This difference arises if $R_z(\phi)$ is not transversal for the QRMCs. If γ was the physical rotation, the logical state after step 1(iv) of Protocol Ib undergoes a Z rotation by (Lemma 1, Sec. V)

$$\gamma' = \gamma - 2 \arctan \left(\frac{\sin(2^{j+1}\gamma)}{(2^{j+2} - 1) + \cos(2^{j+1}\gamma)} \right). \quad (5)$$

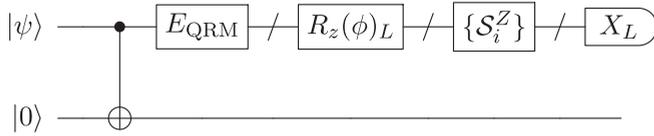


FIG. 5. Steps 1(i)–1(iv) of Protocol Ib. For $k = 1$, $|\psi\rangle = |+\rangle$ or else the output of previous k . E_{QRM} is the encoding circuit for QRM($1, j + 2$), $R_z(\phi)_L$ is logical (transversal) application of the field, $\{S_i^Z\}$ are all the Z stabilizer measurements, and X_L is logical X measurement from which we extract the X syndromes.

For large j this nontransversality has a small effect since $\gamma' = \gamma - O(2^{-j})$. Following the analysis of Protocol Ia, the range of the excluded angles in the worst case is again $2t\gamma$, not $2t\gamma'$.

The probability of logical error in a single interrogation is the probability that the syndrome measurements do not detect the errors and the errors corrupt X measurement. Since ϕ is unknown we cannot apply a suitable dephasing transformation (also known as twirl) on the noisy states to reduce noise to only Z errors, unlike FT quantum computing [26]. So we measure both X and Z stabilizers and the corresponding failure probabilities p_{err}^X and p_{err}^Z are given in Eqs. (19) and (23), Sec. VI. The threshold for p is now obtained by solving $p_f \equiv 1 - (1 - p_{\text{err}}^X)^{2^{j-1}}(1 - p_{\text{err}}^Z)^{2^{j-1}} = \delta(\gamma')$, which corresponds to Eq. (3) at the logical level. This threshold is presented in Fig. 4(b). For higher-order QRMCs, $p_{\text{err}}^X \ll p_{\text{err}}^Z$ below the threshold.

The number of field interrogations, our resources, required for Protocol Ib to converge depends on p_n , the probability of retransmission due to noise, and p_r , the probability of retransmission due to nontransversality. Using Lemma 2, Sec. V, $p_r = 1 - (1 - \frac{1}{2^{j+1}})^{(j+2)2^{j-1}}$. If the probabilities of passing the X and Z error syndrome measurements for bit j are given by $p_{X\text{pass}}$ and $p_{Z\text{pass}}$, respectively [Eqs. (17) and (20), Sec. VI], $p_n = 1 - (p_{X\text{pass}}p_{Z\text{pass}})^{2^{j-1}}$. This gives

$$N = \sum_{j=1}^t 2^{j-1} C(j) \frac{1}{2[\delta(\gamma') - p_f]^2} \ln\left(\frac{2t}{\epsilon}\right), \quad (6)$$

with $C(j) = (2^{j+2} - 1)/(1 - p_n)(1 - p_r)$ being the overhead from the QRMC. We plot $\Delta\phi$ versus the resources required—including extra interrogations due to retransmissions—for a fixed p and γ in Fig. 4(c).

Now we deal with noise in devices, which we assume to be independent of the field noise. This results in the new threshold equation

$$1 - (1 - p_{\text{err}}^X)^{2^{j-1}}(1 - p_{\text{err}}^Z)^{2^{j-1}}(1 - p')^{3 \times 2^{j-1} + 2} = \delta(\gamma') \quad (7)$$

involving noise of the form of Eq. (2) for the field (p) and the devices (p'). The failure probabilities p_{err}^X and p_{err}^Z now have an additional contribution from the noisy devices, which itself includes the effect of noisy nontransversal encoding and noisy syndrome measurements. The latter are E_{QRM} and $\{S_i^Z\}$ and X_L in Fig. 5. Since Eq. (7) involves two variables p and p' , there is no unique solution for the two thresholds, p_{th} and p'_{th} . For small p'_{th} , see Fig. 6 for improvements in p_{th} and Sec. VII A for details.

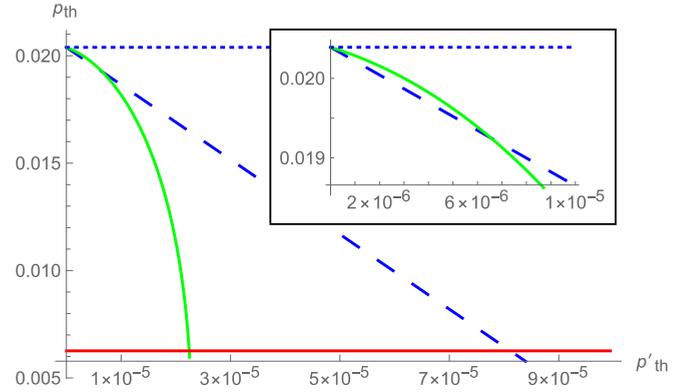


FIG. 6. Relationship between thresholds p_{th} and p'_{th} for $\gamma = \pi/32$ and $j = 4$. Improved threshold for Protocol Ib with device noise (dashed blue) over Ia (solid red/dark gray). Improved threshold of Protocol Ic (solid green/light gray) over Protocol Ib with device noise in subregion enlarged. Protocol Ib without device noise (dotted blue) is provided for reference.

C. Fault tolerance everywhere

Finally, Protocol Ic [Fig. 3(c)] combats noise at any stage of the sensing process. In quantum computation, the lack of transversal universal gate sets [28] is overcome by either gate distillation or code switching. In metrology, the former is prohibitive because ϕ is unknown (see Sec. VII B). Our Protocol Ic proceeds via switching [37] between the QRM(1,3) Steane code which is transversal for H and higher-order QRMCs [38], along with the error detection method of Protocol Ib.

Protocol Ic

For $j = 1, \dots, t$

1. Repeat M times.

- (i) Prepare $|+_{\text{L}}\rangle$ using FT procedure employing the Steane code and switch to QRM($1, j + 2$). Set $k = 1$.
- (ii) Prepare ancilla $|0_{\text{L}}\rangle$ using FT procedure employing QRM($1, j + 2$). Apply transversal FT CNOT between probe and ancilla.
- (iii) Interrogate field transversally with probe. Apply error detection on probe. Restart (i) if syndrome measurements reject.
- (iv) Teleport by measuring probe in logical X and adapting Pauli frame accordingly (see Fig. (8)).
- (v) If $k < 2^{j-1}$, increase k by one, use ancilla as new probe, and return to (ii).
- (vi) FT measurement of logical X .

2. Step 2 and 3 of Protocol Ib.

Protocol Ic behaves exactly as Protocol Ib in terms of convergence and resource requirements. The thresholds for Protocol Ic are given by modifying the failure probabilities p_{err}^X and p_{err}^Z , the number of points of failure, and the noise p' in Eq. (7). Protocol Ic has no non-transversal encoding and failure probabilities just include noisy syndrome measurements (Sec. VII C). Compared to Protocol Ib, Protocol Ic now provides a larger improvement in p_{th} over Protocol Ia, but over a reduced range of p' as shown in Fig. 6. The improvements are limited by the poor QRMC error correction

thresholds. Larger improvements should be attainable if codes with better thresholds and suitable transversality properties can be designed.

IV. ANALYSIS OF THE PARAMETRIZED RUDOLPH-GROVER SCHEME: CONVERGENCE, NOISE RESILIENCE, AND RESOURCES

The unknown phase parameter ϕ is expressed in a radix 2 expansion as $\phi = 2\pi \times 0.b_0b_1b_2 \dots = b_0\frac{2\pi}{2} + b_1\frac{2\pi}{2^2} + b_2\frac{2\pi}{2^3} \dots$. Setting $b_0 = 0$ leads to

$$\phi = b_1\frac{\pi}{2} + b_2\frac{\pi}{4} \dots \tag{8}$$

We denote our estimate of the unknown parameter after the protocol as $\hat{\phi}$.

A. Noiseless case

Assume first that Protocol Ia is implemented in the noiseless case. Let p_1 be the probability of obtaining zero (eigenvalue +1) in our measurements in a noiseless Protocol Ia for $j = 1$. Let \hat{p}_1 be our (real valued) estimate, which comes from averaging over M independent and identically distributed repetitions. Seeking $|\hat{p}_1 - p_1| \leq \delta$ leads to

$$\text{prob}(|\hat{p}_1 - p_1| \leq \delta) \geq 1 - 2e^{-2M\delta^2}$$

from the Hoeffding inequality.

Let us choose $\delta = |\cos^2(\frac{\pi}{4}) - \cos^2(\frac{\pi}{4} - \frac{\gamma}{2})| = |\sin(\gamma)/2|$. For $\gamma = \pi/8$, $\delta \approx 0.191$; for $\gamma = \pi/32$, $\delta \approx 0.049$. This implies the following, for angle ϕ in the allowed region $[0, \pi/2 - \gamma]$ or $[\pi/2 + \gamma, \pi]$.

(i) If $0 \leq \hat{\phi}_1 < (\pi/2 - \gamma)$,

$$\text{prob}\left(0 \leq \phi < \frac{\pi}{2}\right) \geq 1 - 2e^{-2M\delta^2} \tag{9}$$

and $\text{prob}(\hat{b}_1 = b_1 = 0)$ is equally high.

(ii) If $(\pi/2 + \gamma) < \hat{\phi}_1 \leq \pi$,

$$\text{prob}\left(\frac{\pi}{2} \leq \phi < \pi\right) \geq 1 - 2e^{-2M\delta^2}$$

and $\text{prob}(\hat{b}_1 = b_1 = 1)$ is equally high.

This concludes the analysis for $j = 1$.

Assuming that the estimation for $j = 1$ was correct, we proceed to the estimation of the other bits. We use induction to calculate all the conditional probabilities. Suppose all bits $b_k, k < j$ are correctly estimated. The probe after the 2^{j-1} consecutive interrogations is $(|0\rangle + e^{i\phi_j}|1\rangle)/\sqrt{2}$, where $\phi_j = 2^{j-1}\phi = 2\pi \times 0.b_{j-1}b_j b_{j+1} \dots = b_{j-1}\frac{2\pi}{2} + b_j\frac{2\pi}{2^2} + b_{j+1}\frac{2\pi}{2^3} \dots$, where b_{j-1} is known from previous estimation.

Again, using the Hoeffding inequality, we bound the probability of having error smaller than the same parameter δ . The allowed region for $\phi_j - b_{j-1}\pi$ should be again $[0, \pi/2 - \gamma]$ or $[\pi/2 + \gamma, \pi]$, and the following hold.

(i) If $b_{j-1}\pi \leq \hat{\phi}_j < \hat{b}_{j-1}\pi + (\pi/2 - \gamma)$,

$$\text{prob}\left(0 \leq \phi_j - b_{j-1}\pi < \frac{\pi}{2}\right) \geq 1 - 2e^{-2M\delta^2}$$

and $\text{prob}(\hat{b}_j = b_j = 0)$ is equally high, conditioned on the estimations of prior bits being correct.

(ii) If $\hat{b}_{j-1}\pi + (\pi/2 + \gamma) \leq \hat{\phi}_j \leq \hat{b}_{j-1}\pi + \pi$,

$$\text{prob}\left(\frac{\pi}{2} \leq \phi_j - b_{j-1}\pi < \pi\right) \geq 1 - 2e^{-2M\delta^2}$$

and $\text{prob}(\hat{b}_j = b_j = 1)$ is equally high, conditioned on the estimations of prior bits being correct.

This concludes our analysis for j .

The probability that all the bits up to b_t are estimated correctly is lower bounded by $(1 - 2e^{-2M\delta^2})^t \geq 1 - 2te^{-2M\delta^2}$. To have a maximum error ϵ in our estimator to be correct up to the t th bit, we choose M such that $\epsilon \geq 2te^{-2M\delta^2}$. This leads to

$$M \geq \frac{1}{2\delta^2} \ln\left(\frac{2t}{\epsilon}\right). \tag{10}$$

The total overhead in uses of the field to estimate ϕ to t bits with error ϵ becomes

$$N = \frac{2^t - 1}{2\delta^2} \ln\left(\frac{2t}{\epsilon}\right). \tag{11}$$

The allowed angles for which the above convergence arguments hold are as follows. From the analysis above, the estimation of the first bit converges with high probability if $\phi \in [0, \pi/2 - \gamma] \cup [\pi/2 + \gamma, \pi]$. Thus the length of the excluded region is 2γ . For the second bit, consider estimating $\phi_2 = 2\phi$. If $b_1 = 0$, $\phi \in [0, \pi/4 - \gamma/2] \cup [\pi/4 + \gamma/2, \pi/2]$, and, if $b_1 = 1$, $\phi \in [\pi/2, \pi/2 + \pi/4 - \gamma/2] \cup [\pi/2 + \pi/4 + \gamma/2, \pi]$. The length of the excluded region is again 2γ .

In general, consider estimating $\phi_j = 2^{j-1}\phi \text{ mod } 2\pi$. Suppose $b_1 = \dots = b_{j-2} = 0$. If $b_{j-1} = 0$,

$$\phi \in \left[0, \frac{\pi}{2^j} - \frac{\gamma}{2^{j-1}}\right] \cup \left[\frac{\pi}{2^j} + \frac{\gamma}{2^{j-1}}, \frac{\pi}{2^{j-1}}\right],$$

and, if $b_{j-1} = 1$,

$$\phi \in \left[\frac{\pi}{2^{j-1}}, \frac{\pi}{2^{j-1}} + \frac{\pi}{2^j} - \frac{\gamma}{2^{j-1}}\right] \cup \left[\frac{\pi}{2^{j-1}} + \frac{\pi}{2^j} + \frac{\gamma}{2^{j-1}}, \frac{\pi}{2^{j-2}}\right].$$

Continuing with the 2^{j-2} possibilities for b_1, \dots, b_{j-2} , each of which excludes regions of length $\gamma/2^{j-2}$, we obtain a total excluded region of length 2γ . In the worst case, of the regions not being overlapping, the excluded region has total angle $2t\gamma$.

B. Noisy case

We now consider the noisy case and denote the probability of an error occurring in an interrogation step as p . Then, the probability $p_f(p, j)$ of the measurement result being incorrect after a number of interrogations and a final measurement depends on p and the number of interrogations (which depends on j). In Protocol Ia, we undertake 2^{j-1} interrogations, whereby p_f is upper bounded by $1 - (1 - p)^{2^{j-1}}$.

The following analysis holds for any j . Let p_j be the probability of obtaining zero (eigenvalue +1) if there was no noise. With probability p_f , this result we get will be flipped. Let p'_j be the ‘‘noisy’’ probability of obtaining zero. Then

$$p'_j = p_j(1 - p_f) + (1 - p_j)p_f, \tag{12}$$

whereby $p'_j - p_j = p_f(1 - 2p_j)$, implying

$$|p'_j - p_j| \leq p_f. \tag{13}$$

After M repetitions, the Hoeffding inequality gives the noisy estimate \widehat{p}'_j as

$$\text{prob}(|\widehat{p}'_j - p'_j| \geq \delta) \leq 2e^{-2M\delta^2}. \quad (14)$$

Adding $|p'_j - p_j|$ gives

$$\text{prob}(|\widehat{p}'_j - p'_j| + |p'_j - p_j| \geq \delta + |p'_j - p_j|) \leq 2e^{-2M\delta^2}.$$

We then use the fact that $[\text{prob}(x \geq b) \leq c] \wedge (y \leq x) \Rightarrow \text{prob}(y \geq b) \leq c$, which can be proven by writing the probabilities as integrals and changing variables. Since $|\widehat{p}'_j - p_j| \leq |\widehat{p}'_j - p'_j| + |p'_j - p_j|$,

$$\text{prob}(|\widehat{p}'_j - p_j| \geq \delta + |p'_j - p_j|) \leq 2e^{-2M\delta^2}.$$

Thus,

$$\text{prob}(|\widehat{p}'_j - p_j| \geq \delta) \leq 2e^{-2M(\delta - |p'_j - p_j|)^2} \leq 2e^{-2M(\delta - p_f)^2},$$

whereby

$$\text{prob}(|\widehat{p}'_j - p_j| < \delta) > 1 - 2e^{-2M(\delta - p_f)^2}.$$

We therefore get confidence in our estimation for the j th bit only if $p_f < \delta$, in which case the same proof of convergence holds as in the noiseless case. This means that there is a probability p of failure in a single interrogation above which the protocol does not converge and is given by the solution of $1 - (1 - p)^{2^{t-1}} = \delta = |\cos^2(\frac{\pi}{4}) - \cos^2(\frac{\pi}{4} - \frac{\gamma}{2})|$ for a fixed γ and t . We call this the noise threshold p_{th} of the protocol.

Following the same analysis as before and replacing δ by $\delta - p_f(p, t)$ we have

$$N = \frac{2^t - 1}{2(\delta - p_f)^2} \ln \left(\frac{2t}{\epsilon} \right).$$

Standard deviation

A canonical way of quantifying the performance of an estimator is its standard deviation $\Delta\phi$. We derive this for a fixed ϵ adapting the technique from Ref. [16]. At the conclusion of the estimation protocol, with probability $1 - \epsilon$ an estimate ϕ_{est} is obtained which is the correct one up to t bits of precision ($\Delta\phi_{\text{est}} \leq \pi/2^{t+1}$). Otherwise, we get a random estimate ϕ_r , which we assume to be independent of ϕ_{est} to ease our analysis. Thus $\phi = (1 - \epsilon)\phi_{\text{est}} + \epsilon\phi_r$, and

$$\begin{aligned} \Delta\phi &= \sqrt{(1 - \epsilon)^2(\Delta\phi_{\text{est}})^2 + \epsilon^2(\Delta\phi_r)^2} \\ &= \sqrt{(1 - \epsilon)^2 \frac{\pi^2}{2^{2(t+1)}} + \epsilon^2\pi^2}. \end{aligned}$$

We choose ϵ so that $\Delta\phi$ decreases inversely with the largest possible function of the total overhead. Let $\epsilon = 1/2^t$. Since $\Delta\phi = O(2^{-t})$ for noise significantly smaller than the threshold, $N = O(t2^t)$, and we have $\Delta\phi = O(\log N/N)$, ignoring terms logarithmic in t .

V. NONTRANSVERSALITY EFFECTS IN QRMCs

We provide results for QRMCs for the effect of applying transversally gates that are nontransversal for a particular QRMC, under postselection for the correct syndrome outcomes. The equations for bit j in our protocols are obtained by setting $m = j + 2$ in the following lemmas.

Lemma 1. Apply $R_z(-\phi)$ transversally, where $\phi = 0.b_0b_1b_2\dots$, on a logical single qubit state encoded by code QRM(1, m). Postselecting on accepting the syndromes creates, up to a global phase, a logical rotation of

$$\phi' = \phi - 2 \arctan \left(\frac{\sin(\phi_m)}{(2^m - 1) + \cos(\phi_m)} \right), \quad (15)$$

around the Z axis, where $\phi_m = 2^{m-1}\phi = 2\pi \times 0.b_{m-1}b_m b_{m+1} \dots$.

Proof. Let

$$P_{+1} = \prod_{i=1}^{2^m - m - 2} (I + S_i^Z) \prod_{i=1}^m \frac{(I + S_i^X)}{2^m} \quad (16)$$

be the projector to the code space, i.e., the positive eigenspace of the Z and the X syndrome measurements S_i^Z and S_i^X , respectively. The effect of applying $R_z(-\phi)$ transversally and projecting to P_{+1} on logical state $|0_L\rangle$ leads to $P_{+1}R_z(-\phi)^{\otimes 2^m - 1}|0_L\rangle$, which is

$$\frac{1}{\sqrt{2^m}} P_{+1} \left(|0\rangle + e^{-i2^{m-1}\phi} \sum_{x \in \overline{\text{RM}} \setminus \{0\}} |x\rangle \right).$$

The projections coming from the Z stabilizer measurements have no effect on the state. The elements S_i^X correspond to the generators of the $\overline{\text{RM}}$ code (by replacing the ones with X 's and the zeros with I 's) and therefore $\prod_{i=1}^m (I + S_i^X)$ gives a sum over stabilizers that correspond to all $x \in \overline{\text{RM}}$. When applied to the above state they map each codeword to the sum of all codewords in the code and therefore create the same (global) phase:

$$1 + (2^m - 1)e^{-i\phi_m} = 1 + (2^m - 1) \cos \phi_m + i(2^m - 1) \sin \phi_m$$

where $\phi_m = 2^{m-1}\phi$. Similarly for the logical $|1_L\rangle$ state, we get $P_{+1}R_z(-\phi)^{\otimes 2^m - 1}|1_L\rangle$:

$$\frac{1}{\sqrt{2^m}} P_{+1} \left(e^{-i(2^m - 1)\phi} |1\rangle + e^{-i(2^{m-1} - 1)\phi} \sum_{x \in \overline{\text{RM}}} |x + 1\rangle \right).$$

Again, the projectors from the X measurements mix all the phases, leading to a global phase of

$$e^{-i(2^m - 1)\phi} + (2^m - 1)e^{-i(\phi_m - \phi)}.$$

Therefore the whole operation adds between the computational basis states a relative phase of

$$\begin{aligned} \phi' &= \arctan \left(\frac{(2^m - 1) \sin \phi_m}{1 + (2^m - 1) \cos \phi_m} \right) \\ &\quad - \arctan \left(\frac{\sin[(2^m - 1)\phi] + (2^m - 1) \sin(\phi_m - \phi)}{\cos[(2^m - 1)\phi] + (2^m - 1) \cos(\phi_m - \phi)} \right), \end{aligned}$$

from which Eq. (15) emerges via trigonometry. \blacksquare

The cost of postselection for rotations that are not transversal for QRM(1, m) is given below.

Lemma 2. The probability of failure in any of the S_i^X syndrome measurements on a QRM(1, m)-encoded state, on which transversal $R_z(-\phi)$ has been applied, is less than or equal to $1 - (1 - \frac{1}{2^{m-1}})^m$.

Proof. The probability of failure in the postselection of each of the m syndromes is at most $\frac{1}{2^{m-1}}$, for any real rotation. This comes from calculating the probability of getting result zero in measurement i . This is given by

$$p_i = \langle \chi_{i-1} | \frac{I + S_i^X}{2} | \chi_{i-1} \rangle = \frac{1}{2} + \frac{\langle \chi_{i-1} | S_i^X | \chi_{i-1} \rangle}{2} \\ \geq \frac{1}{2} + \frac{2^{m+1} - 8}{2 \times 2^{m+1}} = 1 - \frac{1}{2^{m-1}}$$

for $|\chi_{i-1}\rangle$ being the state that comes after syndrome measurement $i - 1$ (renormalized) and $|\chi_0\rangle = R_z(-\phi)^{\otimes 2^m-1}(|0_L\rangle + e^{i\psi}|1_L\rangle)/\sqrt{2}$, for some ψ . The key observation here is that $S_i^X|\chi_{i-1}\rangle$ is a permutation of the sums of kets of $|\chi_{i-1}\rangle$, where each sum of kets comes from applying $\prod_{j=1}^{i-1}(I + S_j^X)$ on each ket of the initial state $|\chi_0\rangle$ when written in the physical representation.

The probability of failure of all the m X syndromes— X syndromes are the only ones that potentially reject—is therefore $1 - (1 - \frac{1}{2^{m-1}})^m$. This creates an extra overhead in the resource count. ■

VI. PROTOCOL Ib WITH NOISELESS DEVICES: ERROR DETECTION FAILURE PROBABILITIES

In order to calculate the thresholds and resources of Protocol Ib we need to find the probability that the error detection procedure fails at each step k . We exploit the idea of only error detecting for the errors, followed by the decoding of the code subspace to a Hilbert space of one qubit, in order to get improved thresholds [39]. An instance of the circuit used for error detection at each step k of Protocol Ib (Fig. 5) is given for $m = 4$ in Fig. 7.

For Protocol Ib, unlike in magic state distillation in quantum computing (for more details see Ref. [40]), the circuit of Fig. 7 is applied on a physical level. In Protocol Ib errors only enter through the $R_z(\phi)$ gates and of the form of Eq. (2). Rejections after the syndrome measurements can happen either because of noise or because of the nontransversal effects analyzed in Sec. V. There is no dependency between the two sources of rejection and thus we restrict our analysis here to rejections due to noise.

Failure comes when the logical outcome of the X measurement is flipped in the case that no syndrome error is being detected. The failure probabilities at the syndrome detection for X or Z errors, p_{err}^X and p_{err}^Z , respectively, are

$$p_{\text{err}}^X = p(\text{error}|X \text{ pass}) = \frac{p(\text{error}, X \text{ pass})}{p(X \text{ pass})}$$

and, similarly,

$$p_{\text{err}}^Z = p(\text{error}|Z \text{ pass}) = \frac{p(\text{error}, Z \text{ pass})}{p(Z \text{ pass})}.$$

First we focus on the stabilizers that detect the Pauli X errors. These correspond to the rows of the parity check matrix H_z of the RM^* code. The undetected noise operators correspond to the codewords of the RM^* code, including the noiseless case which corresponds to zero, given by $V_{H_z}^\perp$.

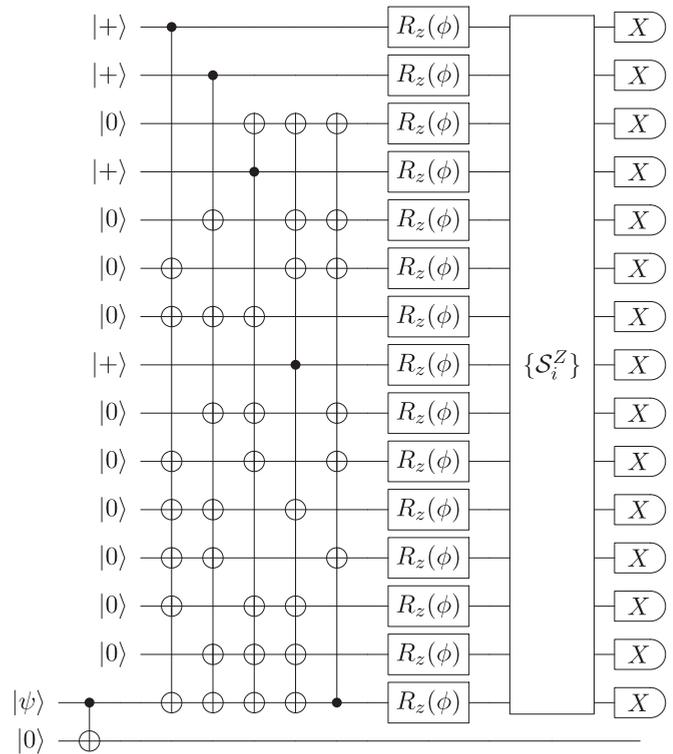


FIG. 7. FT application of transversal $R_z(\phi)$ using QRM(1,4) and teleportation onto input state $|\psi\rangle$.

Thus,

$$p(X \text{ pass}) = W_{V_{H_z}^\perp}(1 - p, p), \tag{17}$$

where $W_V(x, y) = \sum_{c \in V} x^{n-\text{wt}(c)} y^{\text{wt}(c)}$ is the weight polynomial of $V \in \text{GF}(2^n)$ and $\text{wt}(c)$ is the number of ones in the codeword c . We can then write the probability of retransmission due to Pauli X noise as $p_n^X = 1 - W_{V_{H_z}^\perp}(1 - p, p)$.

The above undetected operators could potentially corrupt the logical X measurement if they happen either before or during the application of the $R_z(\phi)$ signal. To understand this we represent the signal plus noise operation as $R_z(\theta)XR_z(\phi - \theta)$ for some angle $\theta \leq \phi$. Up to global phase this is equal to $R_z(2\theta)XR_z(\phi)$, thus equal to the original signal plus a Pauli X that has no effect on the logical X measurement, plus an extra term $R_z(2\theta)$ that can corrupt the logical X measurement when $\theta \neq 0$. From discretization of errors (Ref. [21], Theorem 10.2) and the fact that QRMCs can recover from Z noise, these non-Pauli errors $R_z(2\theta)$ are detected by the X stabilizer measurements unless they correspond to codewords of the Hamming code, and the latter corrupt the logical measurement only when they have odd parity. Since the weights of the codewords that are excluded by these refinements are large, their contribution in the error probability is negligible and therefore we can include in our calculation all codewords of the RM^* code except identity. Therefore,

$$p_{\text{err}}^X = \frac{W_{V_{H_z}^\perp}(1 - p, p) - (1 - p)^{2^m - 1}}{W_{V_{H_z}^\perp}(1 - p, p)}. \tag{18}$$

Using the codeword weights of RM^* from Appendix A, we obtain

$$p_{\text{err}}^X = \frac{(2^m - 1)(1 - p)^{2^{m-1}} p^{2^{m-1}-1} + (2^m - 1)(1 - p)^{2^{m-1}-1} p^{2^{m-1}} + p^{2^m-1}}{(1 - p)^{2^{m-1}} + (2^m - 1)(1 - p)^{2^{m-1}} p^{2^{m-1}-1} + (2^m - 1)(1 - p)^{2^{m-1}-1} p^{2^{m-1}} + p^{2^m-1}}. \quad (19)$$

The results for bit j are obtained by setting $m = j + 2$. Given the form of noise of Eq. (2) and that X error detection is made first, the single qubit X error probability is $p(p_x + p_y)$. However, since the function in Eq. (19) is monotonically increasing in p , we can replace $p(p_x + p_y)$ by p and get an upper bound $\forall p_x, p_y$.

The stabilizers that detect the Pauli Z errors correspond to the rows of the parity check matrix H_x of the dual of the $\overline{\text{RM}}$ code, which is the Hamming code $(2^m - 1, 2^m - 1 - m, 3)$. The undetected noise operators correspond to the codewords of the Hamming code, including the noiseless case which corresponds to zero, given by $V_{H_x}^\perp$. Thus,

$$p(Z \text{ pass}) = W_{V_{H_x}^\perp}(1 - p, p) \quad (20)$$

and the probability of retransmission due to Pauli Z noise is $p_n^Z = 1 - W_{V_{H_x}^\perp}(1 - p, p)$.

The subset of undetected operators that lead to an error in the logical X measurement consists of those which

$$p_{\text{err}}^Z = \frac{1 + (2^m - 1)(2p - 1)^{2^{m-1}-1} + (2^m - 1)(2p - 1)^{2^{m-1}} + (2p - 1)^{2^m-1}}{2[1 + (2^m - 1)(1 - 2p)^{2^{m-1}}]}. \quad (23)$$

Again, the above is an upper bound on the failure probability due to Z errors, when noise is of the form of Eq. (2), for all values of p_z .

VII. NOISY DEVICES

A. Protocol Ib: Noisy device thresholds

If we assume noisy devices in Protocol Ib, by allowing any device to have noise of the form of Eq. (2) with probability p replaced by the device noise probability p' , the threshold calculation is different. Failure probabilities of the detection procedure for X and Z errors are denoted by p_{err}^X and p_{err}^Z , respectively. These probabilities are given by replacing probability p by $p + \text{devIb}(p')$ in Eqs. (19) and (23), respectively. Probability $\text{devIb}(p')$ captures the effect of all device noise [except for state preparation and CNOT error, which are included separately in the last term on the left-hand side of Eq. (26)] on one qubit in the detection procedure and is given by

$$\text{devIb}(p') = [c_e + (2^m - m - 2) + 1]p' \quad (24)$$

where c_e is the number of points of failure in the nontransversal encoding procedure E_{QRM} that affect one qubit. The operations in the encoding procedure correspond to the generator matrix of $\text{RM}^*(1, m)$. On average, there are approximately $(m + 1)2^{m-1}/(2^m - 1)$ points per qubit where the entangling operations apply on the particular qubit. Since each entangling operation in the coding involves approximately 2^{m-1} qubits,

anticommute with the tensor product of X operators: the ones with odd parity. From duality, the parity matrix $H_{\overline{\text{RM}}}$ of the $\overline{\text{RM}}$ code is the generator of the codewords of the Hamming code. The subset of odd codewords is obtained by complementing the code generated by the parity check matrix H_z of RM^* , which is the same as $H_{\overline{\text{RM}}}$ without the $\mathbf{1}$ row, thus keeping only its even generators. Thus,

$$p_{\text{err}}^Z = \frac{W_{V_{H_z}}(p, 1 - p)}{W_{V_{H_x}^\perp}(1 - p, p)}, \quad (21)$$

Using the MacWilliams identity $W_V(x, y) = \frac{1}{|V|} W_{V^\perp}(x + y, x - y)$, we obtain

$$p_{\text{err}}^Z = \frac{|V_{H_x}| W_{V_{H_z}^\perp}(1, 2p - 1)}{|V_{H_z}| W_{V_{H_x}}(1, 1 - 2p)}. \quad (22)$$

Using the codeword weights of RM^* and $\overline{\text{RM}}$ from Appendix A and $|V_{H_x}|/|V_{H_z}| = 2^m/2^{m+1} = 1/2$, we obtain

we have

$$\langle c_e \rangle \approx \frac{(m + 1)2^{m-1}}{2^m - 1} 2^{m-1}. \quad (25)$$

For our protocol, we need to set $m = j + 2$ in the previous two equations.

The failure probability at the output of Protocol Ib with device noise is bounded away from 1 by the joint probability that in all of the 2^{j-1} rounds both the state preparation and CNOT are correct and the detection procedure does not fail. The latter joint probability can be written as the product of the probability of correct state preparation or CNOT and the probability of detection not failing conditioned on correct state preparation or CNOT. The points of failure for state preparation or CNOT are $3 \times 2^{j-1} + 2$. This includes initial probe preparation and Hadamard, as well as ancilla preparation and CNOT (two points of failure) at each interrogation step. Notice that performing the teleportation correction can be avoided by updating the Pauli frame. Then the threshold equation becomes

$$1 - (1 - p_{\text{err}}^X)^{2^{j-1}} (1 - p_{\text{err}}^Z)^{2^{j-1}} (1 - p')^{3 \times 2^{j-1} + 2} = \delta(\gamma'). \quad (26)$$

Since Eq. (26) involves two variables p and p' , there is no unique solution but rather a relation for the two thresholds— p_{th} and p'_{th} —as depicted in Fig. 6.

B. Protocol Ic: Why code switching?

In Protocol Ic we combat noise that can enter at any stage of the phase estimation protocol, in interrogating the field, as

well as probe and ancilla preparation, entangling gates, and measurements.

As in quantum computing, we need to employ some extra encoding throughout the protocol. If we use transversal quantum codes, the same encoding cannot be used everywhere since there is no quantum code transversal for a universal set of gates [28]. Two techniques are known to solve this issue: gate (or state) distillation and code switching. First we explain why the first technique is prohibitively expensive in terms of our resources for phase estimation.

1. Gate distillation

Everything is performed on an underlying quantum error correcting code which is transversal only for Clifford operations, e.g., QRM(1,3), also known as the Steane code. The non-Clifford operations are performed by injecting into this code special states, sometimes called magic states, and then applying a distillation procedure using a higher-order QRMC to reduce their noise [26].

In our case, the non-Clifford part of the computation is the $R_z(\phi)$ rotation. In metrology, however, ϕ is unknown. Similarly to Ref. [26], we could inject a state on which the $R_z(\phi)$ rotation has been applied and teleport it into the rest of distillation circuit using the teleportation circuit of Fig. 2. The distillation would then proceed accounting for discretization effects as described in Sec. V. However, in order for teleportation to succeed, after the logical measurement of the first qubit a logical correction on the second needs to be applied:

$$R_z(\phi)XR_z^\dagger(\phi) \propto R_z(2\phi)X, \quad (27)$$

where proportionality captures an irrelevant global phase.

In quantum computing, commonly $\phi = \pi/2^n$ and $R_z(\phi)$ belongs to the n th level of the Clifford hierarchy. Then, $R_z(2\phi)$ belongs to the $(n-1)$ th level and thus injecting, distilling, and teleporting more magic states to implement the corrections is a terminating process, with the number of steps depending on n (see Refs. [41,42] for more details). For metrology $\phi \in [0, \pi]$ and therefore a similar procedure is not guaranteed to terminate. This, on its own, is not a major issue since we could postselect on measuring zero after k consecutive teleportations with the probability of 1 being exponentially small on k (teleportation measurements are unbiased). The problem is that distilling a $R_z(2^k\phi)$ rotation, for unknown ϕ , means interrogating the field with the same state 2^k times, which will introduce noise of strength $2^k p$. Even for $k=2$, the thresholds we have calculated for the field noise (Protocol Ib) will be worse than the non-FT case (Protocol Ia). Thus, the unknown nature of the rotation, which necessitates using the same field multiple times for the teleportation corrections, means that gate distillation is not giving a benefit over the non-FT protocol.

One could avoid any correction by applying postselection on the very first teleportation step. This leads the failure probability of one $R_z(\phi)$ application in the distillation circuit to be $1/2$. Since the distillation circuit uses QRMCs of block sizes $2^{j+2} - 1$ the failure probability of transversal application on $R_z(\phi)$ on the block is $1 - (1/2)^{2^{j+2}-1}$. For 2^{j-1} interrogations this amounts to $1 - (1/2)^{2^{j-1}(2^{j+2}-1)}$, adding an extra double

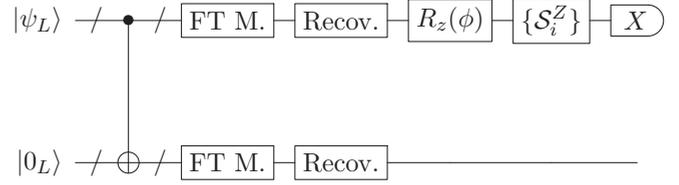


FIG. 8. Protocol Ic circuit. Operations CNOT, $R_z(\phi)$, and X measurement are all transversal. Operations $\{S_i^Z\}$ represent all Z stabilizer measurements. Fault-tolerant measurements and recovery require extra ancillae and correct up to one error.

exponential term in the resource count $C(j)$ from the code. This would be prohibitive.

2. Code switching

We thus resort to the alternative technique of code switching [37,38]. Here, the state is encoded throughout the protocol with a quantum code but is not the same at every stage. Code switching exploits the fact that different members of QRMCs are transversal for different gate sets and one can switch between those codes using ancilla qubits and FT measurements. In Protocol Ic we start with a state $|0\rangle$ encoded (by means of FT measurements) by the Steane code and fault tolerantly apply a Hadamard gate in order to prepare the $|+_L\rangle$ probe state. Then we switch to the QRM(1, m) for $m = j + 2$ on which we apply the rest of the protocol.

The circuit applied for each interrogation, Fig. 8, is similar to that of Protocol Ib (Fig. 5). The difference is that the input state $|\psi\rangle$ is already encoded with the required QRMC and therefore the nontransversal operation E_{QRM} is not needed. The state is entangled by means of a transversal CNOT gate with the ancilla qubit which is also fault-tolerantly encoded with the same QRM(1, m) code. At every step we apply FT syndrome measurements and recovery operations in the same fashion it is applied in quantum computing [21], the failure probability of which is given in Sec. VII D. The overhead that comes from the QRM encoding and switching is not counted since we count as a resource the number of uses of the field, which is the same as in Protocol Ib.

C. Protocol Ic: Noisy device thresholds

Similarly to Sec. VII A, we calculate how the noise in devices affects the error thresholds of Protocol Ic. There are two differences from Protocol Ib. First, the encoding procedure for the QRMCs is now done during the preparation of the probe and ancillae and is fault tolerant. Second, after every operation a round of fault-tolerant error correction is applied. The failure probability of the error correction procedure is denoted by p_{EC} and given in Sec. VII D. The failure probabilities of the detection procedure are denoted $p_{\text{err}}^{\prime X}$ and $p_{\text{err}}^{\prime Z}$ and given by replacing probability p by $p + \text{devIc}(p')$ in Eqs. (19) and (23), respectively, where

$$\text{devIc}(p') = [3 \times 2m + 1 + (2^m - m - 2) + 1]p'. \quad (28)$$

This includes the errors on one qubit from previous syndrome measurements and recovery plus the errors in the error

detection syndrome measurements. For our protocol, we need to set $m = j + 2$ in the above equation.

Now, the number of FT measurement and recovery steps is $3 \times 2^{j-1} + j + 1$. This includes FT probe preparation, FT Hadamard and $j - 1$ steps of switching to QRM(1, $j + 2$), as well as FT ancilla preparation and FT CNOT (two steps) at each interrogation step. We conservatively approximate the success probability of FT probe preparation, FT Hadamard, and each FT switching step by the success probability of FT measurement and the recovery step of QRM(1, $j + 2$). Then the threshold equation becomes

$$1 - (1 - p_{\text{err}}^{\prime X})^{2^{j-1}} (1 - p_{\text{err}}^{\prime Z})^{2^{j-1}} (1 - p_{\text{EC}})^{3 \times 2^{j-1} + j + 1} = \delta(\gamma'). \quad (29)$$

The solution involves two variables and is depicted in Fig. 6. We observe that the range of values of p'_{th} in which p_{th} is improved over Protocol Ia is smaller than in Protocol Ib with device noise, but, within this region, there is a subregion where Protocol Ic gives higher thresholds than Protocol Ib. This improvement, however, is small and the reason for this is the large amount of operations involved in QRMC error correction.

D. Failure probabilities of QRMCs as error-correcting codes

To analyze the thresholds of Protocol Ic we calculate the failure probability of the error correction procedure using QRMCs.

Since QRMCs can correct one error of any type, the noise threshold comes from the probability of having two or more errors during all possible operations between two rounds of fault tolerance. The approximate thresholds for QRM(1,3) are provided in Ref. [21]. We follow the same techniques to calculate approximate thresholds for QRM(1, m) for $m > 3$.

We begin by enumerating the combinations leading to two errors at the output. We consider the FT measurement and recovery operation on the first logical qubit immediately after the application of transversal CNOT in Fig. 8. The number of ways two errors can occur at the output of the first logical qubit is listed below.

(i) Two errors at the previous syndrome measurement and recovery operations. Since there are two blocks with $c_0 = 3 \times 2 \times m \times 2^{m-1} + 2^m - 1$ points of failure in each, this number is c_0^2 .

(ii) One error at the previous syndrome measurement and recovery operations at one of the two blocks, and another during the logical two qubit gate. This number is $2c_0(2^m - 1)$.

(iii) Both during the logical two qubit gate. This number is $\binom{2(2^m - 1)}{2}$.

(iv) Two errors due to incorrect syndrome measurement. This number is $(2m) \binom{2 \times 2^{m-1}}{2}$.

(v) Both at the syndrome measurements: c_0^2 .

(vi) One at the syndrome measurement and another during recovery: $c_0(2^m - 1)$.

(vii) Both during recovery: $(2^m - 1)^2$.

Summing all the above contributions, we get

$$c = 2c_0^2 + \binom{2(2^m - 1)}{2} + (2m) \binom{2^m}{2} + 3c_0(2^m - 1) + (2^m - 1)^2.$$

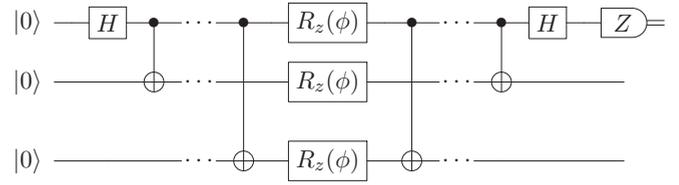


FIG. 9. Parallel phase estimation without fault tolerance.

The probability of failure of the error correction procedure, which is the probability of having at least two errors, is then

$$p_{\text{EC}} \approx cp^2, \quad (30)$$

where p' is the probability of a single component in the device being affected by noise.

VIII. PARALLEL PROTOCOLS

A parallel version of our protocols Ia, Ib, and Ic can be implemented by preparing Greenberger-Horne-Zeilinger states of 2^{j-1} entangled qubits and interrogating the field in parallel, as depicted in Fig. 9. The performance of this parallel version for Protocols Ia and Ib without device noise is identical to the serial versions. The contribution of noisy devices in Protocol Ib and Ic is different due to different preparation and measurement procedures compared to the serial protocol. Since both the serial and the parallel version require the application of a Hadamard gate, we need in both cases to complement the QRM(1, $j + 2$) with a code transversal for the H gate.

IX. DISCUSSIONS

We have illustrated a methodology for FT quantum metrology that allows estimation of phase up to higher bits of precision in the presence of arbitrary local Pauli noise. This is based on improved noise thresholds for our phase estimation scheme. While we have focused on the principle of FT quantum phase estimation, its practical use will depend on reducing resource consumption and increasing thresholds improvements. This should direct future work by calculating fault tolerance thresholds and resources for other known schemes, both nonadaptive [39,43] as well as adaptive [21,43–45].

Noise thresholds have been identified [17] for nonadaptive phase estimation schemes [43] under general additive noise and establish a noise threshold for a modified version of it. While these works do not use QECC or fault tolerance, they do possess thresholds better than ours. This is due to the sophistication of the estimation scheme, and its fault tolerance would therefore be an interesting open question.

Further improvements in FT quantum metrology should be possible with better estimation schemes as well as the quantum error correcting codes, the latter determined by the transversality demands set by the unknown parameter(s) to be estimated. These should spur developments not only in quantum metrology but also in quantum error correction and fault tolerance.

ACKNOWLEDGMENTS

We thank T. Rudolph for communications about Ref. [20], B. Terhal for pointing us to Ref. [17], D. Branford for technical discussions, J. Friel for commenting on the paper, and S. Ferracin for graphics assistance. This work was partly supported by the UK Engineering and Physical Sciences Research Council (Grant No. EP/K04057X/2) and the UK National Quantum Technologies program (Grants No. EP/M013243/1 and No. EP/M01326X/1).

APPENDIX A: QUANTUM ERROR CORRECTION

It is known [23] that transversal gates on stabilizer codes are necessarily at a finite level of the Clifford hierarchy [46]. This is based on the notion of disjointness, which is a metric of stabilizer quantum error-correcting codes and is, roughly speaking, the number of mostly nonoverlapping representatives of any given nontrivial logical Pauli operator.

Theorem 1 (Theorem 5 in Ref. [23]). Consider a stabilizer code with minimum distance d_{\downarrow} , maximum distance d_{\uparrow} , and disjointness Δ . If M is an integer satisfying

$$d_{\uparrow} < d_{\downarrow} \Delta^{M-1},$$

then all transversal logical operators are in the M th level of the Clifford hierarchy \mathcal{C}_M .

This theorem implies that in our construction for FT metrology we cannot hope to use a stabilizer code that is transversal for any gate $R_z(\phi)$ for $\phi \in \mathbb{R}$.

1. Reed-Muller codes

Reed-Muller codes $\text{RM}(r, m)$ of block length $n = 2^m$, for $0 \leq r \leq m$, dimension $\sum_{i=0}^r \binom{m}{i}$, and distance 2^{m-r} are a family of classical block codes [31]. Reed-Muller codes have geometric properties that allow for easy decoding. Codewords of $\text{RM}(r, m)$ correspond to all Boolean functions f of m variables of degree r . Each codeword is the last column of the truth table of f , i.e., the values of f for all different inputs. For example, the rows of the generator matrix of $\text{RM}(1,3)$ contain the values of $a_0 \mathbf{1} + a_1 x_1 + a_2 x_2 + a_3 x_3$, where $\mathbf{1}$ stands for the vector of all ones, for all x_i 's and each row corresponds to a different element of a basis on a_i 's:

$$G = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

We are interested in the divisibility properties of Reed-Muller codes, which have implications for the transversality of the quantum Reed-Muller codes. A classical code C is called divisible by Δ if Δ divides the weight of all $x \in C$. A code is called divisible if it is divisible by $\Delta > 1$. First-order RM codes are divisible by 2^{m-1} because exactly half of the outputs of a boolean function of degree 1 have value 1, except function $\mathbf{1}$, which always has output 1.

QRMCs use codes constructed from RM codes. We present their divisibility properties and weight distribution. The shortened RM code, denoted by $\overline{\text{RM}}$, is taken by keeping only the codewords which begin with zero and deleting their first

coordinate. Codewords of $\overline{\text{RM}}(1, m)$ can be defined by the following recursive process. For $m = 2$,

$$\mathcal{S}_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix},$$

and for higher values of m

$$\mathcal{S}_m = \begin{bmatrix} \mathcal{S}_{m-1} & \mathbf{0} & \mathcal{S}_{m-1} \\ \mathcal{S}_{m-1} & \mathbf{1} & \overline{\mathcal{S}}_{m-1} \end{bmatrix}.$$

Code $\overline{\text{RM}}(1, m)$ therefore has one codeword of weight zero and $2^m - 1$ of weight 2^{m-1} .

The punctured Reed-Muller code RM^* is obtained by adding the $\mathbf{1}$ row to the generator of $\overline{\text{RM}}$. RM^* therefore has one codeword of weight zero, $2^m - 1$ of weight $2^{m-1} - 1$, $2^m - 1$ of weight 2^{m-1} , and one of weight $2^m - 1$.

2. Quantum Reed-Muller codes

A quantum Reed-Muller code $\text{QRM}(1, m)$ is a CSS code based on classical Reed-Muller codes. It is constructed using the punctured Reed-Muller code RM^* and its even subcode $\overline{\text{RM}}$ with logical states $|x\rangle_L \equiv \sum_{y \in \overline{\text{RM}}} |y + x\mathbf{1}\rangle$, for $x \in \{0, 1\}$. The size of the block is $2^m - 1$ qubits. The minimum distance is 3, which is the minimum distance of the dual of the RM that is used to correct the Z errors [47].

Using the following lemma, we justify our choice of $\text{QRM}(r, m)$ code with $r = 1$ and m chosen according to transversality requirements.

Lemma 3 (Corollary 4 in Ref. [48]). Let $\text{QRM}(r, m)$ be created by the construction described above, where $0 < r \leq \lfloor m/2 \rfloor$. Then it is an $[n = 2^m - 1, 1, d = \min(2^{m-r} - 1, 2^{r+1} - 1)]$ code, with transversal T_t for $t = \lfloor m/r \rfloor - 1$.

We can thus calculate the failure probability for $\text{QRM}(r, m)$ with $r = 1$ and for $r > 1$ with a fixed m/r ratio, to have the same transversality property, with an error model where each physical qubit is corrupted with probability $0 \leq p \ll 1$. We calculated the thresholds for $r = 2$, using the following theorem.

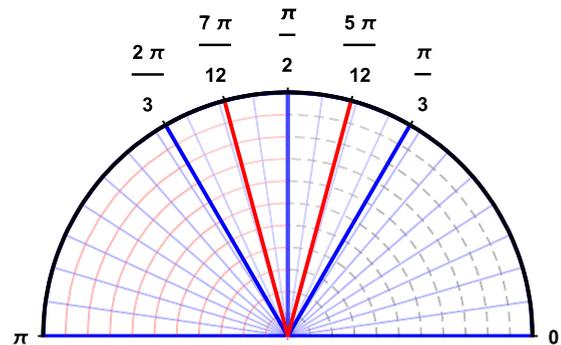


FIG. 10. Estimator of Protocol II. There are three regions: $[0, \pi/2]$, $[\pi/3, 2\pi/3]$, and $[\pi/2, \pi]$. The decision boundaries for $j = 1$ are the red lines. There are no excluded regions.

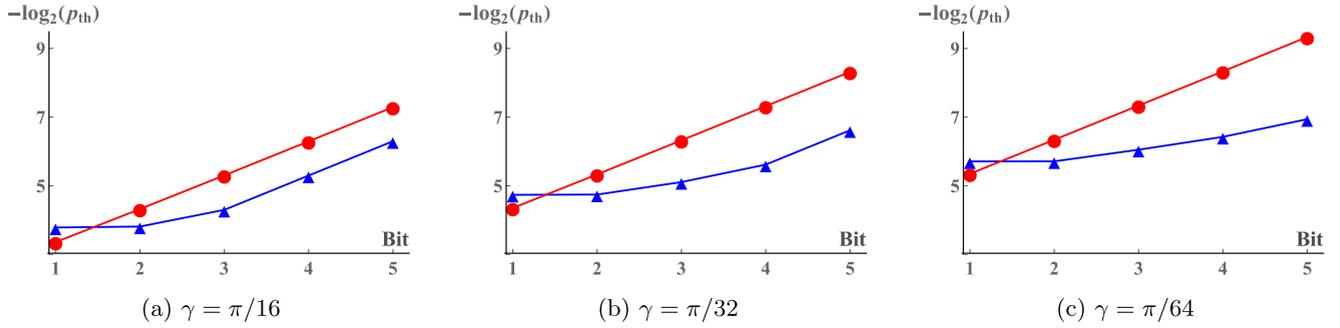


FIG. 11. Interrogation noise thresholds. Red circles, Protocol Ia; blue triangles, Protocol Ib without device noise. For the effect of device noise see Fig. 6.

Theorem 2 (Theorem 8, Chap. 15, in Ref. [31]). Let A_i be the number of codewords of weight i in $\text{RM}(2, m)$. Then $A_i = 0$ unless $i = 2^{m-1}$ or $i = 2^{m-1} \pm 2^{m-1-h}$ for some h , $0 \leq h \leq \lceil \frac{m}{2} \rceil$. Also, $A_0 = A_{2^m} = 1$ and $A_{2^{m-1} \pm 2^{m-1-h}} = 2^{h(h+1)} \frac{(2^m-1)(2^{m-1}-1)\dots(2^{m-2h+1}-1)}{(2^{2h}-1)(2^{2h-2}-1)\dots(2^2-1)}$. Finally, $A_{2^{m-1}} = 2^{1+m} \binom{m}{2} - \sum_{i \neq 2^{m-1}} A_i$.

We use the technique of Sec. VI to calculate the thresholds. We find the thresholds for $r = 2$ with the same transversal properties worse than the case $r = 1$. Given that the threshold calculations for ≥ 3 are too prolix and the block sizes too large, we choose $r = 1$.

Transversality of $\text{QRM}(1, m)$ is based on the fact that all the codewords of $\overline{\text{RM}}$ are divisible by $\Delta = 2^{m-1}$, while their complement is divisible by $\Delta = 2^{m-1} - 1$ or $2^m - 1$. Transversality enables different operations on each logical computational basis-state modulo 2^{m-1} , by applying transversal gates on the $2^m - 1$ physical qubits. In particular, applying transversal T_n on $\text{QRM}(1, n+1)$ will apply the logical T_n^\dagger gate. For example, $\text{QRM}(1, 4)$ is transversal for $T_3 = T$, also known as the phase- $\pi/8$ gate, but not for smaller fractions of rotations around the Z axis.

APPENDIX B: MIXED RADIX EXTENSION OF THE RG ESTIMATOR

The RG estimator [20] only converges if the phase ϕ lies in certain regions as detailed in Sec. IV. This limitation can be overcome by slightly modifying the estimator [49]. It begins

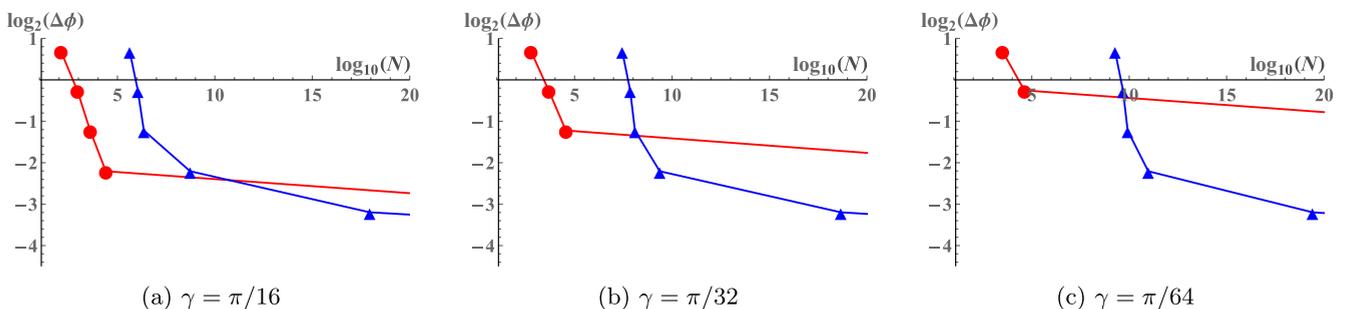


FIG. 12. Precision as a function of the number of interrogations, our resource. Red circles, Protocol Ia; blue triangles, Protocol Ib without device noise; markers denote bits. Improvement from fault tolerance is illustrated in estimating higher bits. Noise chosen at the noise thresholds of Protocol Ia which are closer to 0.63%: (a) $p = 0.639\%$, (b) $p = 0.626\%$, and (c) $p = 0.619\%$.

by expressing the parameter in a mixed base as

$$\phi = v_1 \frac{\pi}{r_1} + v_2 \frac{\pi}{r_1 r_2} + v_3 \frac{\pi}{r_1 r_2 r_3} \dots, \quad (\text{B1})$$

where $r_i \in \{2, 3\}$. In order to estimate dit j the qubit $|+\rangle$ state interrogates the field an appropriate number of times followed by a Pauli X measurement. The protocol is identical to that depicted in Fig. 3, only with a different number of consecutive interrogations. Unlike Protocol Ia, Protocol II below converges for all values of ϕ , since there is no excluded region (Fig. 10).

Protocol II: Extended RG estimator [52]

For $j = 1, \dots, t$

1. Repeat M times.

(i) Prepare $|+\rangle$.

(ii) Interrogate field $\prod_{l=0}^{j-1} r_l$ times ($r_0 = 1$).

(iii) Measure X .

2. Calculate \hat{p}_j as the fraction of the $+1$ measurement outcomes out of M . If $\hat{v}_{j-1} = 0$ set $\hat{\phi}_j = \cos^{-1}(2\hat{p}_j - 1)$ in $[0, \pi]$, or else in $[\pi, 2\pi]$.

(i) If $\hat{v}_{j-1}\pi \leq \hat{\phi}_j < \hat{v}_{j-1}\pi + \frac{5\pi}{12}$, set $\hat{v}_j = 0$ and $r_j = 2$.

(ii) If $\hat{v}_{j-1}\pi + \frac{5\pi}{12} \leq \hat{\phi}_j < \hat{v}_{j-1}\pi + \frac{7\pi}{12}$, set $\hat{v}_j = 1$ and $r_j = 3$.

(iii) If $\hat{v}_{j-1}\pi + \frac{7\pi}{12} \leq \hat{\phi}_j \leq \hat{v}_{j-1}\pi + \pi$, set $\hat{v}_j = 1$ and $r_j = 2$.

3. If $j \neq t$ add one to j and go to step 1, otherwise exit and output

$$\hat{\phi} = \hat{v}_1 \frac{\pi}{r_1} + \hat{v}_2 \frac{\pi}{r_1 r_2} \dots$$

The convergence of the noiseless protocol is proven in [49]. Here we discuss its noise resilience following the analysis for the noisy Protocol Ia in Sec. IV.

Following Protocol Ia, γ is the maximum error allowed in the estimated angle for the protocol to converge. In Protocol II, γ is fixed to $\pi/12$ since an estimation within this error means that (i) $0 \leq \phi_j - v_{j-1}\pi < \pi/2 \Rightarrow (\widehat{v}_j = v_j = 0 | r_j = 2)$; (ii) $\pi/3 \leq \phi_j - v_{j-1}\pi < 2\pi/3 \Rightarrow (\widehat{v}_j = v_j = 1 | r_j = 3)$; and (iii) $\pi/2 \leq \phi_j - v_{j-1}\pi < \pi \Rightarrow (\widehat{v}_j = v_j = 1 | r_j = 2)$.

The associated maximum error in the estimated probability is $\delta = |\cos^2(\frac{5\pi}{24}) - \cos^2(\frac{6\pi}{24})| \approx 0.129$. The noise thresholds are given by the solutions to

$$1 - (1 - p_{\text{th}})^{3^{t-1}} = \delta \quad (\text{B2})$$

since $1 - (1 - p)^{\prod_{l=1}^{t-1} r_l} \leq 1 - (1 - p)^{3^{t-1}}$. The number of field interrogations, our resource, to estimate t dits with error ϵ is

$$N = \sum_{j=1}^t \prod_{l=1}^{j-1} r_l \frac{1}{2(\delta - p_f)^2} \ln\left(\frac{2t}{\epsilon}\right). \quad (\text{B3})$$

A FT protocol for this estimator on the lines of Protocol Ib using QRMCs suffers from nontransversality for phases such as $\phi = \pi/3$. A logical shift in such a phase pushes logical angles ϕ'_j outside $[0, \pi]$ because 3 times the logical rotation corresponding to transversal $\pi/3$ does not equal π . This induces an error in the estimation.

A convergent FT protocol is therefore impossible if we restrict ourselves to codes transversal for rotations $\pi/2^k$ unless we can interrogate the field for a fractional amount of time depending on j and the corresponding logical phase shift given by Lemma 1.

APPENDIX C: GRAPHS FOR DIFFERENT VALUES OF γ

Figure 11 shows the interrogation noise thresholds as a function of the number of bits estimated and Figure 12 shows the precision as a function of the number of interrogations.

-
- [1] R. Demkowicz-Dobrzański, J. Kołodyński, and M. Guta, *Nat. Commun.* **3**, 1063 (2012).
- [2] A. Smirne, J. Kołodyński, S. F. Huelga, and R. Demkowicz-Dobrzański, *Phys. Rev. Lett.* **116**, 120801 (2016).
- [3] J. Preskill, [arXiv:quant-ph/0010098](https://arxiv.org/abs/quant-ph/0010098).
- [4] C. Macchiavello, S. F. Huelga, J. I. Cirac, A. K. Ekert, and M. B. Plenio, in *Quantum Communication, Computing, and Measurement 2* (Springer, Boston, MA), pp. 337–345.
- [5] R. Ozeri, [arXiv:1310.3432](https://arxiv.org/abs/1310.3432).
- [6] W. Dür, M. Skotiniotis, F. Fröwis, and B. Kraus, *Phys. Rev. Lett.* **112**, 080801 (2014).
- [7] E. M. Kessler, I. Lovchinsky, A. O. Sushkov, and M. D. Lukin, *Phys. Rev. Lett.* **112**, 150802 (2014).
- [8] G. Arrad, Y. Vinkler, D. Aharonov, and A. Retzker, *Phys. Rev. Lett.* **112**, 150801 (2014).
- [9] D. A. Herrera-Martí, T. Gefen, D. Aharonov, N. Katz, and A. Retzker, *Phys. Rev. Lett.* **115**, 200501 (2015).
- [10] X.-M. Lu, S. Yu, and C. H. Oh, *Nat. Commun.* **6**, 7282 (2015).
- [11] T. Uden, P. Balasubramanian, D. Louzon, Y. Vinkler, M. B. Plenio, M. Markham, D. Twitchen, A. Stacey, I. Lovchinsky, A. O. Sushkov, M. D. Lukin, A. Retzker, B. Naydenov, L. P. McGuinness, and F. Jelezko, *Phys. Rev. Lett.* **116**, 230502 (2016).
- [12] R. Demkowicz-Dobrzański, J. Czajkowski, and P. Sekatski, *Phys. Rev. X* **7**, 041009 (2017).
- [13] S. Zhou, M. Zhang, J. Preskill, and L. Jiang, *Nat. Commun.* **9**, 78 (2018).
- [14] F. Reiter, A. S. Sørensen, P. Zoller, and C. A. Muschik, *Nat. Commun.* **8**, 1822 (2017).
- [15] D. Layden and P. Cappellaro, *npj Quantum Information* **4**, 30 (2018).
- [16] M. de Burgh and S. D. Bartlett, *Phys. Rev. A* **72**, 042301 (2005).
- [17] S. Kimmel, G. H. Low, and T. J. Yoder, *Phys. Rev. A* **92**, 062315 (2015).
- [18] D. Layden, S. Zhou, P. Cappellaro, and L. Jiang, *Phys. Rev. Lett.* **122**, 040502 (2019).
- [19] R. Demkowicz-Dobrzański and L. Maccone, *Phys. Rev. Lett.* **113**, 250801 (2014).
- [20] T. Rudolph and L. Grover, *Phys. Rev. Lett.* **91**, 217905 (2003).
- [21] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University, Cambridge, England, 2010).
- [22] R. Raussendorf, *Phil. Trans. R. Soc. A* **370**, 4541 (2012).
- [23] T. Jochym-O'Connor, A. Kubica, and T. J. Yoder, *Phys. Rev. X* **8**, 021047 (2018).
- [24] M. Hassani, C. Macchiavello, and L. Maccone, *Phys. Rev. Lett.* **119**, 200502 (2017).
- [25] C. M. Dawson and M. A. Nielsen, *Quantum Inf. Comput.* **6**, 81 (2006).
- [26] S. Bravyi and A. Kitaev, *Phys. Rev. A* **71**, 022316 (2005).
- [27] E. T. Campbell and D. E. Browne, *Phys. Rev. Lett.* **104**, 030503 (2010).
- [28] B. Eastin and E. Knill, *Phys. Rev. Lett.* **102**, 110502 (2009).
- [29] Noise strength is typically defined as the diamond norm of the noise operators.
- [30] R. Raussendorf, J. Harrington, and K. Goyal, *New J. Phys.* **9**, 199 (2007).
- [31] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (Elsevier, Amsterdam, 1977).
- [32] This choice of r is made on explicit calculations (see Appendix A).
- [33] A different protocol using a mixed radix representation of the phase can avoid the excluded regions [49], but its use in our FT methodology (see Appendix B) is left open for want of a code family that is simultaneously transversal for $\text{diag}(1, e^{i2\pi/2^n})$ and $\text{diag}(1, e^{i2\pi/3^n})$.
- [34] Y. Matsuzaki, S. C. Benjamin, and J. Fitzsimons, *Phys. Rev. A* **84**, 012103 (2011).
- [35] R. Chaves, J. B. Brask, M. Markiewicz, J. Kołodyński, and A. Acín, *Phys. Rev. Lett.* **111**, 120401 (2013).
- [36] P. Sekatski, M. Skotiniotis, J. Kołodyński, and W. Dür, *Quantum* **1**, 27 (2017).
- [37] H. Bombin, *New J. Phys.* **17**, 083002 (2015).
- [38] J. T. Anderson, G. Duclos-Cianci, and D. Poulin, *Phys. Rev. Lett.* **113**, 080501 (2014).
- [39] A. Y. Kitaev, [arXiv:quant-ph/9511026](https://arxiv.org/abs/quant-ph/9511026).
- [40] K. Fujii, *Quantum Computation with Topological Codes: From Qubit to Topological Fault-Tolerance* (Springer, New York, 2015), Vol. 8.

- [41] A. J. Landahl and C. Cesare, [arXiv:1302.3240](#).
- [42] E. T. Campbell and J. O’Gorman, [Quantum Science and Technology](#) **1**, 015007 (2016).
- [43] B. Higgins, D. Berry, S. Bartlett, M. Mitchell, H. Wiseman, and G. Pryde, [New J. Phys.](#) **11**, 073023 (2009).
- [44] R. B. Griffiths and C.-S. Niu, [Phys. Rev. Lett.](#) **76**, 3228 (1996).
- [45] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, [Proc. R. Soc. A](#) **454**, 339 (1998).
- [46] Let \mathcal{P} be the group of Pauli operators. The first level of the Clifford hierarchy \mathcal{C}_1 is the normalizer of the Pauli group under conjugation. Then, the n th level of the Clifford hierarchy \mathcal{C}_n is the set of operators that map the Pauli group to the $(n - 1)$ th level of the hierarchy under conjugation. A rotation operator $\text{diag}(1, e^{i2\pi/2^n})$ belongs to the $(n - 1)$ th level of the Clifford hierarchy. Thus, a transversal rotation by a real angle can potentially corrupt the logical space of a stabilizer code. For more details, see Appendix A and Ref. [23].
- [47] The $\overline{\text{RM}}^*$ code used to detect the X errors and the dual of the $\overline{\text{RM}}$ code used to detect the Z errors have different distances, a fact exploited by our scheme.
- [48] B. Zeng, A. Cross, and I. L. Chuang, [IEEE Trans. Inf. Theory](#) **57**, 6272 (2011).
- [49] Z. Ji, G. Wang, R. Duan, Y. Feng, and M. Ying, [IEEE Trans. Inf. Theory](#) **54**, 5172 (2008).