Supplementary Information

The need for ancilla verification—In the theory of quantum fault tolerance there are two well-known methods for performing fault-tolerant error correction. The first, due to Shor [1] and DiVincenzo and Shor [2], makes use of ancillae encoded in the classical repetition code informally called "cat" states. The second, which is due to Steane [3] and applies to the Calderbank-Shor-Steane (CSS) class of quantum codes, uses as ancillae logical $|0\rangle$ and $|+\rangle$ states encoded in the same code as the data. In both methods, the preparation of these ancillae by directly executing their encoding circuit is not in general a fault-tolerant procedure, and extra steps are needed before the ancillae are considered pure enough to be coupled to the data. This purification procedure, also known as *verification*, is performed by running parity checks on the ancilla using additional ancillary verifier states.

Ancilla verification is typically done non-deterministically by simply rejecting ancillae that fail the parity checks of verification and starting anew. This procedure however is disadvantageous when measurement is slow since the verified ancilla qubits will have to be stored for long times in memory before measurements that are part of verification finish. Alternatively, verification can be done deterministically by correcting errors in the verified ancilla and thus avoiding post-selection. (Note that the deterministic protocol in Fig. 4 in [4] that does not correct errors in the ancillae is unusable when measurement is slow: In this protocol, an element of non-determinism exists in *which* ancillae are to be coupled to the data depending on the verification measurement outcomes.) The price for a deterministic verification procedure is a penalty in efficiency: A larger number of verifier qubits and verification operations are needed compared to the non-deterministic procedures (e.g., compare the deterministic protocol in Fig. 9 in [5] with the non-deterministic one in Fig. 11 in [6]). And this increase in qubit and operation overhead translates into a decrease in the accuracy threshold as compared to non-deterministic verification—this is the reason why non-deterministic verification has been used hitherto in almost all threshold studies.

We will here describe how ancilla verification can be avoided altogether and replaced by suitable decoding of the encoded ancillae *after* these interact with the data during error correction. We find that not only does this method improve the efficiency of present schemes that use verification, but it also leads—in the examples of interest we have studied in detail—to an improvement in the accuracy threshold as compared even to non-deterministic verification procedures.

We will first discuss the case of distance-3 quantum codes correcting arbitrary errors on any one qubit in the code block. In the end we will discuss the generalization to codes of higher distance. Throughout, we use the shorthand notation $X \equiv \sigma_{\rm x}$ and $Z \equiv \sigma_{\rm z}$ and we also use superscripts to denote the qubit on which an operator acts (e.g., $Z^{(i)}$ denotes a Pauli $\sigma_{\rm z}$ operator acting on the i-th qubit).

Ancilla decoding instead of verification—The intuition leading to this method is guided by a few basic observations on how fault-tolerant error correction is implemented.

The first observation is that ancilla verification checks particular error patterns and does not need to protect against arbitrary multi-qubit errors. In particular, we are concerned with faults that appear in first order in the encoding circuit and propagate to cause multi-qubit errors at the output of the ancilla encoder that our distance-3 code cannot correct. Verification works by exactly trying to detect (or correct, in deterministic schemes) these particular errors appearing in first order, with the additional condition that the verification step should not, also in first order, introduce multi-qubit errors in the ancilla that is being verified.

The second observation is that the ancilla after interacting with the data block remains, ideally, in a *known* logical state. For example, after the cat state $|\bar{+}\rangle_{\rm rep} \equiv (|00\ldots0\rangle + |11\ldots1\rangle)/\sqrt{2}$ interacts with the data, it remains encoded in either $|\bar{+}\rangle_{\rm rep}$ or $|\bar{-}\rangle_{\rm rep}$ (the latter differs by the sign having flipped from $+$ to $-$ in the above superposition). Similarly in Steane's error correction method, an ancilla prepared in the logical $|0\rangle$ state remains in the same state after interacting with the data. This is more information than just knowing that the ancilla state is protected by a code—we have additional information about what the state should be.

The idea of the new method is to couple the encoded ancilla to the data without attempting any verification, followed by a procedure that is run afterwards on it and allows us to learn and *invert* possible multi-qubit errors produced by the encoder and having propagated to the data. This procedure could be implemented in various ways, but it seems that the most efficient (and eye-pleasing) one is via a suitable decoder. A schematic of this method is given in Fig. 1.

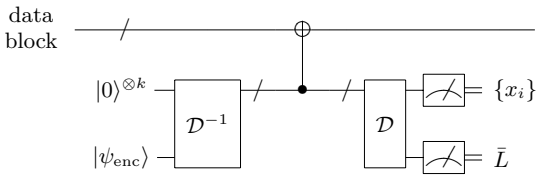

FIG. 1: Schematic of fault-tolerant error correction without ancilla verification for distance-3 codes. The ancilla is encoded by starting with ancillary qubits in a reference state (e.g., $|0\rangle^{\otimes k}$), the state to be encoded ($|\psi_{\rm enc}\rangle$), and running the unitary encoding circuit ($\mathcal{D}^{-1}$). After interacting with the data block (schematically shown as a CNOT), the ancilla is decoded using a unitary decoding circuit ($\mathcal{D}$). The final measurements yield syndrome information ($\{x_i\}$) and the eigenvalue of a logical operator ($\bar{L}$).

To prove that this error-correction (EC) method is fault tolerant, we need to show that properties $0', 0-2$ in [6] are satisfied. Properties 0 (EC without faults takes an arbitrary input to the code space) and 1 (EC without faults corrects single-qubit errors in the data block) are true since, without faults, verification is superfluous and the measurement outcomes after decoding will give the necessary syndrome information to perform ideal error correction. Properties $0'$ (EC with one fault always produces an output deviating by at most a weight-one operator from the code space) and 2 (EC with one fault produces a block with at most one error if the input has no errors) require proof. As with the known error-correction methods that use ancilla verification, showing that property $0'$ holds is made easier after understanding why property 2 is satisfied. And as we will see, satisfying property 2 will determine how our decoding circuit must be designed.

What we need to show is that a single fault in the EC circuitry cannot cause more than one error in the corrected data block (which for property 2 initially has no errors). Consider first the case where the fault occurs during the interaction with the data. Since this interaction is done with transversal gates, no gate operates on more than one qubit in the same block. Therefore a single fault cannot cause more than one error in the data. An error can also appear in the ancilla block, but this does not prevent successful correction: If cat states are used the syndrome extraction is repeated, or in Steane's method the errors in data and ancilla blocks occur always in the same qubit in the code block and a single syndrome extraction can be trusted.

The second case is when the fault occurs inside the ancilla encoder. In general the encoding circuit has no special structure and more than one errors can appear in the produced encoded ancilla. The encoder can however be designed so that no logical error appears at the output due to a single fault inside it and, furthermore, the possible error patterns caused by all such first order fault events are known. Of interest are multi-qubit errors which may propagate to the data via the ancilla-data interaction. However, letting ancilla and data interact without verification as in Fig. 1 is permissible since the information at the output of the following decoder will allow us to diagnose whether such error propagation did occur and invert it. To understand how this is possible, it is useful to think of the decoding circuit as performing error correction while simultaneously decoding its input block to a qubit. Since in the case considered the decoder is fault-free, both processes are executed ideally. The decoder then performs the mapping

$$E_i|\bar{0}\rangle \rightarrow |i\rangle \otimes |0\rangle\,; \;\; E_i|\bar{1}\rangle \rightarrow |i\rangle \otimes |1\rangle\,, \qquad (1)$$

where $\{E_i\}$ is the set of all single-qubit Pauli errors that our distance-3 code corrects, $|\bar{0}\rangle$ ($|\bar{1}\rangle$) is the ideal logical $|0\rangle$ ($|1\rangle$) state, and i is syndrome information that, after decoding, indicates the error E_i (if the code is not *perfect* and the basis $\{E_i|\bar{0}\rangle, E_i|\bar{1}\rangle\}$ does not span the whole Hilbert space, the action of the unitary decoder can be extended to include some non-correctable errors).

Now, if we decode a n-qubit cat state, then measuring the qubits carrying the syndrome will allow us to learn all eigenvalues of the $Z^{(i)}Z^{(j)}$ code stabilizers for $1 \leq i = j-1 \leq n-1$. Hence we can diagnose whether multi-qubit X errors were produced in the encoder and can invert them by updating the Pauli frame of the data block. In Steane's method, the syndrome information will diagnose any X (resp. Z) errors in the logical $|0\rangle$ (resp. $|+\rangle$) ancilla that propagate to the data. In addition, measuring the decoded qubit (the second tensor-product factor in Eq. (1); denoted by $\bar{L}$ in Fig. 1) will reveal the eigenvalue of the *logical* Z (resp. X) operator. This resolves the ambiguity about the error causing a particular syndrome since, for E_i and E_j to have the same syndrome, $E_i^\dagger E_j = \bar{O}$ where $\bar{O}$ is either trivial (equal to the identity or $\bar{L}$) or anti-commutes with $\bar{L}$. Thus, either E_i and E_j are equivalent up to an element of the ancilla stabilizer, or lead to orthogonal decoded states which allows distinguishing them. Again, whenever multi-qubit errors are detected, the appropriate Pauli-frame change is done on the data block to invert them.

The final case to consider is when a single fault occurs in the decoding circuit. In the case discussed above we were concerned with correcting multi-qubit errors caused by a single fault in the encoder and subsequently propagating to the data. But we also need to guarantee that such a corrective step is not mistakenly taken due to a single fault inside the decoder (which can cause no errors to the data block). Thus, to satisfy property 2, we must ensure that no single fault inside the decoding circuit can give the same syndrome (including the eigenvalue of the logical operator $\bar{L}$) as any of the multi-qubit errors which a single fault inside the encoder can produce. Constructing the decoding circuit to meet this condition must be done with care given the chosen ancilla encoder.

In the examples section that follows such decoder designs are shown for some very frequently used cases: fault-tolerant measurements using four- and seven-qubit cat states and Steane's error-correction method for the [[7,1,3]] code. We conjecture that an appropriate decoding circuit can be found for any distance-3 code. In any case, a less efficient but general solution is always possible: We can further encode the ancilla after interacting with the data in the two-bit classical repetition code and then decode the two sub-blocks separately as shown in Fig. 2. In this circuit, when the syndrome for X errors at the two sub-blocks agree, then we can be confident that, to first order, any detected multi-qubit X error has occurred during ancilla encoding and has propagated to the data. Otherwise, if the syndromes for X errors disagree, we conclude that, again to first order, a fault has happened in one of the two decoded sub-blocks and no

multi-qubit X error has propagated to the data. The syndrome for Z errors (revealing Z errors initially in the input data block) can be obtained by taking the *parity* of the syndromes at the two sub-blocks.

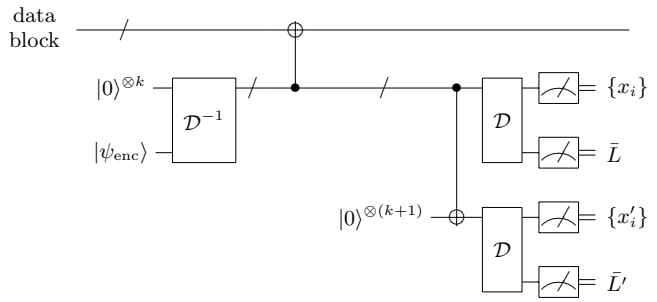

FIG. 2: To ensure that a single fault during ancilla decoding cannot be mistaken for a fault inside the ancilla encoder leading to the same syndrome, the ancilla is encoded in the two-bit classical repetition code and then the two sub-blocks are decoded separately. If the syndrome in *both* sub-blocks indicates a multi-qubit X error then we are confident a fault in the ancilla encoder occurred and propagated to the data. Otherwise the fault must have occurred during the decoding procedure.

For such designs that satisfy property 2, let us now discuss property $0'$. We observe that errors that may propagate from the encoder to the data block (e.g., X errors when ancilla and data interact via a CNOT as in Fig. 1) are decoupled from errors that propagate the other way around (Z errors). Hence detecting and inverting errors caused in the encoder does not interfere with the way errors initially in the data are treated by EC. Therefore, the success of our method for dealing with single faults inside the EC circuitry is independent of whether the data block starts in the code space or not. This implies that EC methods which satisfy property $0'$ when ancilla verification is used (e.g., Steane's method as discussed in [6]), will still satisfy it if decoding of the ancilla is performed instead as described above.

For non-perfect codes we need to worry also about replacing verification against multi-qubit errors that do *not* propagate from the ancilla to the data (e.g., Z errors in Fig. 1). (Recall that a code is called *perfect* if all possible syndromes point to correctable errors, as is e.g. the case for the Steane [[7,1,3]] and Golay [[23,1,7]] codes.) Verification against such errors can be easily avoided by repeating the syndrome extraction: The circuit in Fig. 1 or 2 can be repeated three times and the syndrome for Z errors in the data must only be trusted if at least two of the syndromes for Z errors agree. (The same applies for the X error correction.)

Finally, one technical point must be addressed. With a single syndrome extraction as in Fig. 1, property 2 is satisfied separately for X and Z errors. That is, a single fault inside the ancilla encoder may lead to a single X and a single Z error in the output data block with the two errors acting on *different* qubits inside the block. This is not a problem as long as the subsequent logical operation does not mix X and Z errors, as e.g. is the case for the logical CNOT which are transversal for CSS codes. If however a logical S gate is applied next then we must enforce property 2 in a stricter sense and prevent X and Z errors acting on different qubits at the output of EC. This can be achieved by extracting the syndrome a second time by running the EC circuit again. This modification will have no effect on the accuracy threshold since the logical S gate can be handled via injection by teleportation [4].

A similar ancilla decoding technique can replace verification when EC uses a quantum code that corrects $t > 1$ errors. Now, properties $0-3$ in §10 in [6] are sufficient to guarantee fault tolerance and our decoding circuit must be designed appropriately. Most importantly, we must ensure that, with $k \leq t$ faults inside EC, errors acting on more than k qubits that may propagate from the ancilla to the data can be diagnosed by the subsequent ancilla decoding and inverted. This can be accomplished by encoding the ancilla into a t-bit classical repetition code before decoding each sub-block separately similar to Fig. 2. For example, for the [[23,1,7]] Golay code that corrects $t = 3$ errors, ancilla decoding can replace verification if we encode the ancilla after interaction with the data into the 3-bit classical repetition code [7].

Some examples—We will now give some examples of this method in use. Let us begin with fault-tolerant syndrome measurement using four-qubit cat states, which is e.g. useful for EC with the [[5,1,3]] or [[7,1,3]] codes. The circuit for encoding, verifying and interacting these cat states with the data was shown in Fig. **??**. An alternative circuit that performs the same measurement without ancilla verification was shown in Fig. **??**.

The circuit in Fig. **??** is fault tolerant because the error $X^{(1)}X^{(2)}$ (or its equivalent $X^{(3)}X^{(4)}$) which may appear in the encoder in first order will be detected as it leads to all three measurements of Z after decoding giving outcome -1. In addition, no single fault inside the decoding circuit can flip all three Z-measurement outcomes, something which would lead us to mistakenly cause a weight-two error in the data by applying an unnecessary correction.

The second example is fault-tolerant measurement using seven-qubit cat states, which is e.g. needed for logical measurements that prepare ancilla needed for universality in the [[7,1,3]] code (see Figs. 13 and 14 in [6]). The circuit for encoding and verifying these cat states (Fig. 14 in [6]) is shown in Fig. 3.

The verification can again be omitted if, after interaction with the data, the cat state is decoded with the circuit shown in Fig. 4. To understand how the outcomes of the final measurements of Z allow us to diagnose any multi-qubit X errors having resulted from a single fault in the ancilla encoder, we follow the propagation of these

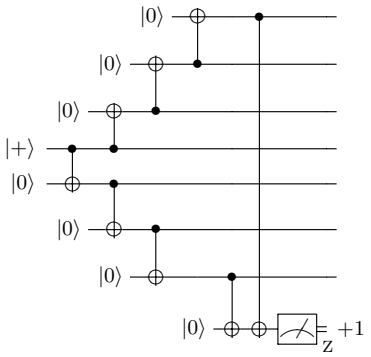

FIG. 3: Encoding and verification of a 7-qubit cat state. Similar to Fig. 1 of the main text, a verifier qubit is used to measure the parity $Z^{(1)}Z^{(7)}$ on the ancilla. Any of the high-weight X errors ($X^{(1)}X^{(2)}$, $X^{(6)}X^{(7)}$, $X^{(1)}X^{(2)}X^{(3)}$, or $X^{(5)}X^{(6)}X^{(7)}$) created in the encoder in first order is thus detected before the ancilla interacts with the data.

errors through the decoding circuit:

$$\begin{aligned} X^{(1)}X^{(2)} &\rightarrow X^{(1)}X^{(2)}X^{(6)} \\ X^{(6)}X^{(7)} &\rightarrow X^{(6)}X^{(7)} \\ X^{(1)}X^{(2)}X^{(3)} &\rightarrow X^{(1)}X^{(2)}X^{(3)}X^{(6)}X^{(7)} \\ X^{(5)}X^{(6)}X^{(7)} &\rightarrow X^{(2)}X^{(4)}X^{(6)}X^{(7)} \end{aligned} \tag{2}$$

An X error appearing on the right-hand side of Eq. (2) will result in the measurement of Z on the corresponding qubit giving an outcome -1. We note that different initial errors propagate to different final error patterns and, hence, distinct measurement outcomes which allows distinguishing them. In addition, it is straightforward to see that no single fault inside the decoder can lead to any of the final error patterns in Eq. (2). So no fault inside the decoder can make us mistakenly apply a multi-qubit correction to the data.

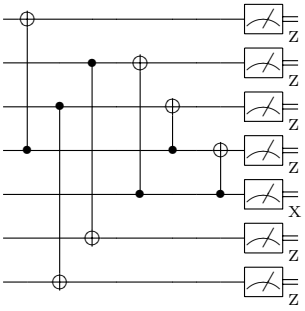

FIG. 4: The decoding circuit that replaces verification for the 7-qubit cat state prepared as in Fig. 3. The outcome of the measurement of X on the fifth qubit gives the eigenvalue of the measured operator on the data. As in Fig. **??**, all measurements of Z give ideally outcome $+1$.

Our third example is fault-tolerant EC using Steane's method for the [[7,1,3]] code. In this method, logical $|0\rangle$ and $|+\rangle$ states are sequentially coupled to the data block

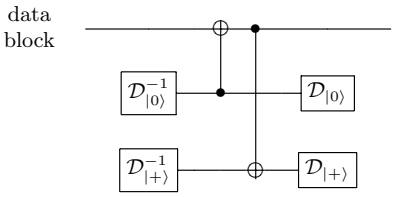

FIG. 5: Steane's EC without ancilla verification for the [[7,1,3]]. The encoding circuit for the $|0\rangle$ state ($\mathcal{D}^{-1}_{|0\rangle}$) is shown separately in Fig. 6, and the corresponding decoder, which here includes the final measurements, ($\mathcal{D}_{|0\rangle}$) in Fig. 7. The encoder and decoder for the $|+\rangle$ state are identical with the direction of the CNOT gates reversed and with qubit preparations and measurements performed in the conjugate bases.

to extract the syndrome information. In Steane's original scheme each ancilla is verified by either comparing two independently-encoded ancilla copies or by measuring suitable parities with extra verifier qubits (for the [[7,1,3]] code the measurement of a single parity is sufficient; see [4]). In our variant of this method no verification is performed and after encoding the ancilla is allowed to interact with the data. The decoding circuit that is applied next to the ancilla is identical with the encoding circuit. A schematic of this EC method is shown in Fig. 5, where the encoder ($\mathcal{D}^{-1}_{|0\rangle}$) and decoder ($\mathcal{D}_{|0\rangle}$) of the logical $|0\rangle$ state are shown separately in Fig. 6 and Fig. 7, respectively.

To show the tolerance of this design to single faults, we first list the possible multi-qubit X errors produced in first order in the encoder $\mathcal{D}^{-1}_{|0\rangle}$: $X^{(1)}X^{(7)}$, $X^{(2)}X^{(3)}$, and $X^{(4)}X^{(5)}$. Propagating them through the decoding circuit of Fig. 7 we obtain

$$\begin{aligned} X^{(1)}X^{(7)} &\rightarrow (X^{(1)})X^{(3)}X^{(5)} \\ X^{(2)}X^{(3)} &\rightarrow (X^{(2)})X^{(6)}X^{(7)} \\ X^{(4)}X^{(5)} &\rightarrow (X^{(4)})X^{(6)}X^{(7)} \end{aligned} , \tag{3}$$

where we have put in parenthesis trivial errors acting on qubits subsequently measured in the X eigenbasis. As seen in Eq. (3), the first weight-two error gives a distinct syndrome from the other two, which have identical syndromes (they both flip the eigenvalues of the measurements of Z on the sixth and seventh qubit). This is however to be expected, because their product $X^{(2)}X^{(3)}X^{(4)}X^{(5)}$ is in the code stabilizer and so the same recovery operator can be applied for both.

Finally, it can be easily checked that the decoder is designed so that a single fault inside it cannot lead to any of the final error patterns in Eq. (3). Note that running the encoding circuit backwards would not have provided a decoding circuit with this property: Indeed, we can see that if e.g. the CNOT gate from the second to the third qubit is applied in the first time step of the decoder, then it will not be possible to distinguish whether the error $X^{(2)}X^{(3)}$ was produced by a fault in the encoder or by

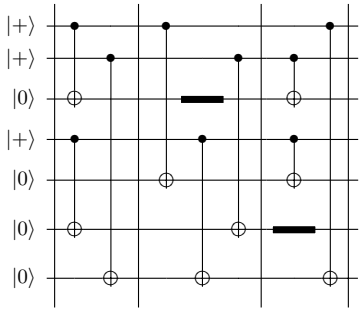

FIG. 6: Our encoder for the logical $|0\rangle$ state in the [[7,1,3]] code. Single fault events in this circuit can lead to weight-two X errors ($X^{(1)}X^{(7)}$, $X^{(2)}X^{(3)}$, or $X^{(4)}X^{(5)}$), which will propagate to the data block through the transversal CNOT gates of Fig. 5.

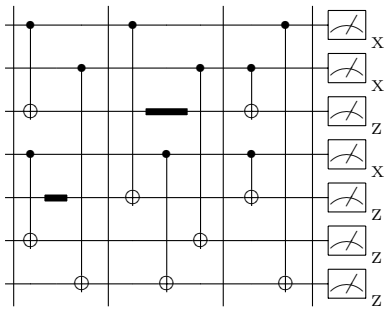

FIG. 7: Our decoder for the logical $|0\rangle$ state in the [[7,1,3]] code corresponding to the encoder of Fig. 6. The measurements of X yield the syndrome for Z errors in the data block, while all measurements of Z give ideally outcome $+1$.

this decoder CNOT gate failing.

Conclusion—Avoiding ancilla verification is helpful when measurements are slow since measurement outcomes need not be available immediately. Furthermore, the EC circuits become more efficient in both the number of qubits and operations compared to the EC circuits that use ancilla verification. For example, using this new method to perform EC inside the [[7,1,3]] CNOT-exRec in [6] decreases the total number of locations from 575 to 351 and the number of ancillary qubits by half. Counting malignant pairs in the new circuit nearly doubles the accuracy threshold lower bound found in [6] which changes from 2.73×10^{-5} to 5.36×10^{-5}. This method may also prove beneficial for fault tolerance with geometric locality constraints since the reduction in the number of qubits will result in a smaller unit cell and so shorter movement. Finally, we would like to comment that it would be interesting to investigate whether a similar ancilla decoding technique can replace verification in the teleported error-correction method discussed in [8].

[1] P. W. Shor. p. 56 in *37th Annual Symposium on Foundations of Computer Science* (FOCS '96), 1996.
[2] D. P. DiVincenzo and P. W. Shor. *Phys. Rev. Lett.* 77, 3260–3263, 1996.
[3] A. Steane. *Phys. Rev. Lett.* 78(2252), 1997.
[4] K. M. Svore, D. P. DiVincenzo, and B. M. Terhal. quant-ph/0604090.
[5] J. Preskill. pp. 213–269 in *Introduction to Quantum Computation*, eds. H.-K. Lo, S. Popescu and T.P. Spiller (1998, World Scientific, Singapore).
[6] P. Aliferis, D. Gottesman, and J. Preskill. *Quant. Inf. Comput.* 6(2), 97–165, 2006.
[7] B. Reichardt, private communication.
[8] E. Knill. *Nature*, 434:39–44, 2005.