A theory of single-shot error correction for adversarial noise

Earl T. Campbell
Department of Physics & Astronomy, University of Sheffield, Sheffield, S3 7RH, United Kingdom.

Single shot error correction is a technique for correcting physical errors using only a single round of noisy check measurements, such that any residual noise affects a small number of qubits. We establish a general theory of single-shot error correction where the crucial property is called good soundness of the code's measurement checks. Good code soundness in topological (or LDPC) codes is shown to entail a macroscopic energy barrier for the associated Hamiltonian. Consequently, 2D topological codes with local checks can not have good soundness. In tension with this, we also show that for any code a specific choice of measurement checks does exist that provides good soundness. In other words, every code can perform single shot error correction but the required checks may be nonlocal and act on many qubits. If we desire codes with both good soundness and simple measurement checks (the LDPC property) then careful constructions are needed. Finally, we use a double application of the homological product to construct quantum LDPC codes with single-shot error correcting capabilities. Our double homological product codes exploit redundancy in measurements checks through a process we call metachecking.

arXiv:1805.09271v2 [quant-ph] 3 Jul 2018

In the simplest model of quantum error correction, noise affecting qubits is corrected under the assumption that measurements are performed perfectly. In reality, measurement results will be unreliable. The standard tactic for combating measurement noise is to repeat the measurements and build a timeline of measurement data. Error correction software can then attempt to infer the most likely explanation of the observed measurement results. The number of measurement rounds required will typically grow with the code size. Recently, single-shot error correction was proposed by Bombin as a radically different solution to measurement noise [1]. In single-shot error correction, no repeated measurements are needed. Benefits include faster error correction and an inherent resilience to temporally correlated noise [2]. However, few codes are known to support single-shot error correction. This idea was proposed in the setting of topological codes in three or four spatial dimensions, such as the three dimensional gauge colour code [3] and four dimensional toric code [4]. Very recently, it has been reported that quantum expander codes also allow for single-shot error correction [5]. Quantum data-syndrome codes are also closely related to single-shot codes [6, 7]. The development and implementation of decoding algorithms for single-shot error correction is also limited with only a few examples [8, 9]. So far progress has been focused on specific examples and one of our goals here is to lay down a common framework within which single-shot error correction can be understood and analysed.

In the idealised setting of perfect measurements, error correction will return the system back into the code-space, either with or without a logical error. A quantum code is parametrised by its distance d where perfect measurements can always detect noise on fewer than d qubits. Consequently, noise on any $(d-1)/2$ qubits can be successfully corrected, even if the damaged qubits are chosen by an adversary who is attempting to corrupt the quantum information. Here we consider adversarial noise in the single-shot setting. We allow for physical qubit errors and measurement errors to appear in any pattern but affecting a limited number of qubits and measurements. Given corrupt measurement data, error correction may not even return the system to the code-space, but will leave some residual qubit error. Single-shot error correction aims to control the size of this residual error. Central to achieving this is the notion of soundness [10, 11]. Loosely, a code has good soundness if small measurement syndromes can be produced by small qubit errors. Good soundness is closely related to local testability of codes [10, 11] and energy barriers in self-correcting quantum memories [12–14]. It is clear that the 4D toric codes have good soundness properties. We shall also show that good soundness entails the existence of a macroscopic energy barrier [12, 15] and consequently 2D topological codes cannot possess good soundness properties. However, we also show that given any quantum code we can adapt the check measurements to ensure good soundness, though in the process any topological and or low-density parity check (LDPC) properties will be lost. This leads to the surprising insight that any quantum error correction code can perform single shot error correction, provided we are content with error correction measurements involving a large number of qubits. The interesting challenge is then to find codes that combine good soundness with LDPC properties.

The second part of this work provides techniques for constructing quantum codes with good single-shot correcting capabilities. Our approach is to use a double application of the homological, or hypergraph, product. The hypergraph product was first used by Tillich and Zemor [16] to show that any two classical codes can be combined to make a new quantum code. Unlike the standard CSS construction, no special relationship between the two codes is required by the hypergraph product. This allowed Tillich and Zemor to use good expander graph codes as the input classical code into the hypergraph product construction, producing so-called quantum expander codes with a good rate (the number of logical qubits k scaling as a constant fraction of the number of physical qubits n) and distance scaling as

$O(\sqrt{n})$. Crucially, their construction was the first quantum LDPC code to achieve such parameters. Subsequent work has established an efficient decoder for quantum expander codes [17, 18] and during the preparation of this manuscript these decoders were shown to support single-shot error correction [5]. Our approach here has overlap in the formal techniques but is more widely applicable since it does not depend on the strong assumption that the initial classical code is an expander graph code. The hypergraph product is closely related to the homological product used in the study of algebraic topology. Bravyi and Hastings [19] used the homological product to construct codes with a linear distance and good rate; though they were not strictly low-density parity check codes. Audoux and Couvreur studied repeated application of the homological product [20].

Our approach will be to use two applications of the homological product to design single-shot codes from any classical code. Two applications of the homological product generates a structure that in homology theory would be described as length 4. Sometimes this length-4 algebraic structure can be embedded within a geometrically local 4-dimensional manifold and the resulting quantum code would be a 4-dimensional topological code. Given a family of LDPC classical codes, our construction gives a family of LDPC quantum codes with good soundness, successfully combining these two desirable properties. However, our approach is inherently algebraic, providing many codes with no natural spatial topology, unless the original classical codes are topological. From the perspective of practical implementations, a topological code of modest dimension may seem preferable. However, topological codes are constrained by trade-off bounds on the achievable code parameters [21, 22] and so non-topological codes can be much more efficient.

We begin by reviewing the key concepts (Sec. I) before giving a more technical statement of the main results (Sec. II). We prove sufficient conditions for single-shot error correction in Sec. III. We discuss the relationship between soundness and energy barriers in Sec. IV. We show how measurement checks can be redefined for any code to provide good soundness in Sec. V. We give a general overview of how homology theory can be used to describe quantum codes in Sec. VI. This establishes the technical groundwork for Sec. VII where we give code constructions that meet our criteria using a double application of the homological product. We conclude with a discussion of the remaining open problems and the limitations of considering adversarial noise rather than stochastic noise.

I. KEY CONCEPTS

The preliminary material covered in this section draws from the work of Bombin [1, 2] and was influenced by Brueckmann's thesis [23], though our presentation is less topological and has some new ideas.

A. Stabiliser codes

An n qubit error correcting code storing k logical qubits can be represented by a projector Π onto the codespace. Stabiliser codes are an important class where Π can be described in terms of the code stabiliser $\mathcal{S}$. That is, $\mathcal{S}$ is an abelian subgroup of the Pauli group such that for all $S \in \mathcal{S}$ we have $S\Pi = \Pi S = \Pi$. To perform error correction we measure some set of checks $\mathcal{M} \subset \mathcal{S}$ that generate $\mathcal{S}$ under multiplication. We require that $\mathcal{M}$ suffices to the generate the whole stabiliser of the codespace but we allow for the possibly of $\mathcal{M}$ being overcomplete. We define the weight $\mathrm{wt}(\cdot)$ of a Pauli operator P as the number of qubits on which P acts nontrivially (the identity is the only trivial Pauli). We say a family of quantum codes Π_n with measurement strategies $\mathcal{M}_n$ are low-density party check codes (LDPC) if there exists a for every n and a constant C such that

1. For all $S \in \mathcal{M}_n$ we have $\mathrm{wt}(S) \leq C$;
2. For every physical qubit in the code, there are no more than C checks in $\mathcal{M}_n$ that act non-trivially on that qubit.

It is crucial that the constant C is the same for every code in the family. One pratical consequence is that for LDPC codes the complexity of measuring checks does not increase with the code size. Note that topological code families are always LDPC.

Also important is the code distance d_Q. We use the subscript Q to distinguish this from the single-shot distance (denoted d_{ss}) that we define later. The distance d_Q is simply the minimum $\mathrm{wt}(P)$ over all P such that $P\Pi = \Pi P$ but $P \notin \mathcal{S}$. To summarise, an $[[n, k, d_Q]]$ code has parameters n (number of physical qubits), k (number of logical qubits) and d_Q (qubit code distance).

The measurement syndrome is the result of measuring $\mathcal{M} = (M_1, M_2, \ldots, M_m)$. Given a physical Pauli error E we can denote $\sigma(E)$ as the syndrome due to E assuming perfect measurements. We use the convention that $\sigma(E)$ is a binary column vector with elements

$$[\sigma(E)]_i = \begin{cases} 1 & \text{if } EM_i = -M_iE \\ 0 & \text{if } EM_i = M_iE \end{cases} \tag{1}$$

We say $E \sim E'$ if they have the same syndrome, formally $\sigma(E) = \sigma(E')$. We will be interested in the weight of the syndrome and always use $|\ldots|$ to denote the Hamming weight of binary vectors. The Hamming weight is the number of nonzero elements.

B. Soundness

Soundness is a property that appears to be crucial to single-shot error correction. Roughly, this extra property is that for low weight syndromes there exists a low weight physical error producing the syndrome. More formally,

Definition 1 (Soundness) *Let t be an integer and $f : \mathbb{Z} \to \mathbb{R}$ be some function called the soundness function. Given some set of Pauli checks $\mathcal{M}$ onto codespace Π, we say it is (t, f)-sound if for all Pauli errors E with $|\sigma(E)| = x \leq t$, it follows that there exists an $E^\star \sim E$ such that $\mathrm{wt}(E^\star) \leq f(x)$.*

The phrase soundness comes from the literature on locally testable codes [10, 11]. In particular, the above definition is similar to Def 14 of Ref. [10] though this earlier work did not allow for the $\mathrm{wt}(E) \leq t$ clause.

The above definition is somewhat vacuous since for $t = 0$ or $f(x) = n$ any n-qubit code will obviously be (t, f)-sound. Rather we are interested in good cases where t is large and f is in some sense small. A more rigorous notion of good soundness requires us to consider not just a single code but an infinite family of codes.

Definition 2 (Good soundness) *Consider an infinite family of n-qubit codespaces Π_n with measurement checks $\mathcal{M}_n$. We say the family has good soundness if each Π_n is (t, f)-sound where:*

1. *t grows with n such that $t \geq an^b$ for some positive constants a, b. That is, $t \in \Omega(n^b)$ with $b > 0$;*
2. *and $f(x)$ is some polynomial that is monotonically increasing with x and independent of n.*

It is clear that not all code families have good soundness. For 2D toric codes with the standard choice of checks, an error violating only 2 checks can be of arbitrarily large size.

C. Energy barriers

Energy barriers play an important role in the design of passive quantum memories [13, 14]. While passive quantum memories are a distinct topic from active single-shot error correction, the two topics are intertwined. Earlier work [10] has commented on the relationship between soundness and energy barriers, though they used a more restrictive notion of soundness. For a stabiliser code with checks $\mathcal{M}$ we define a Hamiltonian

$$H = -\sum_{S \in \mathcal{M}} S. \tag{2}$$

We are interested in walks of quantum states $W = \{\psi_0, \psi_1, \psi_2, \ldots, \psi_L\}$ that fulfil

1. groundstates: ψ_0 and ψ_L are groundstates of H;
2. orthogonality: ψ_0 and ψ_L are orthogonal;
3. local errors: for every $j \in [1, L]$ there exists a single-qubit Pauli P_j such that $|\psi_j\rangle = P_j|\psi_{j-1}\rangle$.

For every such walk we associate an energy penalty

$$ep(W) = \max_{\psi_j \in W} \langle\psi_j|H|\psi_j\rangle - E_{gs}, \tag{3}$$

where E_{gs} is the ground state energy. The energy barrier of check set $\mathcal{M}$ and associated Hamiltonian is then the minimum $ep(W)$ over all walks W satisfying the above conditions. Less formally, the energy barrier is the minimum energy required to go from one ground state to another.

Every quantum code will have some size energy barrier. We are really interested in the scaling with code size. Given an infinite family of n-qubit quantum codes with checks $\mathcal{M}_n$, if the energy barrier scales as $\Omega(n^c)$ for some positive constant c, then we say the family has a *macroscopic* energy barrier.

D. Measurement redundancy and single shot distance

We have allowed for some redundancy so that checks $\mathcal{M}$ may be overcomplete. This is pivotal for us to capture the single-shot properties of the 4D toric codes since they are only known to exhibit good soundness when an overcomplete set of checks are used. We quantify the amount of redundancy in a measurement scheme as the ratio between the number of measurements performed and the minimum number required to generate the stabiliser of the code and use υ to denote this ratio. Good soundness can always be achieved by allowing υ to grow with n by simply repeating the same measurements. Rather, the interesting cases are code families where υ is no more than a small constant factor. Since topological codes can use redundancy to achieve good soundness, it is reasonable to ask whether redundancy is necessary for good soundness? We will see later that redundancy is not always essential for good soundness (see Thm. 3 and Sec. V). However, it seems that redundancy does play an important role when one attempts to marry good soundness with LDPC properties.

Check redundancy provides consistency conditions that one can inspect for evidence of measurement errors. These are checks on checks and we call them metachecks. They do not represent a physical measurement but classical postprocessing on the measurement outcomes. It is essentially a classical error correcting code that can be represented by a parity check matrix H. Given a binary string s representing the outcome of syndrome measurements, we say Hs is the metacheck syndrome, where Hs is evaluated modulo 2. If there are no measurement errors then $s = \sigma(E)$ where E is the physical error. We model measurement errors as introducing an additional error u so that $s = \sigma(E) + u$. Since the metachecks are intended to look for measurement errors, we require that $H\sigma(E) = 0$ for all E. It follows that the metasyndrome $Hs = H(\sigma(E) + u) = Hu$ depends only on the measurement error u. Every metacheck must represent some redundancy between check operators, but we do not require that every redundancy present is represented by a metacheck. That is we allow for the possibility that there are syndromes s such that there is no error E satisfying

$s = \sigma(E)$. This motivates the following definition.

Definition 3 (Single shot distance) *For a code with checks $\mathcal{M}$ and metacheck matrix H we define the single shot distance as*

$$d_{ss} = \min\{|s| : \forall s \text{ with } Hs = 0 \text{ and } \nexists E \text{ s.t. } s = \sigma(E)\}. \quad (4)$$

We use the convention that $d_{ss} = \infty$ if for all s there exists some E such that $s = \sigma(E)$.

The single-shot distance relates to how many measurement errors can be tolerated before a failure occurs that we call a metacheck failure. In a metacheck failure, the syndrome has no explanation in terms of qubit errors. We remark that for any $\mathcal{M}$ we can always chose H in such a way that d_{ss} is infinite. However, sometimes a finite single shot distance may be preferred to ensure that the metacheck decoding process can be implemented using a local decoder and the literature already includes such examples [23]. For a code with metachecks we extend the notation $[[n, k, d_Q]]$ to $[[n, k, d_Q, d_{ss}]]$.

II. SUMMARY OF RESULTS

When we have N rounds of error correction we use a label $\tau \in \{1, \ldots, N\}$ for the round number. On round τ, we denote u_τ for the measurement errors and E_τ for the new physical errors. This accounts for both a single-shot ($N = 1$) and repeated applications of single-shot error correction ($N > 1$). We say single-shot error correction has been successful after the τ^{th} round if any residual noise has weight less than $d_Q/2$. Here we prove the following:

Theorem 1 (Single shot success) *Consider a quantum error correcting code with parameters $[[n, k, d_Q, d_{ss}]]$ that is (t, f)-sound. Single shot error correction (using a minimum weight decoder) will be successful if for every time step τ we have*

1. $|u_\tau| < \frac{1}{2}\min[d_{ss}, t]$;
2. $f(2|u_\tau|) + f(2|u_{\tau-1}|) + \text{wt}(E_\tau) < \frac{1}{2}d_Q$;

For the above bounds to be useful, the code must have a soundness function f that is fairly gentle (e.g. some polynomial). The proof is mostly linear algebra and is given in Sec. III.

Our second result is an observation on the connection between soundness and energy barriers.

Theorem 2 *Any LDPC code family with good soundness and code distance d_Q growing as $\Omega(n^c)$ for some constant $0 < c$ will also have a macroscopic energy barrier.*

This is proved in Sec. IV. We remark that Aharonov and Eldar made a similar observation [10] though using a much stronger notion of soundness. Since Bravyi and Terhal proved that no 2D topological code can have a macroscopic energy barrier [24], it follows immediately that

Corollary 1 *Any 2D topological code family with code distance d_Q growing as $\Omega(n^c)$ for some constant $0 < c$ will not have good soundness.*

We thank Michael Beverland for pointing out that this corollary follows directly from Thm. 2 and the Bravyi and Terhal result.

Next, we show that

Theorem 3 *For any n-qubit quantum error correcting code we can find a set of checks generating the code stabiliser (without any redundancy) such that these checks are $(\infty, f(x) = x)$-sound.*

The proof is elementary and given in Sec. V. While this is a simple result, it carries important implications for our understanding of soundness. It shows that any code family can be bestowed with good soundness by appropriate choice of checks, but in the process the LDPC property may be lost. Therefore, the interesting question is for which code families we can find checks that are simultaneously LDPC and of good soundness.

Our last main result is a recipe for quantum codes with the required properties. We show that

Theorem 4 (Construction of single-shot codes) *Given a classical error correcting code with parameters $[n, k, d]$ we can construct a quantum error correcting code with parameters $[[n_Q, k^4, d_Q \geq d, d_{ss} = \infty]]$ where*

$$n_Q = n^4 + 4n^2(n-k)^2 + (n-k)^4. \quad (5)$$

Furthermore, the code is (d, f)-sound with $f(x) = x^3/4$ or better. The check redundancy is bounded $\upsilon < 2$. Given a family of classical LDPC codes, this construction gives a family of quantum LDPC codes.

Before giving the proof, we establish how the mathematics of homology theory and chain complexes can be used to define quantum codes with metachecks. As such, we provide a pedagogical interlude in Sec. VI that introduces this correspondence. The proof is then given in Sec. VII and uses the homological product on chain complexes. Where possible we have converted abstract homological proofs into linear algebra. The constructions of Thm. 4 will emerge as a simple, special case of the techniques explored in Sec. VII, and we will see that codes with finite single-shot distance are also possible. An important metric is the encoding rate, the number of logical qubits per physical qubit k_Q/n_Q. The expressions for the inverse rate are neater to write

$$\frac{n_Q}{k_Q} = \frac{n^4 + 4n^2(n-k)^2 + (n-k)^4}{k^4} \quad (6)$$
$$= 6\left(\frac{n}{k}\right)^4 - 12\left(\frac{n}{k}\right)^3 + 10\left(\frac{n}{k}\right)^2 - 4\left(\frac{n}{k}\right) + 1.$$

From this, it is clear that for any family of classical codes with constant rate $n/k \leq A$, will yield a family of quantum codes with constant rate $n_Q/k_Q \leq A_Q \sim O(A^4)$.

We remark that the distance bound $d_Q \geq d$ and soundness properties are loosely bounded and for many codes could be significantly better than shown here.

Combining Thms. 1 and 4, we have that

Corollary 2 *Using the codes of Thm. 4, single shot error correction (using a minimum weight decoder) will be successful whenever for every time step τ we have*

1. $2|u_\tau|^3 + 2|u_{\tau-1}|^3 + \mathrm{wt}(E_\tau) < \frac{1}{2}d$;

These codes have infinite d_{ss} and so a metacheck failure never occurs. This does not mean the code can tolerate an infinite amount of measurement noise since the amount of residual noise still grows with the amount of measurement noise. Therefore, the conditions for single-shot error correction simplify down to the single condition shown.

III. CONDITIONS FOR SUCCESSFUL SINGLE-SHOT ERROR CORRECTION

This section proves that single-shot error correction will be successful provided the noise is sufficiently low as stated in Thm. 1. For most of this section, we consider a single round of error correction and so drop the subscript τ, but it will return later when we consider multiple rounds of single round of error correction. We will just use E for the physical errors present at the start of that round. Some of these errors will be newly acquired and some will be residual from the previous round. Given measurement data s we wish to decode as follows

Definition 4 (Single shot error decoding) *Given measurement outcomes $s = \sigma(E) + u$, we:*

1. *Syndrome decode: find s_{rec} with minimal $|s_{rec}|$ such that $s+s_{rec}$ passes all metachecks (so $H(s+s_{rec}) = 0$);*
2. *Qubit decode: find E_{rec} with minimal $\mathrm{wt}(E_{rec})$ such that $\sigma(E_{rec}) = s + s_{rec}$;*

We call $R = E \cdot E_{rec}$ the residual error.

This is the most common notion of weight minimisation. However, it might be possible to formulate single-shot error correction in an alternative way.

It is not possible to always find solutions to the above problem. For instance, one may find a minimising s_{rec} but then there is no E_{rec} satisfying the second condition. We call such an event a metacheck failure. However, we do have the following guarantee

Lemma 1 (Meta-check success) *We can find a solution to single-shot decoding provided that $|u| < d_{ss}/2$.*

The proof is essentially the same as standard proofs for correcting adversarial qubit errors. Metacheck failures correspond to cases where there exists a minimal weight s_{rec} where $H(s + s_{rec}) = 0$ but there is no physical Pauli error E such that $\sigma(E) = s + s_{rec}$. Note that whenever we use "+" between two binary vectors it should be read as addition modulo 2. First, we note that $H(s + s_{rec}) = H(\sigma(E) + u + s_{rec})$ and using $H\sigma(E) = 0$ we get that s_{rec} must satisfy $H(u + s_{rec}) = 0$. Since, $s_{rec} = u$ would satisfy this requirement and s_{rec} is minimum weight, we infer that $|s_{rec}| \leq |u|$. Using the triangle inequality we get $|s_{rec}+u| \leq 2|u| < d_{ss}$. By the definition of single shot distance, it follows that there exists a physical error E' such that $\sigma(E') = s_{rec} + u$. Using the syndrome relation $\sigma(E \cdot E') = \sigma(E) + \sigma(E')$ we obtain

$$\sigma(E \cdot E') = s + u + s_{rec} + u = s + s_{rec}. \tag{7}$$

Therefore, there is always a physical error (e.g. $E_{rec} = E \cdot E'$) consistent with the repaired syndrome $s + s_{rec}$ and the lemma is proved.

The above proof shows that the code can tolerant up to $d_{ss} - 1$ adversarial measurement errors and provide a solution to single-shot decoding. However, the story is not finished since even if a metacheck failure does not occur, a conventional logical failure might yet occur. Therefore, next we address the question of how we can ensure the residual error $R = E_{rec} \cdot E$ has bounded size. From $\sigma(E_{rec}) = s + s_{rec}$ we deduce $\sigma(R) = u + s_{rec}$ and so

$$|\sigma(R)| \leq 2|u| < d_{ss} \tag{8}$$

This prompts the question, given a small syndrome (consistent with metachecks) does there even exist a small weight physical error generating this syndrome! Indeed, this is not always the case; unless the code has nice soundness properties. Using our notion of soundness we can prove the following

Lemma 2 (An upper bound on residual error) *Consider a quantum error correcting code with parameters $[[n, k, d_Q, d_{ss}]]$ that is (t, f)-sound. Given measurement error u and physical error E. If*

1. *$|u| < d_{ss}/2$: the measurement error is small enough to ensure no metacheck failures;*
2. *$|u| < t/2$: the measurement error is small enough to use soundness properties;*
3. *$f(2|u|) + \mathrm{wt}(E) < d_Q/2$: the combined errors are sufficiently small;*

It follows that a solution to single-shot decoding will yield a residual error $R = E \cdot E_{rec}$ that such $R = S \cdot R^\star$ where S is a stabilizer of the code and $\mathrm{wt}(R^\star) \leq f(2|u|)$.

We know from above (Eq. 8) that the residual error R satisfies $|\sigma(R)| \leq 2|u| < d_{ss}$. By using the definition of (t, f)-soundness, we know that provided $2|u| \leq t$ there exists an $R^\star$ such that $\sigma(R) = \sigma(R^\star)$ and $\mathrm{wt}(R^\star) \leq f(2|u|)$. It remains to show that $S = RR^\star$ is a stabiliser of the code. Clearly, $\sigma(RR^\star) = \sigma(S) = 0$ so S is either a stabiliser or a nontrivial logical operator. It can only be a nontrivial logical operator if $d_Q \leq \mathrm{wt}(RR^\star)$.

The remainder of the proof shows that we instead have $\mathrm{wt}(RR^\star) < d_Q$ and so S is a stabiliser. We start with

$$R \cdot R^\star = E \cdot E_{rec} \cdot R^\star, \tag{9}$$

and

$$\mathrm{wt}(R \cdot R^\star) = \mathrm{wt}(E \cdot E_{rec} \cdot R^\star). \tag{10}$$

Using the triangle inequality

$$\mathrm{wt}(R \cdot R^\star) \leq \mathrm{wt}(E_{rec}) + \mathrm{wt}(E \cdot R^\star). \tag{11}$$

Since, E_{rec} is a minimum weight solution, we can assume that $\mathrm{wt}(E_{rec}) \leq \mathrm{wt}(E \cdot R^\star)$, and hence

$$\mathrm{wt}(R \cdot R^\star) \leq 2\mathrm{wt}(E \cdot R^\star) \leq 2\mathrm{wt}(E) + 2\mathrm{wt}(R^\star). \tag{12}$$

Using again that $\mathrm{wt}(R^\star) \leq f(2|u|)$ we obtain

$$\mathrm{wt}(R \cdot R^\star) \leq 2(f(2|u|) + \mathrm{wt}(E)). \tag{13}$$

We are interested in when the LHS is upper bounded by d_Q, which follows from the RHS being upper bounded by d_Q, which is precisely the third condition of the lemma. Therefore, $\mathrm{wt}(R \cdot R^\star) < d_Q$ and consequently $R = S \cdot R^\star$.

In many rounds of error correction, the error E will have two components, the new physical noise and the noise residual from the previous round. Assuming all previous rounds of error correction have been successful, on the τ^{th} round the residual error has weight upper bounded by $f(2|u_{\tau-1}|)$. So the physical error has total weight upper bounded by $f(2|u_{\tau-1}|) + \mathrm{wt}(E_\tau)$ where E_τ is the new error. Therefore, the condition for success on the τ^{th} round is expressed by the conditions of the Thm. 1. Indeed, this concludes the proof.

IV. SOUNDNESS AND ENERGY BARRIERS

Here we discuss the relationship between the concept of code soundness and energy barriers in physical systems, resulting in a proof of Thm. 2. The reader ought to ensure familiarity with the introductory material in subsections I B and I C. Aharonov and Eldar remarked in Ref. [10] that codes with good soundness lead to large energy barriers, though they were interested in a strictly stronger definition of soundness.

A key lemma is the following

Lemma 3 *Consider a $[[n, k, d_Q]]$ quantum code with checks $\mathcal{M}$ that is (t, f)-sound and where all qubits are involved in no more than C checks. It follows that the energy barrier is at least $f^{-1}(w)$ where $w = \min[t/C, (d_Q - 1)/2]$ and f^{-1} is the inverse of the soundness function.*

For any walk of states $\{\psi_1, \psi_2, \ldots \psi_L\}$ we have a sequence of Pauli operators $\{\mathbb{1}, E_1, E_2, \ldots E_L\}$. For every E_j in the sequence we consider the reduced weight

$$\mathrm{wt}_R(E) := \min_V \{\mathrm{wt}(EV) : V \in \mathcal{P}, \sigma(V) = 0\}, \tag{14}$$

where the minimisation is over all V in the Pauli group $\mathcal{P}$. Herein we use V_j to denote Pauli operators that achieve the above minimisation. Since $\sigma(V_j) = 0$ every V_j is either a stabiliser or a nontrivial logical operator. By the groundstates and orthogonality property, it follows that $V_0 = \mathbb{1}$ and $V_n = E_n$. So the sequence starts with a stabiliser and ends with a nontrivial logical operator. Therefore, there must exist a $j^\star$ such that $V_{j^\star}$ is a stabiliser and $V_{j^\star+1}$ is a nontrival logical operator. Therefore, $V_{j^\star}V_{j^\star+1}$ must also be a nontrivial logical operator and so

$$d_Q \leq \mathrm{wt}(V_{j^\star}V_{j^\star+1}). \tag{15}$$

Furthermore, using the triangle inequality we have

$$\begin{aligned}\mathrm{wt}(V_{j^\star}V_{j^\star+1}) \leq & \mathrm{wt}(V_{j^\star}E_{j^\star}) + \mathrm{wt}(V_{j^\star+1}E_{j^\star+1}) \\ & + \mathrm{wt}(E_{j^\star}E_{j^\star+1}) \\ & = \mathrm{wt}_R(E_{j^\star}) + \mathrm{wt}_R(E_{j^\star+1}) + 1. \end{aligned} \tag{16}$$

We have used $\mathrm{wt}_R(E_j) = \mathrm{wt}(V_jE_j)$ on the first two terms and the local errors condition on the last term. Combining this with Eq. (15), leads to

$$d_Q \leq 2\mathrm{max}[\mathrm{wt}_R(E_{j^\star}), \mathrm{wt}_R(E_{j^\star+1})] + 1, \tag{17}$$

and so

$$\frac{d_Q - 1}{2} \leq \max[\mathrm{wt}_R(E_{j^\star}), \mathrm{wt}_R(E_{j^\star+1})]. \tag{18}$$

Consider the sequence of reduced weights $\{\mathrm{wt}_R(E_0), \mathrm{wt}_R(E_1), \ldots, \mathrm{wt}_R(E_n)\}$. The sequence starts and ends with zero and at some point must reach $(d_Q - 1)/2$ or higher. Furthermore, the local error condition entails that $|\mathrm{wt}_R(E_{j+1}) - \mathrm{wt}_R(E_j)|$ is either 0 or 1 and so the sequence of reduced weights must include every integer from 0 to $(d_Q - 1)/2$. Therefore, we can set w equal to $\min[t/C, (d_Q - 1)/2]$ and there must exist an E_j with $\mathrm{wt}_R(E_j) = w$. Next, we consider the syndrome $\sigma(E_j)$ and note that $\sigma(E_j) = \sigma(E_jV_j)$ where $\mathrm{wt}(E_jV_j) = \mathrm{wt}_R(E_j)$. The LDPC condition of the code ensures that for any E we have $|\sigma(E)| \leq C\mathrm{wt}(E)$. Therefore, for the E_j with $\mathrm{wt}_R(E_j) = w$ we have $|\sigma(E_j)| \leq Cw$. Since $w \leq t/C$ we have $|\sigma(E_j)| \leq t$ and the soundness property can be deployed to conclude that $f^{-1}(w) \leq |\sigma(E_j)|$. Since this holds for every possible walk, $f^{-1}(w)$ gives a lower on the error barrier and we have proved Lem. 3.

From Lem. 3 we can quickly obtain a proof of Thm. 2. We consider an infinite family of $[[n, k, d_Q]]$ low-density parity check codes with checks $\mathcal{M}$ and good soundness. That is, the codes are (t_n, f)-sound such that: the soundness function $f \in O(x^a)$ is independent of n; and t_n grows as $\Omega(n^b)$ for some constants a and b. We further assume that the code distance d_Q grows as $\Omega(n^c)$ for some constant c. Since $d_Q \in \Omega(n^c)$ and $t \in \Omega(n^b)$, we can choose $w = \min[t/C, (d_Q - 1)/2] \in \Omega(n^{\min[c,b]})$ in Lem. 3. It follows that the energy barrier scales as $\Omega(n^{\min[c,b]/a})$ since $f \in O(x^a)$ and so $f^{-1} \in \Omega(x^{1/a})$. Therefore this code

family has a macroscopic energy barrier. Notice that soundness is not the only ingredient in the proof, the LDPC condition is also crucial. It is unclear whether a similar result can be shown without the LDPC condition.

We remark that the converse statement would be that any LDPC code family with a macroscopic energy barrier has good soundness. We have neither proof nor counterexample and so the status of this converse statement remains open.

Bravyi and Terhal proved that no 2D topological stabiliser codes have a macroscopic energy barrier [24]. Therefore, such codes cannot have good soundness as we stated in corollary 1. This is nearly a statement that single-shot error correction is impossible in 2D topological stabiliser codes and we believe this to be the case. Though one must be cautious as we have shown good soundness to be sufficient condition for single shot error correction but not a necessary one. Clearly, if a code does not have good soundness then minimum weight decoding (in the sense of Def. 4) can lead to large weight residual error. However, if one deviates from the minimum weight decoding strategy then the picture becomes less clear. For instance, one strategy might be that when the minimum weight solution is high weight, we do not attempt to return the system to the codespace but instead apply a partial recovery. For instance, if we observe two far apart checks with "-1" outcomes in the 2D toric code, then we could apply a partial recovery that reduces the distance between these checks. Indeed, there are cellular automata decoders for the 2D toric code that behave just like this [9, 25–27]. These fail to qualify as single-shot decoders in the usual sense as they rely on the syndrome history (partial stored in a cellular automata). But they highlight that single-shot error correction might be possible using an imaginative decoder approach based on partial recoveries.

V. GOOD SOUNDNESS FOR ALL CODES

Often we conflate a quantum error correction code with a set of checks $\mathcal{M}$ that generate the stabiliser. But there are many choices of checks for any given code. Crucially, the soundness properties depend on the set of checks. Here we prove Thm.3, which roughly states that for any code we can find a check set with good soundness properties. The proof follows from the following lemma.

Lemma 4 *Given an $[[n, k, d_Q]]$ quantum error correction code with stabiliser $\mathcal{S}$ there exists a minimal set of generators $\mathcal{M} = \{M_1, M_2, \ldots, M_{n-k}\}$ and pure Pauli errors $\mathcal{E} = \{E_1, E_2, \ldots, E_{n-k}\}$ such that: (1) $[M_i, E_j] \neq 0$ if and only if $i = j$; and (2) every E_j acts non-trivially on only a single qubit and so* $\mathrm{wt}(E_j) = 1$.

We first consider the consequence of this lemma. Given such a set of checks, it follows that if s is a syndrome unit vector (so $|s| = 1$) with a 1 entry in the j^{th} location, then $s = \sigma(E_j)$ (recall Eq. (1)). More generally, s can be written a product of $|s|$ unit vectors and therefore $s = \sigma(E)$ where

$$E = \prod_{j:s_j=1} E_j. \tag{19}$$

Since $\mathrm{wt}(E_j) = 1$ we have $\mathrm{wt}(E) \leq |s|$ (with more work one can prove equality). Therefore, the checks are (t, f)-sound with $t = \infty$ and $f(x) = x$ since: the argument holds for any weight syndrome, and so the value of t is unbounded; and the weight of the physical error is no more than the weight of the syndrome, so we have $f(x) = x$.

The proof of Lem. 4 is essentially a step in the proof Lem. 2 of Ref. [28]. In Ref. [28], it is shown that upto to qubit labelling and local Clifford unitaries, the generators M_j can be brought into a diagonalised form inspired by the graph state formalism. In this form, M_j acts on the j^{th} qubit with Pauli X. On all others qubits with labels 1 through to $n - k$, the operator M_j acts as either Pauli Z or the identity. Therefore, Pauli Z acting on qubit j anticommutes with generator M_j and commutes with all other generators. Accounting for local Cliffords and original qubit labelling, the required E_j may act on a different qubit and may be different from Pauli Z, but it will be a single qubit Pauli. This completes the proof.

The soundness properties proven above are extremely strong. This leads to the counter-intuitive result that single shot error correction is possible for any code and without any check redundancy. The price to pay is that one must use a certain set of checks such as the diagonalised form above. As such, if the checks are initially low weight (e.g. the code is a member of an LDPC family) then this property may be lost as the diagonalisation process leads to high weight checks. Indeed, we can prove the following strong limitation on diagonalisation methods.

Claim 1 *Consider a family of codes with checks in the diagonalised form used in the proof of Lem. 4. Assume also the family is LDPC for the diagonalised checks, such that in every code no qubit is acted on by more than C checks. It follows that the distance is bounded $d_Q \leq C+1$ for all codes in the family.*

We prove this by constructing an explicit error $F \neq \mathbb{1}$ such that $\sigma(F) = 0$ and $\mathrm{wt}(F) \leq C + 1$. First, we let P be some single qubit Pauli ($\mathrm{wt}(P) = 1$) acting on a qubit with label exceeding $n-k$. By the LDPC property $|\sigma(P)| \leq C$. Furthermore, following previous arguments there exists an E acting on the first $n-k$ qubits such that $\sigma(E) = \sigma(P)$ and $\mathrm{wt}(E) \leq |\sigma(P)|$. Combing $\mathrm{wt}(E) \leq |\sigma(P)|$ and $|\sigma(P)| \leq C$ gives $\mathrm{wt}(E) \leq C$. Setting $F = EP$, we have that

$$\sigma(F) = \sigma(E) + \sigma(P) = 2\sigma(E) = 0 \tag{20}$$

and

$$\mathrm{wt}(F) \leq \mathrm{wt}(E) + \mathrm{wt}(P) \leq C + 1. \tag{21}$$

Lastly, $F \neq \mathbb{1}$ follows since E and P have nontrivial action on disjoint sets of qubits.

The LDPC property is highly desirable and so too is growing code distance. Therefore, we need an alternative route to good soundness.

VI. TANNER GRAPHS, CHAIN COMPLEXES AND HOMOLOGY THEORY

From here on we specilise to codes with checks $\mathcal{M}$ that can be partitioned into checks in the Z and X Pauli basis. For such codes, we describe quantum codes in a graphical language that extends on the classical use of Tanner graphs. We will explain the correspondence between the graphical representation and a linear algebra description in terms of concepts from algebraic topology.

Several example graphs are given in Fig. 1. In every case, the graph breaks up into $D+1$-partitions and we will refer to D as the length of the graph. Each partition comes with a set of vertices C_j. We use a binary matrix δ_j to describe the adjacency between vertices in C_j and C_{j+1}. Specifically, matrix δ_j has a "1" in entry (a,b) if and only if the b^{th} vertex in C_j is connected to the a^{th} vertex in C_{j+1}. Therefore, δ_0 is the well-known parity check matrix of a classical code. Furthermore, δ_0 is the parity check matrix for bit-flip (X) errors in a quantum code. Using superscript T for transpose, the matrix δ_{-1}^T is the parity check matrix for phase-flip (Z) errors in a quantum code.

We conflate thinking of C_j as a set of vertices and also as a binary vector space $\mathbb{Z}_2^{n_j}$ where n_j denotes the number of vertices in C_j. A unit vector $\hat{u}$ has only a single entry with value 1 and identifies single vertex in C_j. Therefore, given a pair of unit vectors $\hat{u} \in C_j$ and $\hat{v} \in C_{j+1}$, we have $\hat{v}^T \delta_j \hat{u} = 1$ if and only if the corresponding vertices are connected. Therefore, given a unit vector $\hat{u} \in C_1$ identifying a measurement (or check) for bit-flip errors, the vector $\delta_0^T \hat{u}$ identifies the (qu)bits involved in that check. We use the notation

$$X[u] := \otimes_j X_j^{u_j}, \tag{22}$$

$$Z[v] := \otimes_j Z_j^{v_j}, \tag{23}$$

where u and v are binary vectors. The graph should be read as not just defining a code but also the measurement scheme. So for every unit vector $\hat{u}$ in C_1, the graphical formalism stipulates that we measure the operator $Z[\delta_0^T \hat{u}]$. So in our earlier notation $Z[\delta_0^T \hat{u}]$ would be a member of $\mathcal{M}$ and is a stabiliser of the code. Since the stabiliser is a group, we have that $Z[\delta_0^T u]$ is a stabiliser for any vector $u \in C_1$. Similarly, $X[\delta_{-1} v]$ is a stabiliser of the code for every $v \in C_{-1}$. Operators $X[\delta_{-1} v]$ and $Z[\delta_0^T u]$ will commute if and only if $(\delta_0^T u)^T \delta_{-1} v = u^T \delta_0 \delta_{-1} v = 0$ where all such equations should be read using addition modulo 2. Since we need all such operators to commute, we require that $\delta_0 \delta_{-1} = 0$. Conversely, if $X[e]$ with $e \in C_0$ is an error, the vector $\delta_0 e$ is the Z-measurement syndrome assuming ideal measurements.

In homology theory, this whole structure is called a chain complex and the operators δ_j are called boundary maps provided the relation $\delta_{j+1}\delta_j = 0$ holds for all j. Therefore, given a homological chain complex the commutation relations are automatically satisfied since $\delta_0 \delta_{-1} = 0$. Remarkably, requiring $\delta_{j+1}\delta_j = 0$ not only gives us the required commutation relations but also ensures that the metachecks are suitably defined. We will show this formally. Consider a physical error $X[e]$. It will generate Z-syndrome $\delta_0 e$ assuming no measurement errors. Since there are no measurement errors, the metasyndrome $x = \delta_1 \delta_0 e$ ought to be the all zero vector, which is ensured if $\delta_1 \delta_0 = 0$.

Let us connect this back to the notation used in the first part of this paper. The check set is

$$\mathcal{M} = (Z[\hat{u}_1], \ldots, Z[\hat{u}_{n_1}], X[\hat{v}_1], \ldots, X[\hat{v}_{n_{-1}}]) \tag{24}$$

where $\hat{u}_j$ and $\hat{v}_j$ are unit vectors with the unit in the j^{th} location. Any Pauli error can be expressed as $E = X[e]Z[f]$ for some vectors e and f. The syndrome of this Pauli is then the combination of the Z and X syndromes, so that

$$\sigma(X[e]Z[f]) = \begin{pmatrix} \delta_0 e \\ \delta_{-1}^T f \end{pmatrix}. \tag{25}$$

Furthermore, the whole metasyndrome matrix has block matrix form

$$H = \begin{pmatrix} \delta_1 & 0 \\ 0 & \delta_{-2}^T \end{pmatrix}. \tag{26}$$

From this we see that the condition required earlier (that $H\sigma(E) = 0$ for all Pauli E) follows from the fundamental property of chain complexes, specifically $\delta_1 \delta_0 = 0$ and $\delta_{-2}^T \delta_{-1}^T = 0$.

Next, we study some parameters of chain complexes. We use n_j to denote the number of vertices in C_j, and equivalently the dimension of the associated vector space $\mathbb{Z}_2^{n_j}$. The matrix δ_j will have n_j columns and n_{j+1} rows. An important parameter is the j^{th} Betti number, which we denote k_j. For our purposes, it suffices to define

$$k_j := \text{nullity}(\delta_j) - \text{rank}(\delta_{j-1}). \tag{27}$$

Here, nullity is the dimension of the kernal, denoted $\ker(\delta_j)$, which is the space of vectors u such that $\delta_j u = 0$. The rank is the number of linearly independent rows in a matrix. Alternatively, the rank is equal to the dimension of the image, denoted $\text{im}(\delta_{j-1})$, which is the space of vectors v such that there exists a u satisfying $v = \delta_{j-1} u$. Those familiar with homology theory may prefer to think of k_j as the dimension of the j^{th} homology group $H_j = \ker(\delta_j)/\text{im}(\delta_{j-1})$. This counts the number of different homology classes at a particular level of the chain complex. Let c be an element of C_j. If $c \in \ker(\delta_j)$ then we say c is a cycle. However, for any $c \in \text{im}(\delta_{j-1})$ it immediately follows from $\delta_j \delta_{j-1} = 0$ that also $c \in \ker(\delta_j)$ and such a cycle is said to be a trivial

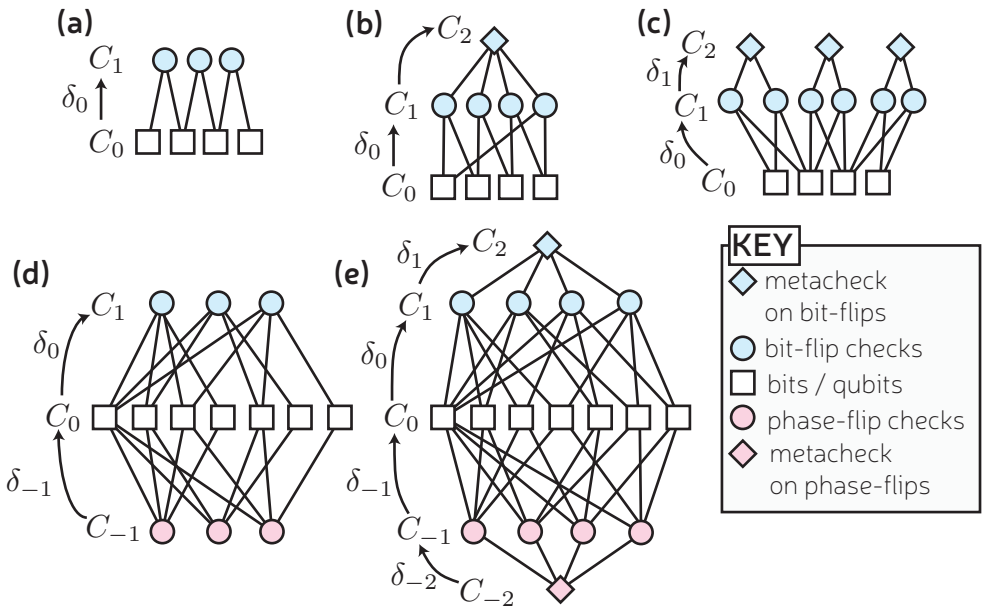

FIG. 1: A graphical representation of some example classical and quantum error correcting codes, including scheme for parity check measurements and metachecks. (a) the 4 bit classical repetition code; (b) the 4 bit classical repetition code with an additional check and corresponding metachecks; (c) the 4 bit classical repetition code with an repeated checks and corresponding metachecks; (d) the 7-qubit Steane code; (e) the 7-qubit Steane code with additional checks and corresponding metachecks. The symbol δ_j is a matrix describing the connectivity between vertices in set C_j and C_{j+1}. It can also be considered as a linear map known as the boundary map in homology theory.

cycle. On the other hand, if $c \in \ker(\delta_j)$ but $c \notin \mathrm{im}(\delta_{j-1})$ then c is a non-trivial cycle. If any non-trivial cycles exist then $k_j > 0$, and the value of k_j counts the number of different non-trivial cycles (factoring out homological equivalence). Note that for k_j with the lowest value of j in the chain complex, the matrix δ_{j-1} is not defined and so Eq. (27) should be read with δ_{j-1} substituted by the zero matrix. Similarly, for the largest possible j value we must take δ_j as the zero matrix.

One can similarly look at the cohomologies

$$k_j^T := \mathrm{nullity}(\delta_{j-1}^T) - \mathrm{rank}(\delta_j^T). \tag{28}$$

Poincaré duality entails that $k_j^T = k_j$ and for completeness we give a simple proof in App. A using only linear algebra. For quantum codes, k_0 is important as it gives the number of logical qubits encoded by the code. It is useful for us to also to consider k_j for other values of j. For instance, in a code with metachecks, k_1 is the number of classes of syndromes x such that they pass all the metachecks ($\delta_1 x = 0$) but there does not exist an explanation in terms of qubit errors ($\nexists e$ such that $x = \delta_0 e$).

In the context of error correction, we are interested not just in the number of non-trivial cycles, but also their minimum distance. As such, we define

$$\begin{aligned} d_j &:= \min\{|c| : c \in \ker(\delta_j), c \notin \mathrm{im}(\delta_{j-1})\}, \\ d_j^T &:= \min\{|c| : c \in \ker(\delta_j^T), c \notin \mathrm{im}(\delta_{j+1}^T)\}, \end{aligned} \tag{29}$$

where $|c| := \sum_j c_j$ is the Hamming weight. We use the convention that $d_j = \infty$ whenever $k_j = 0$ and similarly for d_j^T. We know of no simple relationship between d_j and d_j^T. This is enough for us to define the usual parameters of the corresponding $[[n, k, d_Q]]$ quantum code as $n = n_0$, $k = k_0$ and $d_Q = \min[d_0, d_{-1}^T]$. However, we also introduce a new parameter that we call the single-shot distance as follows.

Definition 5 (Single shot distance) *Given a length-4 chain complex we define the single-shot distance as* $d_{ss} := \min[d_1, d_{-2}^T]$ *where* d_1 *and* d_{-2}^T *are special cases of Eq.* (29).

The single-shot distance relates to how many measurement errors can be tolerated before a failure occurs that we call a metacheck failure. In a metacheck failure, the syndrome has no explanation in terms of qubit errors. See Fig. 2b4 for an example of metacheck failure in the 2D Ising model with periodic boundary conditions.

Let us review different ways we can use this formalism. Consider a length-1 chain complex $C_0 \to_{\delta_0} C_1$. We can consider the vertices in the zeroth level as bits and the first level as parity checks. Thus a length-1 chain complex can be regarded as a classical code. Consider a length-2 chain complex $C_{-1} \to_{\delta_{-1}} C_0 \to_{\delta_0} C_1$. This could represent either a quantum code (without any metachecks) or alternatively a classical code equipped with metachecks. In the classical case, our convention is to increment all the indices by one to have $C_0 \to_{\delta_0} C_1 \to_{\delta_1} C_2$. We

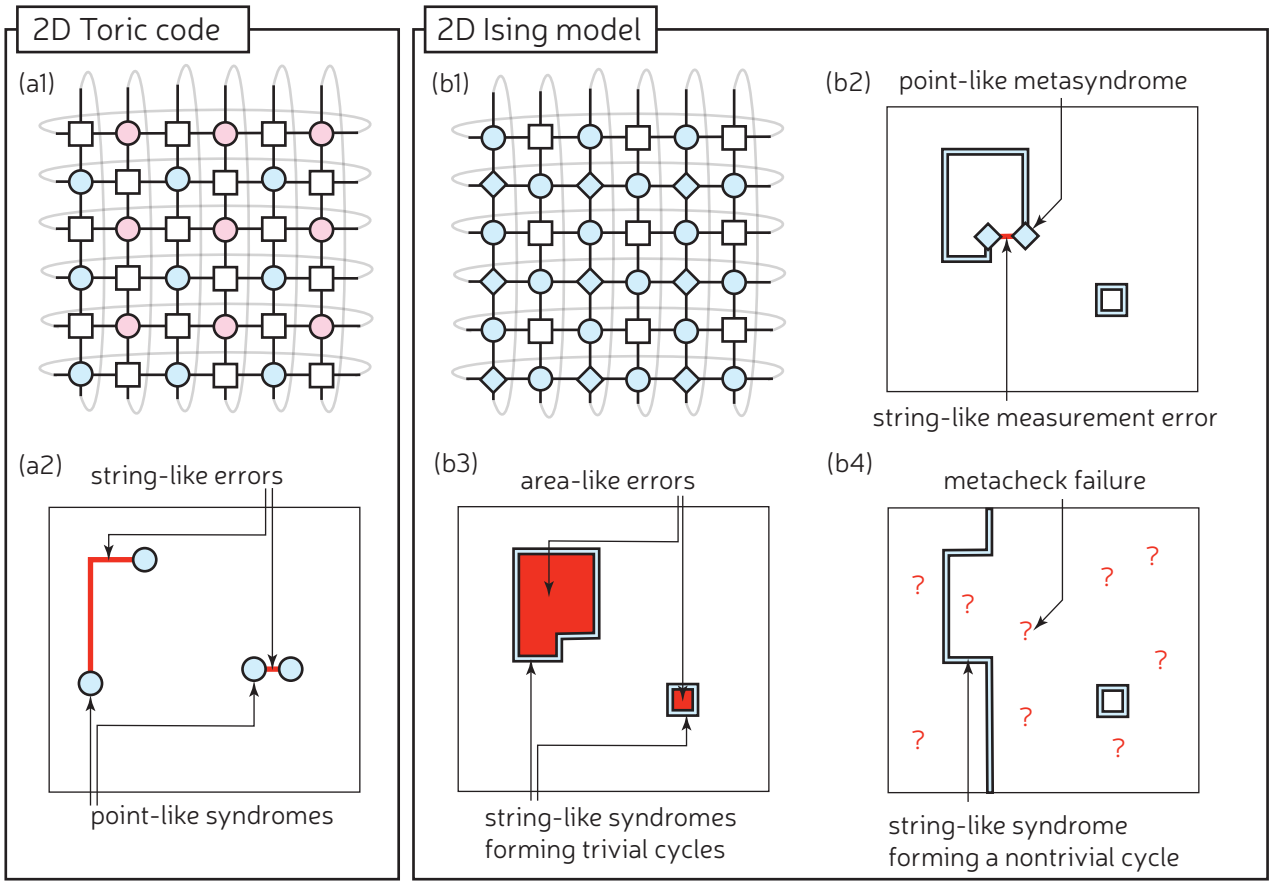

FIG. 2: In (a) we illustrate the 2D toric code. Part (a1) describes the toric code using the vertex labelling from Fig. 1 with grey curved lines highlighting the periodic boundary conditions of the torus. Part (a2) shows the relationship between error and syndromes. Notice that a weight 2 syndrome (two endpoints) could require an arbitrarily long string to produce the syndrome. Therefore, the code does not have good soundness. In (b) we illustrate the 2D Ising model as a classical error correction code. Part (b1) again uses the vertex labelling from Fig. 1. Notice that (b1) represents the same graph as (a1) but with the different types of vertex changing role. Part (b2) shows a measurement error that is detected by metachecks. Part (b3) shows a measurement syndrome that passes all metachecks (i.e. it would be the corrected syndrome of (b2)). The red region shows an error pattern that generates the syndrome. Notice that the size of the physical error scales at most quadratically with the size of the syndrome. Therefore, the code does have good soundness. Part (b4) show a metacheck failure. There is a syndrome that spans the code and forms a non-trivial cycle. Due to periodic boundary conditions there is no error region with this syndrome as its boundary.

choose this convention such that C_0 always labels the physical bits or qubits. In Fig. 2a1 and Fig. 2b1 we show two graphs representing length-2 chain complexes. The graphs are identical except in Fig. 2a1 it represents a quantum code and in Fig. 2b1 it represents a classical code with metachecks.

Given a length-4 chain complex, the additional layers of homology describe metachecks on the X and Z checks. Note that the additional layers of the chain complex have no direct effect on the code parameters.

We could also consider length-3 chain complexes with metachecks on either X and Z checks. It is also plausible that a length-3 chain complex could support single-shot error correction of both error types by using a form of gauge fixing such has been proposed in 3D colour codes [1]. However, we will not explore this here.

We also need to translate the notion of soundness into the language of chain complexes

Definition 6 (Soundness of maps) *Let t be an integer and $f : \mathbb{Z} \to \mathbb{R}$ be some function called the soundness function. Given a linear map δ, we say it is (t, f)-sound if for all r such that $|\delta r| \leq t$, it follows that:*

$$x \leq |\delta r| \implies \min\{|r'| : \forall r' \text{ s.t. } \delta r' = \delta r\} \leq f(x). \quad (30)$$

Furthermore, we say a quantum error correcting code is (t, f)-sound if the above holds for both δ_0 and δ_{-1}^T. For a classical error correcting code this is required for just δ_0.

We saw earlier than 2D topological codes cannot have good soundness and we illustrate this in Fig. 21b. Whereas, for the 4D toric code, with an appropriate

choice of checks, geometric arguments show that low weight syndromes can always be generated by small weight errors. To visualise this, it is easier to instead think of the 2D Ising model as a classical error correcting code. In such a code, syndrome cycles have a weight equal to their perimeter and the error generating the syndrome has weight equal to the area (see Fig. 2b3). The area of a 2D region can be no more than $x^2/4$ of the perimeter length x and so the Ising model has a quadratic soundness function. Therefore, it can be helpful to think of soundness as describing the geometric area law relationship between syndromes and errors, albeit in purely algebraic terms.

Check redundancy provides consistency conditions that one can inspect for evidence of measurement errors. These checks on checks are illustrated in Fig. 1 using diamonds. We call these metachecks. They do not represent a physical measurement but classical postprocessing on the measurement outcomes. That is, for a given metacheck node we calculate the parity of all the checks it is connected to. If this parity is odd, a measurement error must have occurred on one of the adjacent nodes. Recall that we quantify the amount of redundancy in a measurement scheme as the ratio between the number of measurements performed (which equals $n_1 + n_{-1}$) and the minimum number required to generate the stabiliser of the code (which equals $n_0 - k_0$). We use υ to denote this ratio, so that

$$\upsilon = \frac{n_1 + n_{-1}}{n_0 - k_0}, \tag{31}$$

with $\upsilon = 1$ indicating no redundancy. In Fig. 1 we give examples of codes with such redundancy (Fig. 1b, Fig. 1c and Fig. 1c). We are interested in code families where υ is no more than a small constant factor.

VII. CONSTRUCTING SINGLE SHOT CODES CODES

Here we show how the homological product can be used to construct new codes supporting single-shot error correction. This will culminate in a proof of Thm. 4 though the techniques allow for a broader range of constructions, including codes where the single-shot distance is finite.

A. A single application constructions

As a warm-up, we begin by considering a single application of the homological product. Our approach is to take a length-1 chain complex (e.g. a conventional classical code) and use the homological, or hypergraph, product to build a length-2 chain complex with the desired properties. In general, one could take two different input classical codes and combine them together using these techniques, but for simplicity we take both input codes to be the same. Furthermore, there are a few different notions of the homological product. For instance, Bravyi and Hastings use a simplified variant that they call the single sector homological product, whereas we will use a more standard textbook variant that Bravyi and Hastings would call a multi sector homological product [19]. Furthermore, there is some freedom in the notation and we use a convention such that the homological product in this section is manifestly equivalent to the hypergraph product of Tillich and Zemor [16].

Given a chain complex $C_0 \to_{\delta_0} C_1$ we can define a new chain complex $\tilde{C}_{-1} \to_{\tilde{\delta}_{-1}} \tilde{C}_0 \to_{\tilde{\delta}_0} \tilde{C}_1$ of the form

$$C_0 \otimes C_1 \to_{\tilde{\delta}_{-1}} (C_0 \otimes C_0) \oplus (C_1 \otimes C_1) \to_{\tilde{\delta}_0} C_1 \otimes C_0. \tag{32}$$

The notation $\otimes$ represents the tensor product. For example, if $a \in C_0$ and $b \in C_1$ then $a \otimes b \in C_0 \otimes C_1$, and the space $C_0 \otimes C_1$ further contains any linear combinations of such vectors. The symbol $\oplus$ represents a direct product. For instance, vectors in $(C_0 \otimes C_0) \oplus (C_1 \otimes C_1)$ can be written as $w = u \oplus v$ where $u \in (C_0 \otimes C_0)$ and $v \in (C_1 \otimes C_1)$. All vectors should be read as column vectors and so the direct product of vectors can also be read as stacking these vectors

$$u \oplus v = \begin{pmatrix} u \\ v \end{pmatrix}. \tag{33}$$

We will use the weight identities $|u \otimes v| = |u| \cdot |v|$ and $|u \oplus v| = |u| + |v|$. The boundary map $\tilde{\delta}_{-1}$ is defined such that for product vectors $a \otimes b \in C_0 \otimes C_1$, we have

$$\tilde{\delta}_{-1}(a \otimes b) = (a \otimes (\delta_0^T b)) \oplus ((\delta_0 a) \otimes b), \tag{34}$$

and it extends linearly to non-product vectors. This is often more concisely denoted as $\tilde{\delta}_{-1} = (\mathbb{1} \otimes \delta_0^T) \oplus (\delta_0 \otimes \mathbb{1})$. The boundary map $\tilde{\delta}_0$ is defined such that for product vectors $a \otimes b \in C_0 \otimes C_0$ and $c \otimes d \in C_1 \otimes C_1$, we have

$$\tilde{\delta}_0((a \otimes b) \oplus (c \otimes d)) = ((\delta_0 a) \otimes b) + (c \otimes (\delta_0^T d)), \tag{35}$$

and again extending linearly to non-product vectors. Both the new boundary maps can also be represented in block matrix form

$$\tilde{\delta}_{-1} = \begin{pmatrix} \mathbb{1} \otimes \delta_0^T \\ \delta_0 \otimes \mathbb{1} \end{pmatrix}, \tag{36}$$
$$\tilde{\delta}_0 = \begin{pmatrix} \delta_0 \otimes \mathbb{1} & \mathbb{1} \otimes \delta_0^T \end{pmatrix}.$$

From here it is easy to verify that they satisfy the requirement that $\tilde{\delta}_0 \tilde{\delta}_{-1} = 2(\delta_0 \otimes \delta_0^T) = 0$, where we have used that all mathematics is being performed modulo 2. These matrices fully characterise the new chain complex and from them we can find graphs of the sort shown in Fig. 1. We give a graphical overview in Fig. 3.

Now we discuss the parameters of this new structure, with some of these results obtained in Ref. [16]. Simple dimension counting tells us that the new chain complex has

$$\begin{aligned} \tilde{n}_{-1} &= n_0 n_1, \\ \tilde{n}_0 &= n_0^2 + n_1^2, \\ \tilde{n}_1 &= n_0 n_1. \end{aligned} \tag{37}$$

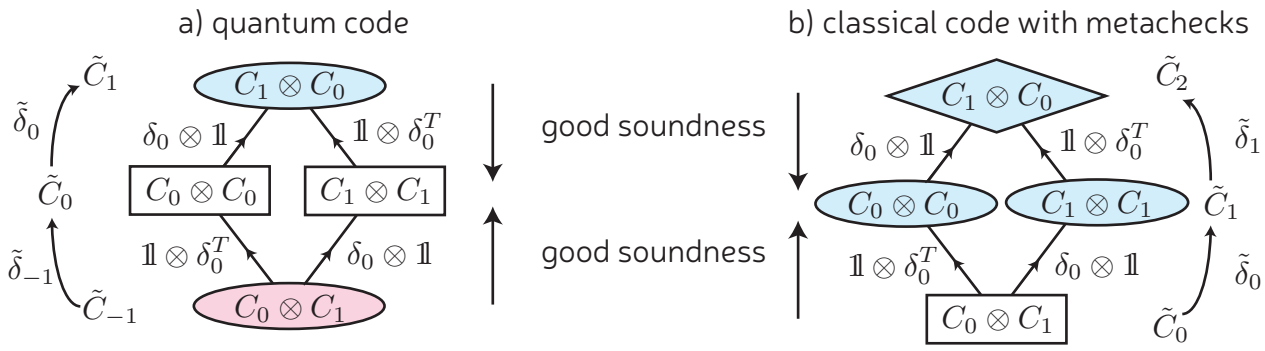

FIG. 3: An overview of a single application of the homological product to generate a length-2 chain complex from a length-1 chain complex (that can be viewed as a classical code). In (a) we label the chain-complex under the assumption that it defines a quantum code, and where the subscripts are consistent with the main text. In (a) we label the chain-complex under the assumption that it defines a classical code. In order that $\tilde{C}_0$ denotes the bits, we have increments all the new subscripts by 1. Throughout we use rectangles to show a collection of bit/qubit vertices; we use ovals to show a collection of checks; and diamonds to show a collect of metachecks.

The dimension of the homological classes is more involved, but a well known result from homology theory (the Künneth formula [19, 29]) tells us that

$$\begin{aligned} \tilde{k}_{-1} &= k_0 k_1, \\ \tilde{k}_0 &= k_0^2 + k_1^2, \\ \tilde{k}_1 &= k_1 k_0. \end{aligned} \tag{38}$$

The distance of the code is trickier yet again to prove and is not a standard quantity in homology theory. Nevertheless, one can show that

$$\tilde{d}_{-1} = d_0 d_0^T, \tag{39}$$

$$\tilde{d}_0^T = d_0 d_0^T, \tag{40}$$

$$\tilde{d}_0 \geq \min(d_0, d_0^T), \tag{41}$$

$$\tilde{d}_{-1}^T \geq \min(d_0, d_0^T). \tag{42}$$

We provide proofs in App. C for Eq. (39) and Eq. (40). The results of Eq. (41) and Eq. (42) were shown by Tillich and Zemor [16] but we give an independent proof in the homological formalism in App. C.

Here we instead focus on the following lemma

Lemma 5 (First soundness lemma) *Let $C_0 \to_{\delta_0} C_1$ be a chain complex. Applying the above homological product we obtain a new chain complex where the map $\tilde{\delta}_0^T$ is (d_0, f)-sound and $\tilde{\delta}_{-1}$ is (d_0^T, f)-sound with $f(x) = x^2/4$.*

We make no assumptions about the soundness properties of the original chain complex but find this emerges due to the nature of the homological product. However, if one knows that the original chain complex is sound, one could prove a stronger soundness result (with f growing slower than $x^2/4$) for the new chain complex. We prove this lemma in App. D and next discuss its implications.

Using the above homological product, we can construct a quantum code with parameters $[[\tilde{n}_0, \tilde{k}_0, d_Q]]$ where $d_Q = \min[\tilde{d}_0^T, \tilde{d}_0]$. These codes will not necessarily support single-shot error corrections because the soundness property in Lem. 5 is not the property required by Thm. 1, which requires that $\tilde{\delta}_0$ and $\tilde{\delta}_{-1}^T$ have good soundness properties.

Why prove Lem. 5 if it is does not directly provide quantum codes with single-shot capabilities? First, in the next section we will make a second application of the homological product and Lem. 5 will be used, and so it is a stepping stone result. Second, Lem. 5 is highly instructive as it gives a way to construct classical codes that exhibit single-shot error correction. Let us explore this second point further. Just like a quantum code, a classical code with metachecks needs three layers of structure (recall Fig. 1). Also, our convention is that the subscript 0 in C_0 always denotes the bits or qubits. So for a classical code with metachecks, we want a chain complex of the form $\tilde{C}_0 \to_{\tilde{\delta}_0} \tilde{C}_1 \to_{\tilde{\delta}_1} \tilde{C}_2$. We can use the chain complex generated by the homological product by simply increasing all the subscripts by 1. With these incremented subscripts, Lem. 5 tells us that $\tilde{\delta}_0$ is (d_0^T, f)-sound with $f(x) = x^2/4$. It is easy to get lost in subscripts, so we emphasize that the important feature is that soundness runs in the direction from bits/qubits to checks. This is illustrated in Fig. 3 where it clearly runs the correct way for the classical code but not the quantum code. For instance, the 2D toric code and 2D Ising code can both be obtained by applying the homological product to a classical repetition code, but only the 2D Ising code exhibits good soundness (recall Fig. 2).

Next, we comment on the redundancy of the new quantum code.

Claim 2 (Updated redundancy) *Let $C_0 \to_{\delta_0} C_1$ be a chain complex associated with an $[[n, k, d]]$ classical code with check redundancy $\upsilon = n_1/(n_0 - k_0)$. Applying the above homological product we obtain a new chain complex*

and associated quantum code with check redundancy

$$\tilde{\upsilon} = \upsilon \frac{n}{\upsilon(n-k)+k} < 2\upsilon. \tag{43}$$

Notice that if $\upsilon = 1$ *then* $\tilde{\upsilon} = 1$.

To prove this, we begin with the definition of redundancy and apply Eqs. (37) and Eqs. (38)

$$\tilde{\upsilon} = \frac{\tilde{n}_1 + \tilde{n}_{-1}}{\tilde{n}_0 - \tilde{k}_0} \tag{44}$$

$$= \frac{2n_0 n_1}{n_0^2 + n_1^2 - k_0^2 - k_1^2} \tag{45}$$

$$= \frac{2n_0 n_1}{(n_0-k_0)(n_0+k_0)+(n_1-k_1)(n_1+k_1)}. \tag{46}$$

Using that for a length-1 chain complex $n_1 - k_1 = n_0 - k_0$ and the definition of υ, we find

$$\tilde{\upsilon} = \frac{2n_0 n_1}{(n_0-k_0)(n_0+k_0+n_1+k_1)} \tag{47}$$

$$= 2\upsilon \frac{n_0}{n_0+k_0+n_1+k_1}.$$

Since the fraction is clearly less than 1, we have that $\tilde{\upsilon} < 2\upsilon$. Furthermore, using $n_1 - k_1 = n_0 - k_0$ to eliminate k_1 and $\upsilon = n_1/(n_0 - k_0)$ to eliminate n_1, we obtain

$$\tilde{\upsilon} = \upsilon \frac{n_0}{\upsilon(n_0-k_0)+k_0}, \tag{48}$$

and the identification $n = n_0$ and $k = k_0$ gives the final expression for $\tilde{\upsilon}$.

We conclude this section by considering a simple application of the above homological product. Given a classical $[n, k, d]$ code, we can associate many different length-1 chain complexes, depending on whether there is redundancy in the check operators. However, for any code there always exists a minimal chain complex where there is no redundancy ($\upsilon = 1$). For such a minimal chain complex, we have $n_1 = n - k$, $k_1 = 0$ and $d_0^T = \infty$. This is useful as it allows us to make statements that depend only on well known code properties.

Corollary 3 (Quantum code constructions) *Consider a classical* $[n, k, d]$ *code. Applying the above homological product to the minimal chain complex of this code, we obtain a* $[[2n(n-k), k^2, d]]$ *quantum code with no check redundancy.*

B. A second application of the homological product

For a quantum error correcting code with metachecks we need a length-4 chain complex, which can be constructed by applying the homological product to a length-2 chain complex. We use breve ornaments over symbols in this section to identify matrices, variables and vector spaces associated with the length-4 chain complex, as follows

$$\breve{C}_{-2} \to_{\breve{\delta}_{-2}} \breve{C}_{-1} \to_{\breve{\delta}_{-1}} \breve{C}_0 \to_{\breve{\delta}_0} \breve{C}_1 \to_{\breve{\delta}_1} \breve{C}_2. \tag{49}$$

The homological product between a pair of 2-dimensional chain complexes will generate a length-4 chain complex according to the general rule that

$$\breve{C}_m = \bigoplus_{i-j=m} \tilde{C}_i \otimes \tilde{C}_j. \tag{50}$$

The boundary maps are illustrated in Fig. 4 and can be written as block matrices as follows

$$\breve{\delta}_{-2} = \begin{pmatrix} \mathbb{1} \otimes \tilde{\delta}_0^T \\ \tilde{\delta}_{-1} \otimes \mathbb{1} \end{pmatrix}, \tag{51}$$

$$\breve{\delta}_{-1} = \begin{pmatrix} \mathbb{1} \otimes \tilde{\delta}_{-1}^T & 0 \\ \tilde{\delta}_{-1} \otimes \mathbb{1} & \mathbb{1} \otimes \tilde{\delta}_0^T \\ 0 & \tilde{\delta}_0 \otimes \mathbb{1} \end{pmatrix}, \tag{52}$$

$$\breve{\delta}_0 = \begin{pmatrix} \tilde{\delta}_{-1} \otimes \mathbb{1} & \mathbb{1} \otimes \delta_{-1}^T & 0 \\ 0 & \tilde{\delta}_0 \otimes \mathbb{1} & \mathbb{1} \otimes \tilde{\delta}_0^T \end{pmatrix}, \tag{53}$$

$$\breve{\delta}_1 = \begin{pmatrix} \tilde{\delta}_0 \otimes \mathbb{1} & \mathbb{1} \otimes \delta_{-1}^T \end{pmatrix}. \tag{54}$$

One can verify that $\breve{\delta}_{j+1}\breve{\delta}_j = 0$ for all j follows from the same condition on the $\tilde{\delta}$ matrices. As before, one obtains the relations

$$\breve{n}_m = \sum_{i-j=m} \tilde{n}_i \tilde{n}_j, \tag{55}$$

$$\breve{k}_m = \sum_{i-j=m} \tilde{k}_i \tilde{k}_j,$$

where the first is simple dimension counting and the second line follows from the Künneth formula.

The distances are lower bounded as follows

$$\breve{d}_0, \breve{d}_{-1}^T \geq \min[\tilde{d}_{-1}, \max[\tilde{d}_0, \tilde{d}_{-1}^T], \tilde{d}_0^T], \tag{56}$$

$$\breve{d}_1, \breve{d}_{-2}^T \geq \min[\tilde{d}_0, \tilde{d}_{-1}^T],$$

which we prove in App. E. Note that the distance will often be significantly larger than these lower bounds. Our main technical goal is to prove the following soundness result.

Lemma 6 (Second soundness lemma) *Let* $\tilde{C}_{-1} \to_{\tilde{\delta}_{-1}} \tilde{C}_0 \to_{\tilde{\delta}_0} \tilde{C}_1$ *be a chain complex such that* $\tilde{\delta}_0^T$ *is* (t, f)*-sound and* $\tilde{\delta}_{-1}$ *is* (t, f)*-sound with* $f(x) = x^2/4$. *Applying the above homological product we obtain a new length-4 chain complex (as in Eq. 49) where the map* $\breve{\delta}_0$ *is* (t, g)*-sound and* $\breve{\delta}_{-1}^T$ *is* (t, g)*-sound with soundness function* $g(x) = x^3/4$.

We show the direction of the resulting soundness in Fig. 4 and this should be contrasted with the direction of the soundness arrows in Fig. 3. We will only prove the results for $\breve{\delta}_0$ with the proof for $\breve{\delta}_{-1}^T$ being essentially identical.

Let us first discuss how the problem can be divided into three subproblems. Let $s \in \text{im}(\breve{\delta}_0)$ so there must exist at least one $r \in \breve{C}_0$ such that $\breve{\delta}_0 r = s$. We divide r into components

$$r = \begin{pmatrix} r_a \\ r_b \\ r_c \end{pmatrix}, \tag{57}$$

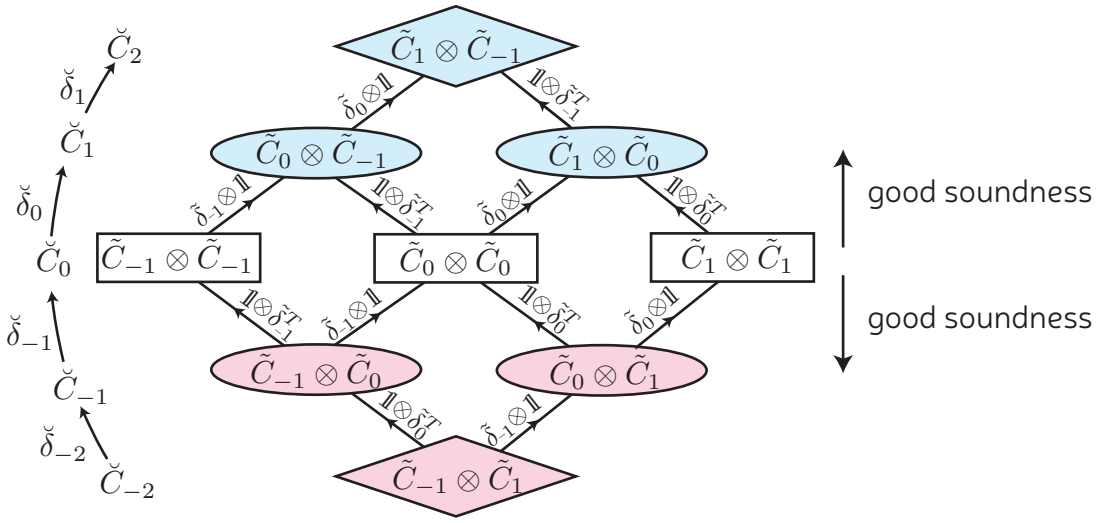

FIG. 4: An overview of the second application of the homological product to generate a length-4 chain complex from a two dimensional chain complex (that can be viewed as a quantum code).

and consider two distinct images

$$s_L = (\tilde{\delta}_{-1} \otimes \mathbb{1}) r_a + (\mathbb{1} \otimes \tilde{\delta}_{-1}^T) r_b, \tag{58}$$

$$s_R = (\mathbb{1} \otimes \tilde{\delta}_0^T) r_c + (\tilde{\delta}_0 \otimes \mathbb{1}) r_b, \tag{59}$$

where

$$\breve{\delta}_0 r = \begin{pmatrix} s_L \\ s_R \end{pmatrix}. \tag{60}$$

One always has the weight relations $|r| = |r_a| + |r_b| + |r_b|$ and $|s| = |s_L| + |s_R|$.

For a syndrome that passes all metachecks we have that

$$\breve{\delta}_1 s = (\tilde{\delta}_0 \otimes \mathbb{1}) s_L + (\mathbb{1} \otimes \tilde{\delta}_{-1}^T) s_R = 0, \tag{61}$$

which entails that

$$m := (\tilde{\delta}_0 \otimes \mathbb{1}) s_L = (\mathbb{1} \otimes \tilde{\delta}_{-1}^T) s_R, \tag{62}$$

where we have defined this new quantity to be m. Given a physical error pattern r that generates the syndrome (as in Eqs. (58)-(59)) the metachecks are always passed and one finds that

$$m = (\tilde{\delta}_0 \otimes \tilde{\delta}_{-1}^T) r_b. \tag{63}$$

It is interesting that this depends only on the r_b component of r. We can first try to find low weight r_b that solves Eq. (63). This leads to the following partial solution to the problem

Lemma 7 (Partial soundness result) *Let $\tilde{C}_{-1} \to_{\tilde{\delta}_{-1}} \tilde{C}_0 \to_{\tilde{\delta}_0} \tilde{C}_1$ be a chain complex. Applying the above homological product we obtain a new length-4 chain complex (as in Eq. 49) with the following property. For any $s \in \mathrm{im}(\breve{\delta}_0)$ there exists an r_b with the following properties*

1. *correctness: $(\tilde{\delta}_0 \otimes \tilde{\delta}_{-1}^T) r_b = m = (\tilde{\delta}_0 \otimes \mathbb{1}) s_L = (\mathbb{1} \otimes \tilde{\delta}_{-1}^T) s_R$;*
2. *low weight: $|r_b| \leq |s_L| \cdot |s_R|$;*
3. *small s_L remainder: $s_L - (\mathbb{1} \otimes \tilde{\delta}_{-1}^T) r_b = \sum_i \alpha_i \otimes \hat{a}_i$ where $\hat{a}_i$ are unit vectors and $\alpha_i \in \ker \tilde{\delta}_0$. There are at most $|s_L|$ nonzero α_i and these are bounded in size $|\alpha_i| \leq |s_L|$;*
4. *small s_R remainder: $s_R - (\tilde{\delta}_0 \otimes \mathbb{1}) r_b = \sum_i \hat{b}_i \otimes \beta_i$ where $\hat{b}_i$ are unit vectors and $\beta_i \in \ker \tilde{\delta}_{-1}^T$. There are at most $|s_R|$ nonzero β_i and these are bounded in size $|\beta_i| \leq |s_R|$.*

The proof has a similar flavour to the earlier soundness result and is deferred until App. F. Notice that the lemma does not require any soundness of the initial chain complex. Next, we want to find low-weight r_a and r_c such that they provide the remaining elements of the syndrome as follows

$$(\tilde{\delta}_{-1} \otimes \mathbb{1}) r_a = s_L - (\mathbb{1} \otimes \tilde{\delta}_{-1}^T) r_b, \tag{64}$$

$$(\mathbb{1} \otimes \tilde{\delta}_0^T) r_c = s_R - (\tilde{\delta}_0 \otimes \mathbb{1}) r_b. \tag{65}$$

Fortunately, Lem. 7 ensures that these remainder syndromes are "small" in the defined sense. We may next use the following observation

Claim 3 (Inheritance of soundness) *If $\tilde{\delta}_{-1}$ is (t, f)-sound then $\tilde{\delta}_{-1} \otimes \mathbb{1}$ is also sound in the following strong sense. Let $q \in \mathrm{im}(\tilde{\delta}_{-1} \otimes \mathbb{1})$ with decomposition $q = \sum_i \alpha_i \otimes \hat{a}_i$ such that $|\alpha_i| \leq t$ then there exists an r_a such that $(\tilde{\delta}_{-1} \otimes \mathbb{1}) r_a = q$ and $|r_a| = \sum_i f(|\alpha_i|)$. A similar result holds when we interchange the order of tensor products and consider $\tilde{\delta}_0^T$.*

The proof is fairly straightforward. Since $|\alpha_i| \leq t$ for all i and by assumption $\tilde{\delta}_{-1}$ is (t, f)-sound, there must exist γ_i such that $\tilde{\delta}_{-1}\gamma_i = \alpha_i$ and $|\gamma_i| \leq f(|\alpha_i|)$. By linearity, there exists $r_a = \sum_i \gamma_i \otimes \hat{a}_i$ such that $(\tilde{\delta}_{-1} \otimes \mathbb{1})r_a = q$ and $|r_a| = \sum_i |\gamma_i| \leq \sum_i f(|\alpha_i|)$.

Next, we put these pieces together. Combining Lem. 3 and Claim. 3 together with the assumption that $|s| \leq t$ one immediately obtains that there exist r_a and r_c solving Eq. (64) with weights upper bounded by

$$|r_a| \leq |s_L| f(|s_L|) \tag{66}$$
$$|r_c| \leq |s_R| f(|s_R|) \tag{67}$$

Therefore, we have the total weight

$$|r| \leq |s_L| f(|s_L|) + |s_L| \cdot |s_R| + |s_R| f(|s_R|). \tag{68}$$

We take $f(x) = x^2/4$ as stated in Thm. 6, which leads to

$$|r| \leq \frac{1}{4}|s_L|^3 + |s_L| \cdot |s_R| + \frac{1}{4}|s_R|^3 \tag{69}$$
$$\leq \frac{1}{4}(|s_L| + |s_R|)^3 \tag{70}$$
$$= \frac{1}{4}|s|^3. \tag{71}$$

Therefore, we have proven (t, g)-sound of $\breve{\delta}_0$ with $g(x) = x^3/4$. This completes the proof that Thm. 6 follows from Lem. 7.

Next, we comment on the check redundancy of these codes

Claim 4 (Updated redundancy part 2) *Consider a length-2 chain complex and associated quantum code with check redundancy $\tilde{\upsilon}$. Applying the above homological product we obtain a length-4 chain complex and new quantum code with check redundancy $\breve{\upsilon} < 2\tilde{\upsilon}$.*

To prove this we recall the definition of redundancy and then use Eqs. (55) to obtain

$$\breve{\upsilon} = \frac{\breve{n}_1 + \breve{n}_{-1}}{\breve{n}_0 - \breve{k}_0} \tag{72}$$
$$= \frac{2\tilde{n}_0\tilde{n}_1}{(\tilde{n}_{-1}^2 + \tilde{n}_0^2 + \tilde{n}_1^2) - (\tilde{k}_{-1}^2 + \tilde{k}_0^2 + \tilde{k}_1^2)}. \tag{73}$$

Since $\tilde{n}_j \geq \tilde{k}_j$ for all j, the denominator is greater than $\tilde{n}_0^2 - \tilde{k}_0^2$, which itself can be factorised as $(\tilde{n}_0 - \tilde{k}_0)(\tilde{n}_0 + \tilde{k}_0)$ and so

$$\breve{\upsilon} \leq \frac{2\tilde{n}_0\tilde{n}_1}{(\tilde{n}_0 - \tilde{k}_0)(\tilde{n}_0 + \tilde{k}_0)}, \tag{74}$$
$$= 2\tilde{\upsilon}\frac{\tilde{n}_0}{\left(\tilde{n}_0 + \tilde{k}_0\right)}, \tag{75}$$

Last, we use the loose bound that the fraction is less than 1.

C. Combining homological products

Here we combine the results of the preceding two subsections. Parameters carrying a breve are first expressed in term of parameters carrying a tilde, and then the tilde parameters are replaced with unornamented parameters.

$$\breve{n}_0 = \tilde{n}_1^2 + \tilde{n}_0^2 + \tilde{n}_{-1}^2 = (n_0^2 + n_1^2)^2 + 2n_0^2 n_1^2, \tag{76}$$
$$\breve{n}_1 = \breve{n}_{-1} = \tilde{n}_0(\tilde{n}_1 + \tilde{n}_{-1}) = 2(n_0^2 + n_1^2)n_0 n_1,$$
$$\breve{k}_0 = \tilde{k}_1^2 + \tilde{k}_0^2 + \tilde{k}_{-1}^2 = (k_0^2 + k_1^2)^2 + 2k_0^2 k_1^2,$$
$$\breve{k}_1 = \breve{k}_{-1} = \tilde{k}_0(\tilde{k}_1 + \tilde{k}_{-1}) = 2(k_0^2 + k_1^2)k_0 k_1,$$
$$\breve{d}_0 = \breve{d}_{-1}^T \geq \min[d_0, d_0^T],$$
$$\breve{d}_1 = \breve{d}_{-1}^T \geq \min[d_0, d_0^T].$$

Furthermore, by combining Claim. 2 and Claim. 4 we obtain an upper bound on the check redundancy

$$\breve{\upsilon} < 2\tilde{\upsilon} = 2\upsilon\frac{n}{\upsilon(n-k)+k}, \tag{77}$$

where υ is the check redundancy of the $[[n, k, d]]$ classical code associated with the initial length-1 chain complex.

The simplest case is when we use a minimal chain complex representing the initial $[[n, k, d]]$ classical code. Then $\upsilon = 1$, $k_1 = 0$ and $n_1 = n - k$ and the above equations simplify to

$$\breve{n}_0 = n^4 + 4n^2(n-k)^2 + (n-k)^4, \tag{78}$$
$$\breve{n}_1 = \breve{n}_{-1} = 2n(n-k)(n^2 + (n-k)^2),$$
$$\breve{k}_0 = k^4,$$
$$\breve{k}_1 = \breve{k}_{-1} = 0$$
$$\breve{\upsilon} < 2.$$
$$\breve{d}_0 = \breve{d}_{-1}^T \geq d,$$

We also know that $\breve{d}_1 = \breve{d}_{-1}^T = \infty$ as a consequence of $\breve{k}_1 = \breve{k}_{-1} = 0$. We make the following identifications: $\breve{n}_0$ gives the number of physical qubits n_Q; $\breve{k}_0$ is the number of logical qubits k_Q; $\breve{d}_0$ and $\breve{d}_{-1}$ give the qubit error distance d_Q; and $\breve{d}_1$ and $\breve{d}_{-1}^T$ give the single shot distance d_{ss}. This proves Thm. 4.

In Table I we provide some concrete examples. These are the smallest examples since they use very small initial classical codes. Though the resulting quantum code is much larger. The first three examples correspond to 4D toric codes with cubic tilling either with closed boundary conditions (examples 1 and 2) or periodic boundary conditions (example 3). The last example corresponds to no previous codes that we know of. We have deliberately chosen codes that have low check weight as these will be the most experimentally feasible. How useful these codes are will depend on their exact code distance, which currently have a large range of possible values. Our constructions could potentially be slightly improved using a generalisation of the hypergraph improvements analogous to use of rotated toric lattices [30].

Input classical code						Double homological product code						
	parameters			max. check	redundancy	parameters				max. check	mean check	redundancy
δ	n	k	d	weight	υ	n_Q	k_Q	d_Q	d_{ss}	weight	weight	$\check{\upsilon}$
$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$	3	1	3	2	1	241	1	$3 \leq d_Q \leq 9$	∞	6	4.87179	1.3
$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$	4	1	4	2	1	913	1	$4 \leq d_Q \leq 16$	∞	6	5.18	1.31579
$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$	3	1	3	2	1.5	486	6	$3 \leq d_Q \leq 9$	3	6	6	1.33884
$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$	6	2	4	3	1	3856	16	$4 \leq d_Q \leq 16$	∞	8	5.48077	1.3

TABLE I: Some example small classical codes used to generate a quantum code with good soundness through a double application of the homological product. Many of the parameters come directly from equations in the main text. The mean check weight and redundancy are calculated exactly by constructing the explicit parity check matrices. We only have lower and upper bounds on the code distance as this is more difficult to numerically evaluate.

VIII. DISCUSSION & CONCLUSIONS

This is a paper of two halves. The first half was conceptual and gave a presentation of single-shot error correction. We found an intimate connection between single-shot error correction and a property called good soundness. We saw that good soundness in LDPC codes entails a macroscopic energy barrier, which further confirms a relationship between passive quantum memories and single-shot error correction. However, our results leave open whether there exist any codes with a macroscopic energy barrier that lack good soundness. Michael Beverland suggested in discussion that it would be interesting to look at whether Haah's cubic code [31, 32] has good soundness. The Haah cubic code is notable because it does have a macroscopic energy barrier but is not a good passive quantum memory at all scales due to entropic effects. Also curious is the role of metachecks and redundancy. We saw that good soundness can be achieved by any code without any check redundancy, but the proof used a diagonlised form of the stabiliser generators that typically destroys any LDPC properties.

The second half of this paper was more technical and focused on specific code constructions capable of providing both good soundness and LDPC properties. It has long been known that homology theory provides a natural mathematical framework for CCS codes, but we saw that homology theory is especially useful when metachecks (checks on measurements) are added to the picture. It is well known that for topological codes the energy barrier and single shot error correction are intimately related to the dimensionality of the code. We abstract away the topological structure and instead work with algebraic homological structure. While these codes no longer have a dimensionality in the geometric sense, we saw that using the homological product can imbued codes with a sort of effective dimensionality. More precisely, a double application of the homological product resulted in single-shot properties similar to 4-dimensional topological codes. Many readers will feel more comfortable with topological codes because of the conceptual and visual crutches they provide. However, topological codes are significantly limited in terms of the code parameters they can achieve due to trade-off bounds [21, 22]. So by freeing ourselves from the constraints of topological codes and pursuing their more abstract cousins, we can seemingly benefit from many of the advantages of high-dimensional topological codes (e.g. single-shot error correction) but with improved code parameters. This prompts the question what other topological code properties might hold for homological product codes. We know that 3D and 4D topological code can support transversal non-Clifford gates [33–39], which suggests that a similar property might hold for suitably defined homological product codes.

Our code constructions married good soundness and LDPC properties, through the use of check redundancy and associated metachecks. But do any codes exist without check redundancy that have good soundness and LDPC properties. A excellent candidate are the quantum expander codes since they are LDPC codes that can perform single-shot error correction [5]. Indeed, they must either have good soundness or they support single-shot error correction through a different mechanism from that discussed in this paper. Ref. [5] is very recent so the jury is still out on how it relates to our work. Nevertheless, we can speculate. Recall that quantum expander codes are constructed using a single application of the hypergraph or homological product. A single application is not always sufficient to provide good soundness (the 2D toric

code is a counterexample). But quantum expander codes use classical codes with strong graph expansion properties and it is plausible, and we conjecture, that these expansion properties lead to good soundness.

The main limitation of this work is that we restrict our attention to adversarial noise. Stochastic noise models instead distribute errors according to some probability distribution and assign a non-zero probability to every error configuration. If the probability of a high weight error is low, then we can still leverage proofs from the adversarial noise setting. However, in an independent noise model where each qubit is affected with probability p, a code with n qubits will typically suffer around pn errors. For code families, the distance scales sublinearly, and so there is some scale at which the code is likely to suffer an error considerable larger than the code distance. Nevertheless, one is often able to prove the existence of an error correcting threshold. The crucial point is that even though some errors of weight pn might not be correctable, these represent a small fraction of all weight pn errors and so happen with small probability. At this point, proof techniques diverge. We can prove that this works for concatenated codes, topological codes and low-density parity check codes [40]. As such, while there is a single theoretical framework for adversarial noise, there is no single theory for stochastic noise in all settings. The situation is likely the same in the setting of single-shot error correction. The pioneering work of Bombin demonstrated that three dimensional colour codes can perform single-shot error correction against a stochastic noise model [1], and so in this sense our results are strictly weaker. On the other hand, our approach is strictly more general as it applies to a broad range of codes, including many new code constructions such as those presented here. It is then natural to wonder what are sufficient and necessary conditions for single-shot error correction to work against stochastic noise? It is reasonable to conjecture that any concatenated or LDPC that meets our criteria for adversarial noise will also perform single shot error correction against stochastic noise.

Acknowledgements.- This work was supported by the EPSRC (EP/M024261/1) and the QCDA project which has received funding from the QuantERA ERA-NET Cofund in Quantum Technologies implemented within the European Union's Horizon 2020 Programme. I would like to thank Nicolas Delfosse for his tutorial on hypergraph product codes during the FTQT 2016 workshop at the Centro de Ciencias de Benasque Pedro Pascual. Thank you to Simon Willerton, Michael Beverland, Mike Vasmer, Anthony Leverrier, Barbara Terhal and Ben Brown for conservations and comments on the manuscript.

[1] H. Bombín, Phys. Rev. X **5**, 031043 (2015).
[2] H. Bombín, Phys. Rev. X **6**, 041034 (2016).
[3] H. Bombín, New Journal of Physics **17**, 083002 (2015).
[4] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, Journal of Mathematical Physics **43**, 4452 (2002).
[5] A. L. Omar Fawzi, Antoine Grospellier, in prep.
[6] Y. Fujiwara, Phys. Rev. A **90**, 062304 (2014).
[7] A. Ashikhmin, C.-Y. Lai, and T. A. Brun, in *Information Theory (ISIT), 2016 IEEE International Symposium on* (IEEE, 2016), pp. 2274–2278.
[8] B. J. Brown, N. H. Nickerson, and D. E. Browne, Nat Commun **7** (2016).
[9] N. P. Breuckmann, K. Duivenvoorden, D. Michels, and B. M. Terhal, Quant. Inf. and Comp. **17**, 0181 (2017).
[10] D. Aharonov and L. Eldar, SIAM Journal on Computing **44**, 1230 (2015).
[11] M. B. Hastings, in *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)* (2017), vol. 67 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pp. 25:1–25:26.
[12] R. Alicki, M. Horodecki, P. Horodecki, and R. Horodecki, Open Systems & Information Dynamics **17**, 1 (2010).
[13] B. M. Terhal, Rev. Mod. Phys. **87**, 307 (2015).
[14] B. J. Brown, D. Loss, J. K. Pachos, C. N. Self, and J. R. Wootton, Rev. Mod. Phys. **88**, 045005 (2016).
[15] D. Bacon, Phys. Rev. A **73**, 012340 (2006).
[16] J.-P. Tillich and G. Zémor, IEEE Transactions on Information Theory **60**, 1193 (2014).
[17] A. Leverrier, J.-P. Tillich, and G. Zémor, in *Foundations of Computer Science (FOCS), 2015 IEEE 56th Annual Symposium on* (IEEE, 2015), pp. 810–824.
[18] A. Grospellier, A. Leverrier, and O. Fawzi, in *Journées codage et cryptographie 2017* (2017).
[19] S. Bravyi and M. B. Hastings, in *Proceedings of the forty-sixth annual ACM symposium on Theory of computing* (ACM, 2014), pp. 273–282.
[20] B. Audoux and A. Couvreur, arXiv preprint arXiv:1512.07081 (2015).
[21] S. Bravyi, D. Poulin, and B. Terhal, Phys. Rev. Lett. **104**, 050503 (2010).
[22] N. Delfosse, in *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on* (IEEE, 2013), pp. 917–921.
[23] N. P. Breuckmann, Ph.D. thesis, Aachen, arXiv preprint arXiv:1802.01520 (2018).
[24] S. Bravyi and B. Terhal, New Journal of Physics **11**, 043029 (2009).
[25] J. W. Harrington, Ph.D. thesis (2004), `http://thesis.library.caltech.edu/1747/1/jimh_thesis.pdf`.
[26] M. Herold, E. T. Campbell, J. Eisert, and M. J. Kastoryano, npj Quantum Information **1**, 15010 (2015).
[27] M. Herold, M. J. Kastoryano, E. T. Campbell, and J. Eisert, New Journal of Physics **19**, 063012 (2017).
[28] E. T. Campbell and D. E. Browne, Phys. Rev. Lett. **104**, 030503 (2010).
[29] A. Hatcher, Cambridge UP, Cambridge **606** (2002).
[30] A. A. Kovalev and L. P. Pryadko, in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on* (IEEE, 2012), pp. 348–352.
[31] J. Haah, Phys. Rev. A **83**, 042330 (2011).
[32] S. Bravyi and J. Haah, Phys. Rev. Lett. **111**, 200501 (2013).

[33] H. Bombin and M. A. Martin-Delgado, Phys. Rev. Lett. **97**, 180501 (2006).
[34] H. Bombin, R. Chhajlany, M. Horodecki, and M. Martin-Delgado, New Journal of Physics **15**, 055023 (2013).
[35] F. H. Watson, E. T. Campbell, H. Anwar, and D. E. Browne, Phys. Rev. A **92**, 022312 (2015).
[36] A. Kubica, B. Yoshida, and F. Pastawski, New Journal of Physics **17**, 083026 (2015).
[37] A. Kubica and M. E. Beverland, Phys. Rev. A **91**, 032330 (2015).
[38] M. Vasmer and D. E. Browne, arXiv preprint arXiv:1801.04255 (2018).
[39] E. T. Campbell, B. M. Terhal, and C. Vuillot, Nature **549**, 172 (2017).
[40] A. A. Kovalev and L. P. Pryadko, Phys. Rev. A **87**, 020304 (2013).

Appendix A: A simple proof of relation between Betti numbers

We give a simple proof that $k_j = k_j^T$ as defined in Eq. (27) and Eq. (28). The proof uses simple linear algebra rather than sophisticated homological techniques that are needed in more exotic settings. We use the rank-nullity theorem that for any matrix A,

$$\text{rank}(A) + \text{nullity}(A) = n, \tag{A1}$$

where n is the number of columns in A. This entails that

$$\text{rank}(\delta_j) + \text{nullity}(\delta_j) = n_j, \tag{A2}$$

$$\text{rank}(\delta_{j-1}^T) + \text{nullity}(\delta_{j-1}^T) = n_j. \tag{A3}$$

Taking the definition of k_j^T (recall Eq. (28)) and using Eq. (A3) to eliminate the dependence on $\text{nullity}(\delta_{j-1}^T)$, we obtain

$$k_j^T = n_j - \text{rank}(\delta_{j-1}^T) - \text{rank}(\delta_j^T). \tag{A4}$$

Using that for any matrix $\text{rank}(A) = \text{rank}(A^T)$, we deduce

$$k_j^T = n_j - \text{rank}(\delta_{j-1}) - \text{rank}(\delta_j). \tag{A5}$$

Using Eq. (A2) to eliminate $\text{rank}(\delta_j)$, we get

$$\begin{aligned} k_j^T &= n_j - \text{rank}(\delta_{j-1}) - [n_j - \text{nullity}(\delta_j)] \\ &= \text{nullity}(\delta_j) - \text{rank}(\delta_{j-1}), \end{aligned} \tag{A6}$$

which is precisely the definition of k_j given in Eq. (27). This completes this simple but educational proof.

Appendix B: Further notation

1. Vector reshaping

Throughout the appendices we often reshape vectors into matrices to present proofs. If we have a vector v belonging to some tensor product space $A \otimes B$, then we can reshape v into a matrix V. We always use lower-case symbols for vectors and upper-case for the resulting matrix after reshaping. Let $\{\hat{a}_i\}$ and $\{\hat{b}_j\}$ be unit basis vectors for A and B, respectively. Then any vector v can be decomposed in this basis as

$$v = \sum_{i,j} V_{i,j} \hat{a}_i \otimes \hat{b}_j, \tag{B1}$$

where the coefficients $V_{i,j}$ are elements of the matrix representation. That is, $V_{i,j}$ is the entry in the i^{th} row and j^{th} column of matrix V. Furthermore, given matrices $M : A \to A$ and $N : B \to B$ we will rewrite equations as follows

$$(M \otimes N)v \to MVN^T, \tag{B2}$$

which is easily verified.

2. Matrix support

We further introduce the notion of column and row support. Given any matrix X we let $\text{colsupp}(X)$ denote the set of columns in X with at least one nonzero entry. Given any matrix X we let $\text{rowsupp}(X)$ denote the set of rows in X with at least one nonzero entry. We shall often use $|\dots|$ to denote the number of rows or columns within some support. That is, $|\text{colsupp}(X)|$ is the number of columns in X with at least one nonzero entry.

Appendix C: Distance bounds: part one

Here we give proofs of distances associated with length-2 chain complexes constructed using the homological product (see Eqs. (39)-(42)).

1. First bound

We begin by showing that $\tilde{d}_{-1} \geq d_0 d_0^T$. The quantity $\tilde{d}_{-1}$ is the weight of the smallest nonzero vector $r \in C_0 \otimes C_1$ such that $\tilde{\delta}_{-1} r = 0$. We use that $r \in C_0 \otimes C_1$ can be reshaped into a matrix R; see B 1 for discussion of reshaping. The condition $\tilde{\delta}_{-1} r$ entails that every column of R must be in $\ker(\delta_0)$ and every row of R must be in $\ker(\delta_0^T)$. Assuming, R is nonzero, there must be at least one non-zero column. Since this column has weight at least d_0, it follows that there are at least d_0 non-zero rows. Each of these rows has weight at least d_0^T. Therefore, the total weight is at least $d_0 d_0^T$ as required. Next, we show $\tilde{d}_{-1} \leq d_0 d_0^T$. We assume, $d_0 \neq \infty$ and $d_0^T \neq \infty$ otherwise the inequality is trivially true. Let α be a minimal weight non-zero vector in the kernal of δ_0, so $|\alpha| = d_0$. Similarly let $\beta \in \ker(\delta_0^T)$ with $|\beta| = d_0^T$. Then $\alpha \otimes \beta \in C_0 \otimes C_1$ has $|\alpha \otimes \beta| = d_0 d_0^T$ and is easily verified to satisfy $\tilde{\delta}_{-1}(\alpha \otimes \beta) = 0$. The proof of $\tilde{d}_0^T = d_0 d_0^T$ follows by symmetry.

2. Second bound

Next we show that $\tilde{d}_0 \geq \min[d_0, d_0^T]$. Recall, this is the weight of the smallest vector r such that $\tilde{\delta}_0 r = 0$ and $r \notin \mathrm{im}(\tilde{\delta}_{-1})$. All r can be decomposed as

$$r = \begin{pmatrix} r_a \\ r_b \end{pmatrix}, \tag{C1}$$

where $\tilde{\delta}_0 r = 0$ entails that $(\delta_0 \otimes \mathbb{1}) r_a = (\mathbb{1} \otimes \delta_0^T) r_b$. Assuming r is a non-trivial cycle, it follows that there must exist a cocycle $w = (w_a, w_b)$ such that $w^T r = 1$. Therefore, $w_a^T r_a + w_b^T r_b = 1$ and either $w_a^T r_a = 1$ or $w_b^T r_b = 1$. We proceed assuming $w_a^T r_a = 1$ and further note that the cocycle can always be assumed to have the form $w = (e \otimes f) \oplus 0$. This is a good place to remind the reader that $\oplus$ is the direct product and when applied to columns vectors means that we stack the columns. Since w ought to be a cocycle it must satisfy $\tilde{\delta}_{-1}^T w = 0$ which entails that $\delta_0 f = 0$. The relation $w^T r = 1$ then becomes $(e^T \otimes f^T) r_a = 1$. We can reshape some vectors into matrices, and these equations become

$$(e^T \otimes f^T) r_a = 1 \implies e^T R_a f = 1 \tag{C2}$$

$$(\delta_0 \otimes \mathbb{1}) r_a = (\mathbb{1} \otimes \delta_0^T) r_b \implies \delta_0 R_a = R_b \delta_0 \tag{C3}$$

We consider the vector $R_a f$. From $\delta_0 R_a = R_b \delta_0$ we infer that $\delta_0 (R_a f) = R_b \delta_0 f$. Using also that $\delta_0 f = 0$ we have a proof that $\delta_0 (R_a f) = 0$ and so $R_a f \in \ker(\delta_0)$. However, $R_a f \neq 0$ otherwise it would be impossible to satisfy $e^T R_a f = 1$. It follows that $d_0 \leq |R_a f|$. Since $R_a f$ is formed from linear combinations of columns from R_a, we have $|R_a f| \leq |R_a|$ and hence $d_0 \leq |R_a|$. It follows that $d_0 \leq |r|$ in this case. For the $w_b^T r_b = 1$ case, a similar argument follows but giving a lower bound of $d_0^T \leq |r|$. Therefore, the actual lower bound on $|r|$ is the minimum of these two cases.

Appendix D: Coexpansion proof: part one

Here we prove Lem. 5 for $\tilde{\delta}_0^T$, with the $\tilde{\delta}_{-1}$ proof following a similar fashion. Recalling the definition of soundness, we consider $s \in \tilde{C}_0$ and assume $|s| < d_0^T$ and $s \in \mathrm{im}(\delta_0^T)$. There must exist at least one $r \in \tilde{C}_1 = C_1 \otimes C_0$ such that $s = \tilde{\delta}_0^T r$. This will not be the only possible solution, but let us begin by exploring the relationship between $|s|$ and $|r|$.

The vector s has two components $s = s_L \oplus s_R$ and breaking $s = \tilde{\delta}_0^T r$ into components, we have

$$\begin{aligned} s_L &= (\delta_0^T \otimes \mathbb{1}) r, \\ s_R &= (\mathbb{1} \otimes \delta_0) r. \end{aligned} \tag{D1}$$

Next, we reshape r, s_L and s_R into matrices (see B 1 for discussion of reshaping) so that

$$\begin{aligned} s_L = (\delta_0^T \otimes \mathbb{1}) r \to S_L = \delta_0^T R, \\ s_R = (\mathbb{1} \otimes \delta_0) r \to S_R = R \delta_0^T. \end{aligned} \tag{D2}$$

In terms of support (recall notation of App. B 2) the above equations entail that

$$\begin{aligned} \mathrm{colsupp}(S_L) \subseteq \mathrm{colsupp}(R), \\ \mathrm{rowsupp}(S_R) \subseteq \mathrm{rowsupp}(R). \end{aligned} \tag{D3}$$

In general, this means that

$$|\mathrm{colsupp}(S_L)| \leq |\mathrm{colsupp}(R)|, \tag{D4}$$

$$|\mathrm{rowsupp}(S_R)| \leq |\mathrm{rowsupp}(R)|. \tag{D5}$$

Since $|\mathrm{colsupp}(X)| \leq |X|$ and $|\mathrm{rowsupp}(X)| \leq |X|$ for any X, equality in the above relations entails that

$$\begin{aligned} |S_L| \geq |\mathrm{colsupp}(S_L)|, \\ |S_R| \geq |\mathrm{rowsupp}(S_R)|, \end{aligned} \tag{D6}$$

and since $|s| = |S| = |S_L| + |S_R|$ we have

$$|s| \geq |\mathrm{colsupp}(S_L)| + |\mathrm{rowsupp}(S_R)|. \tag{D7}$$

Squaring both sides and using $(a+b)^2/4 \geq ab$ for integer a and b, we obtain

$$|s|^2/4 \geq |\mathrm{colsupp}(S_L)| \cdot |\mathrm{rowsupp}(S_R)|. \tag{D8}$$

We would like to substitute in Eqs. (D4)-(D5) but the inequality signs do not align correctly. We would be able to proceed if Eqs. (D4)-(D5) held with strict equality, but this is not always the case.

To proceed we use that the above R is not the only possible solution. Given an initial R we can transform to obtain a new R so that Eqs. (D2) are preserved, but so that also Eq. (D4) and Eq. (D5) become equalities. In particular, given a pair of vectors $a \in \ker \delta_0^T$ and $b \in \ker \delta_0^T$ we can perform $R \to R + ab^T$ and Eqs. (D2) will be preserved. We assume for now that neither Eq. (D4) nor Eq. (D5) are strict equalities, and so we may take both a and b^T to be column and row vectors from R. It follows that the new $R + ab^T$ has column and row support strictly contained within that of R, and the support may even reduce in size. Notice that adding ab^T will add a to every column in R on which b^T is supported. So if the support of a and b^T intersect in R, we can strictly decreased the number of columns or rows in R. Repeating this process must terminate when one (or more) of the following conditions holds

(i) Eq. (D4) is a strict equality;

(ii) Eq. (D5) is a strict equality;

(iii) Neither Eq. (D4) nor Eq. (D5) is a strict equality, but there are no column/row pairs with the appropriate intersection.

The last condition is easier to illustrate using a block matrix equation. It asserts that R has the form

$$R = \begin{pmatrix} 0 & W & 0 \\ A & S & 0 \\ 0 & 0 & 0 \end{pmatrix}, \tag{D9}$$

where we have taken the liberty of permuting columns and rows, such that: the columns in $\ker(\delta_0^T)$ run through blocks W and S; the row vectors (transposed) in $\ker(\delta_0^T)$ run through blocks A and S. Actually, this block matrix describes all three cases if we allow A and W to be zero matrices. That is, case (i) is equivalent to $A = 0$ and case (ii) is equivalent to $W = 0$.

Having transformed into this special form, we next use additional assumptions under which A and W blocks vanish and so Eq. (D4) and Eq. (D5) become strict equalities. We use our assumption that $|s| < d_0^T$ and Eq. (D7) to conclude that

$$d_0^T > |\text{colsupp}(S_L)| + |\text{rowsupp}(S_R)|. \tag{D10}$$

Consider a column vector intersecting subblock A. The weight of this vector is less than $|\text{colsupp}(S)|$ and so less than d_0^T. However, we also know this vector is a non-zero vector in the kernal of the map δ_0^T, but all these vectors have weighted of d_0^T or greater. Therefore, we have a contradiction that is only resolved if $A = 0$, and similarly running this argument for row vectors we conclude $W = 0$. Therefore, we see that the above transformation must yield a form with where Eqs. (D4)-(D5) hold with strict equality. This can be combined with Eq. (D8) to conclude that

$$|s|^2/4 \geq |\text{colsupp}(R)| \cdot |\text{rowsupp}(R)|. \tag{D11}$$

Furthermore, if R is supported on a submatrix of size $|\text{colsupp}(R)|$ by $|\text{rowsupp}(R)|$ then the size of this submatrix gives an upper bound on $|R| = |r|$ so that

$$|\text{colsupp}(R)| \cdot |\text{rowsupp}(R)| \geq |r|. \tag{D12}$$

Combining Eq. (D11) and Eq. (D12) produces the desired bound $|s|^2/4 \geq |r|$.

Appendix E: Distance bounds: part two

Here we prove Eqs. (56).

1. First bound

We begin with

$$\breve{d}_0 \geq \min[\tilde{d}_{-1}, \max[\tilde{d}_0, \tilde{d}_{-1}^T], \tilde{d}_0^T] \tag{E1}$$

and remark that the proof for $\breve{d}_{-1}^T$ will follow a similar fashion. Recall that $\breve{d}_0$ is the weight of the smallest vector r such that $\breve{\delta}_0 r = 0$ and $r \notin \text{im}(\breve{\delta}_{-1})$. All r can be decomposed as

$$r = \begin{pmatrix} r_a \\ r_b \\ r_c \end{pmatrix}, \tag{E2}$$

where $\breve{\delta}_0 r = 0$ requires that

$$\begin{aligned} (\mathbb{1} \otimes \tilde{\delta}_{-1}^T) r_b &= (\tilde{\delta}_{-1} \otimes \mathbb{1}) r_a, \\ (\tilde{\delta}_0 \otimes \mathbb{1}) r_b &= (\mathbb{1} \otimes \tilde{\delta}_0^T) r_c. \end{aligned} \tag{E3}$$

Taking the components of r and reshaping into a matrices, the vector equations transform into matrix equations as follows

$$(\tilde{\delta}_0 \otimes \mathbb{1}) r_b = (\mathbb{1} \otimes \tilde{\delta}_0^T) r_c \implies \tilde{\delta}_0 R_b = R_c \tilde{\delta}_0, \tag{E4}$$

$$(\mathbb{1} \otimes \tilde{\delta}_{-1}^T) r_b = (\tilde{\delta}_{-1} \otimes \mathbb{1}) r_a 0 \implies R_b \tilde{\delta}_{-1} = \tilde{\delta}_{-1} R_a. \tag{E5}$$

Assuming r is a non-trivial cycle, it follows that there must exist a nontrivial cocycle $w = (w_a, w_b, w_c)$ such that $w^T r = 1$. Furthermore, the cocycle can be assumed to be of the form $w = (e_a \otimes f_a, e_b \otimes f_b, e_c \otimes f_c)$ since the span of such vectors encompasses all nontrivial cocycles.

Therefore, $w_a^T r_a + w_b^T r_b + w_c^T r_c = 1$ and at least one of these terms must equal 1 and there are four cases to consider

1. $w_a^T r_a = 1$ and $w_b^T r_b = w_c^T r_c = 0$, in which case we may assume $w = (e_a \otimes f_a) \oplus 0 \oplus 0$;
2. $w_c^T r_c = 1$ and $w_a^T r_a = w_b^T r_b = 0$, in which case we may assume $w = 0 \oplus 0 \oplus (e_c \otimes f_c)$;
3. $w_b^T r_b = 1$ and $w_a^T r_a = w_c^T r_c = 0$, in which case we may assume $w = 0 \oplus (e_b \otimes f_b) \oplus 0$;
4. $w_a^T r_a = w_b^T r_b = w_c^T r_c = 1$; in which case we can find a new w satisfying one of the above 3 cases.

We again remind the reader that all vectors are column vectors. Furthermore, $\oplus$ is the direct product and when applied to columns vectors means that we stack the columns.

We first consider case 1. For $w = (e_a \otimes f_a) \oplus 0 \oplus 0$ to be a cocycle requires that $\tilde{\delta}_{-1} f_a = 0$. Furthermore, the condition $w^T r = (e_a^T \otimes f_a^T) r_a = 1$ in reshaped form becomes $e_a^T R_a f_a = 1$. We consider the vector $R_a f_a$, and find

$$\tilde{\delta}_{-1} R_a f_a = R_b \tilde{\delta}_{-1} f_a = 0, \tag{E6}$$

where we have used Eq. (E5) and $\tilde{\delta}_{-1} f_a = 0$. In other words, $R_a f_a \in \ker(\tilde{\delta}_{-1})$. However, $R_a f_a$ is non-zero otherwise it would be impossible to satisfy $e_a^T R_a f_a = 1$. It follows that $\tilde{d}_{-1} \leq |R_a f_a|$. Since $R_a f_a$ is formed from linear combinations of columns from R_a, we have $|R_a f_a| \leq |R_a|$ and hence $\tilde{d}_{-1} \leq |R_a|$. It follows that $\tilde{d}_{-1} \leq |r|$ in case 1.

Next, we consider case 2. The proof method is essentially the same but we repeat for completeness. For $w = 0 \oplus 0 \oplus (e_c \otimes f_c)$ to be a cocycle requires that $\tilde{\delta}_0^T e_c = 0$. Furthermore, the condition $w^T r = (e_c^T \otimes f_c^T) r_c = 1$ in reshaped form becomes $e_c^T R_c f_c = 1$. We consider the vector $R_c^T e_c$, and find

$$\tilde{\delta}_0^T R_c^T e_c = (R_c \tilde{\delta}_0)^T e_c = (\tilde{\delta}_0 R_b)^T e_c = R_b^T \tilde{\delta}_0^T e_c = 0, \tag{E7}$$

where we have used Eq. (E4) and $\tilde{\delta}_0^T e_c = 0$. In other words, $R_c^T e_c \in \ker(\tilde{\delta}_0^T)$. However, $R_c^T e_c$ is non-zero otherwise it would be impossible to satisfy $e_c^T R_c f_c = 1$. It follows that $\tilde{d}_0^T \leq |R_c^T e_c|$. Since $R_c^T e_c$ is formed from linear combinations of rows from R_c, we have $|R_c^T e_c| \leq |R_c|$ and hence $\tilde{d}_0^T \leq |R_c|$. It follows that $\tilde{d}_0^T \leq |r|$ in case 2.

Next, we consider case 3 then $w = 0 \oplus (e_b \otimes f_b) \oplus 0$. Furthermore, the condition $w^T r = (e_b^T \otimes f_b^T) r_b = 1$ in reshaped form becomes $e_b^T R_b f_b = 1$. The proof is slightly different from the above two cases. The cocycle conditions now tells us that both $\tilde{\delta}_{-1}^T e_b = 0$ and $\tilde{\delta}_0 f_b = 0$. We have

$$\tilde{\delta}_0 R_b f_b = R_c \tilde{\delta}_0 f_b = 0, \tag{E8}$$

$$\tilde{\delta}_{-1}^T R_b^T e_b = (R_b \tilde{\delta}_{-1})^T e_b = (\tilde{\delta}_{-1} R_a)^T e_b = R_a^T \tilde{\delta}_{-1}^T e_b = 0, \tag{E9}$$

where we have used $\tilde{\delta}_0 f_b = 0$ and $\tilde{\delta}_{-1}^T e_b = 0$ as asserted earlier. Furthermore, $R_b f_b \notin \mathrm{im}(\tilde{\delta}_{-1})$ since otherwise $R_b f_b = \tilde{\delta}_{-1} u$ for some u and then $e_b^T R_b f_b = e_b^T \tilde{\delta}_{-1} u = (\tilde{\delta}_{-1}^T e_b)^T u$. However, since $\tilde{\delta}_{-1}^T e_b = 0$ this would entail $e_b^T R_b f_b = 0$ which is a contradiction and so we must have $R_b f_b \notin \mathrm{im}(\tilde{\delta}_{-1})$. Similarly, one has that $R_b^T e_b \notin \mathrm{im}(\tilde{\delta}_0^T)$ otherwise $R_b^T e_b = \tilde{\delta}_{-1} v$ for some v which would again lead to the contradiction $e_b^T R_b f_b = 0$ when combined with the fact that $\tilde{\delta}_0 f_b = 0$. Combining $R_b f_b \in \ker(\tilde{\delta}_0)$ and $R_b f_b \notin \mathrm{im}(\tilde{\delta}_{-1})$ entails that $R_b f_b$ is a nontrivial cycle and so $\tilde{d}_0 \leq |R_b f_b|$. Since $R_b f_b$ is formed from linear combinations of columns from R_b, we have $|R_b f_b| \leq |R_b|$ and hence $\tilde{d}_0 \leq |R_b|$. Similarly, combining $R_b^T e_b \in \ker(\tilde{\delta}_{-1}^T)$ and $R_b^T e_b \notin \mathrm{im}(\tilde{\delta}_0^T)$ leads to $\tilde{d}_{-1}^T \leq |R_b|$. This suffices to prove that in case 3 we have $|r| \geq \max[\tilde{d}_0, \tilde{d}_{-1}^T]$.

Since any one of the three cases may hold, we must take the minimum over the three cases. This yields the distance lower bound on $\breve{d}_0$.

2. Second bound

Here we prove

$$\breve{d}_1 \geq \min[\tilde{d}_0, \tilde{d}_{-1}^T], \tag{E10}$$

and remark that the proof for $\breve{d}_{-2}^T$ will follow a similar fashion. Let $s = s_a \oplus s_b \in \breve{C}_1$ be a minimal distance nontrivial cycle for $\breve{\delta}_1$. From $\breve{\delta}_1 s = 0$ we may infer

$$(\tilde{\delta}_0 \otimes \mathbb{1}) s_a = (\mathbb{1} \otimes \tilde{\delta}_{-1}^T) s_b. \tag{E11}$$

Since s is a nontrivial cycle, there must exist a nontrivial cocycle $w = w_a \oplus w_b$ such that $w^T s = 1$. There are two possible cases

1. $w_a^T s_a = 1$ and $w_b^T s_b = 0$, in which case we may assume $w = (e_a \otimes f_a) \oplus 0$;
2. $w_b^T s_b = 1$ and $w_a^T s_a = 0$, in which case we may assume $w = 0 \oplus (e_b \otimes f_b)$;

For case 1, since w is a cocycle $\breve{\delta}_1^T w = 0$ and so both $\tilde{\delta}_{-1}^T e_a = 0$ and $\tilde{\delta}_{-1} f_a = 0$. However, $e_a \notin \mathrm{im}(\tilde{\delta}_0)$ otherwise w would be a trivial cocycle. As in other proofs, we now reshape into matrix equations

$$w^T s = 1 \implies e_a^T S_a f_a = 1 \tag{E12}$$

$$(\tilde{\delta}_0 \otimes \mathbb{1}) s_a = (\mathbb{1} \otimes \tilde{\delta}_{-1}^T) s_b \implies \tilde{\delta}_0 S_a = S_b \tilde{\delta}_{-1}. \tag{E13}$$

Therefore,

$$\tilde{\delta}_0 (S_a f_a) = S_b \tilde{\delta}_{-1} f_a = 0 \tag{E14}$$

where we have used Eq. (E13) and $\tilde{\delta}_{-1} f_a = 0$. In other words, $S_a f_a \in \ker(\tilde{\delta}_0)$. However, $S_a f_a \notin \mathrm{im}(\tilde{\delta}_{-1})$ otherwise there would exist a u such that $S_a f_a = \tilde{\delta}_{-1} u$ and then $e_a^T S_a f_a = e_a^T \tilde{\delta}_{-1} u = 0$ by virtue of $\tilde{\delta}_{-1}^T e_a = 0$. This is in contradiction with Eq. (E12) and so $S_a f_a$ is a nontrivial cycle of $\tilde{\delta}_0$ and must satisfy $\tilde{d}_0 \leq |S_a f_s|$. It follows that $\tilde{d}_0 \leq |S_a| \leq |s|$.

For case 2, a similar proof entails that $\tilde{d}_{-1}^T \leq |S_b| \leq |s|$. Since either case may hold the distance is given by the minimum of these two quantities.

Appendix F: Partial soundness

Here we prove Lem. 7, which is a major technical component of Thm. 7. We are working towards a low-weight solution of

$$m = (\tilde{\delta}_0 \otimes \tilde{\delta}_{-1}^T) r_b. \tag{F1}$$

So far we only know that there must be at least one r_b satisfying this equation. We proceed by looking for other r_b consistent with Eq. (F1) that have a low weight and other additional properties. At this point it is convenient to reshape our vectors into matrices (recall App. B 1) and the previous equations become

$$S_L = \tilde{\delta}_{-1} R_a + R_b \tilde{\delta}_{-1}, \tag{F2}$$

$$S_R = \tilde{\delta}_0 R_b + R_c \tilde{\delta}_0, \tag{F3}$$

$$M = \tilde{\delta}_0 S_L = S_R \tilde{\delta}_{-1} = \tilde{\delta}_0 R_b . \tilde{\delta}_{-1}. \tag{F4}$$

If R_b has any columns in the kernal of $\tilde{\delta}_0$, these can be removed without changing M. Similarly, if R_b has any rows in the kernal of $\tilde{\delta}_{-1}^T$, these can be removed without changing M.

Simple matrix algebra (recall notation from App. B 2) then leads to the inclusions

$$\mathrm{rowsupp}(R_b \tilde{\delta}_{-1}) \subseteq \mathrm{rowsupp}(R_b), \tag{F5}$$

$$\mathrm{colsupp}(\tilde{\delta}_0 R_b) \subseteq \mathrm{colsupp}(R_b), \tag{F6}$$

$$\mathrm{colsupp}(M) \subseteq \mathrm{colsupp}(S_L), \tag{F7}$$

$$\mathrm{rowsupp}(M) \subseteq \mathrm{rowsupp}(S_R). \tag{F8}$$

Next, we describe how we may transform R_b while preserving M. Given a vector c such that $\tilde{\delta}_0 c = 0$, we may

add c to any of the columns in R_b and M will not change. Furthermore, if colsupp(R_b) intersects with colsupp(c) then we can perform a transformation that removes one row from R_b. Specifically, let v be a row vector of R_b that is one of the rows from colsupp$(R_b) \cap$ colsupp(c). Then the transform $R_b \to R_b' = R_b + cv^T$ satisfies the following

1. the transform will preserve M;
2. the new R_b' will have column support in colsupp$(R_b) \cup$ colsupp$(c) - \{j\}$. If one further has that colsupp(c) is contained within colsupp(R_b) then the number of rows has strictly decreased.
3. the new R_b' will have row support within the original rowsupp(R_b).

Similarly, if one has a row vector v^T such that $v^T\tilde{\delta}_{-1} = 0$ and rowsupp(R_b) intersects with rowsupp(v). Then taking c to be a suitable column of R_b the transform $R_b \to R_b' = R_b + cv^T$ satisfies the following

1. the transform will preserve M;
2. the new R_b' will have row support in rowsupp$(R_b) \cup$ rowsupp$(v^T) - \{j\}$. If one further has that rowsupp(v^T) is contained within rowsupp(R_b) then the number of columns has strictly decreased.
3. the new R_b' will have column support within the original colsupp(R_b).

We now proceed to use these transforms in the following way. First, given any R_b we can find a new R_b' such that M is preserved and

$$\text{colsupp}(R_b') \subseteq \text{colsupp}(R_b), \tag{F9}$$
$$\text{rowsupp}(R_b') \subseteq \text{rowsupp}(R_b), \tag{F10}$$
$$\text{colsupp}(\tilde{\delta}_0 R_b') = \text{colsupp}(R_b'), \tag{F11}$$
$$\text{rowsupp}(R_b'\tilde{\delta}_{-1}) = \text{rowsupp}(R_b'), \tag{F12}$$
$$\text{colsupp}(R_b'\tilde{\delta}_{-1}) \subseteq \text{colsupp}(S_L), \tag{F13}$$
$$\text{rowsupp}(\tilde{\delta}_0 R_b') \subseteq \text{rowsupp}(S_R), \tag{F14}$$

The first two equations tell us that the transform will not add any new rows or columns. The second two equations are enforced by removing any columns in the kernal of $\tilde{\delta}_0$ and removing any rows v^T such that $v \in \tilde{\delta}_{-1}^T$. The last two equations are slightly more subtle. First note that if $R_b\tilde{\delta}_{-1}$ has any nonzero columns outside colsupp(S_L), the column must be in the kernal of $\tilde{\delta}_0$. To prove this, note that if the offending column was outside ker$(\tilde{\delta}_0)$ then colsupp$(\tilde{\delta}_0 R_b \tilde{\delta}_{-1})$ would be strictly larger than colsupp$(\tilde{\delta}_0 S_L)$ which contradicts $\tilde{\delta}_0 R_b \tilde{\delta}_{-1} = \tilde{\delta}_0 S_L$. Since the column is in ker$(\tilde{\delta}_0)$ and within colsupp$(R_b\tilde{\delta}_{-1})$, its presence allows us to remove a row from R_b. Similarly, if the last equation does not hold, we can remove a column from R_b. Such a process must terminate before we eliminate all rows and columns from R_b (unless of course $M = 0$ which is a trivial case) and so after a finite number of such transformations the above conditions must hold.

Next, we perform some further transformations to impose the conditions

$$\text{rowsupp}(R_b\tilde{\delta}_{-1}) \subseteq \text{rowsupp}(S_L), \tag{F15}$$
$$\text{colsupp}(\tilde{\delta}_0 R_b') \subseteq \text{colsupp}(S_R). \tag{F16}$$

Assume the first condition is not true. Then there exists at least one column, say c, of $R_b\tilde{\delta}_{-1}$ such that rowsupp(c) is not contained within rowsupp(S_L). Furthermore, if c' is the corresponding column of S_L we must have that $c' \neq c$. However, since $\tilde{\delta}_0 R_b \tilde{\delta}_{-1} = \tilde{\delta}_0 S_L$ we must have that $\tilde{\delta}_0 c = \tilde{\delta}_0 c'$. Therefore, the vector $w = c' - c$ satisfies the following properties: $w \neq 0$; $w \in$ ker$(\tilde{\delta}_0)$ and rowsupp$(w) \subseteq$ rowsupp$(R_b\tilde{\delta}_{-1}) \cup$ rowsupp(S_L). Therefore, we can use this column vector to remove a row from R_b and the set rowsupp$(R_b\tilde{\delta}_{-1}) \cup$ rowsupp(S_L) strictly decreases in size. A similar argument allows us to reduce the column support.

By repeating the above transformations until the process terminates, we ensure that $R_b\tilde{\delta}_{-1}$ has row and column support strictly within that of S_L. Therefore, the combination $S_L - R_b\tilde{\delta}_{-1}$ also has row and column support strictly within that of S_L. We can infer that $S_L - R_b\tilde{\delta}_{-1} = \sum_i \alpha_i \otimes \hat{a}_i$ where α_i are the column vectors. Since S_L has at most $|S_L|$ columns, there can be at most $|S_L|$ nonzero α_i. Since S_L has at most $|S_L|$ rows, each α_i has weight at most $|S_L|$. This proves the small $|S_L|$ remainder property of our lemma (see property 3). The small $|S_R|$ remainder property holds by a similar fashion (see property 4). Furthermore, combining Eq. (F16) and Eq. (F11), we conclude that the final R_b has fewer rows than S_L and so no more than $|S_L|$ rows. Similarly, we deduce that the final R_b has fewer columns than S_R and so no more than $|S_R|$ rows. Since the nonzero values of R_b are contained within a submatrix of size $|S_L|$ by $|S_R|$, we know $|R_b| \leq |S_L| \cdot |S_R|$. This proves property 2 of the lemma. It should be clear that property 1 holds because the value of M was initially correct and has been preserved through all transformations.