

2-designs and Redundant Syndrome Extraction for Quantum Error Correction

Vickram N. Premakumar,¹ Hele Sha,¹ Daniel Crow,¹ Eric Bach,² and Robert Joynt^{1,3}

¹*Physics Department, University of Wisconsin-Madison, 1150 Univ. Ave., Madison, WI, USA*

²*Computer Science Department, University of Wisconsin-Madison, Madison, WI, USA*

³*Kavli Institute for Theoretical Sciences, University of Chinese Academy of Sciences, Beijing 100190, China*

(Dated: April 30, 2019)

Imperfect measurement can degrade a quantum error correction scheme. A solution that restores fault tolerance is to add redundancy to the process of syndrome extraction. In this work, we show how to optimize this process for an arbitrary ratio of data qubit error probability to measurement error probability. The key is to design the measurements so that syndromes that correspond to different errors are separated by the maximum distance in the signal space, in close analogy to classical error correction codes. We find that the mathematical theory of 2-designs, appropriately modified, is the right tool for this. Analytical and simulation results for the bit-flip code, the 5-qubit code, and the Steane code are presented. The results show that this redundant syndrome extraction shows an improvement in both cost and performance relative to conventional fault-tolerant error-correction schemes in situations, quite important in practice, where measure errors are common. In the near term, the construction of a fault-tolerant logical qubit with a small number of noisy physical qubits will benefit from targeted redundancy in syndrome extraction.

I. INTRODUCTION

A working quantum computer must be fault-tolerant: the reliability of all components must be considered, and appropriate measures taken for compensation of malfunctions [1, 2]. Error correction forms the core of this process. Error syndromes are extracted and used to generate the information needed to set the computer back on the right path. The syndrome information may itself contain errors because of imperfect measurements. This aspect of fault tolerance was recognized at an early stage of the development of the theory. In the two most prominent syndrome extraction protocols, the remedy was to repeat measurements already made [3, 4], thereby building in redundancy. This is a straightforward way to make the syndrome information more reliable.

In the last few years, more sophisticated schemes have been proposed. Fujiwara *et al.* noted that measuring more than a minimal set of stabilizers could be a more efficient way to extract reliable information and noted a possible connection to designs [5, 6]. Ashikmin *et al.* generalized existence theorems and the quantum Singleton bound of standard quantum error correction (QEC) theory so that they take into account redundancy in measurements [7]. Crow *et al.* used this redundant syndrome extraction (RSE) to give thresholds for qubit performance in a coherent error-correction scheme [8].

In this letter, we show how to optimize the process of RSE using the theory of 2-designs [9], which have long been used in classical error correction [?]. We take a rather simple model for the faults. The key feature of this model is to separately define the qubit error probability p_q and the syndrome measurement error probability p_m . Different physical implementations of quantum computation will have very different values of the ratio p_q/p_m and this will strongly influence the optimal RSE protocol. In this work we will only consider the simple situation of a quantum memory that is periodically refreshed by error correction; more complicated scenarios

with active gates would complicate the analysis but not introduce significant new concepts. The discussion is restricted to stabilizer codes [10]. It may be possible to use 2-designs to improve other codes, but it appears to be more complicated. We stress that RSE is equally applicable to measurement-based error correction and coherent error correction. For definiteness, we will use the language of measurement-based QEC in this work.

II. BIT FLIP CODE

This section is included in order to introduce the basic ideas of RSE. It treats the elementary example of the 3-qubit bit flip code [11]. The 3 physical qubits store 1 bit of quantum information and there is a probability p_q of a bit flipping. No other qubit errors are allowed. Stabilizers $S_1 = Z_1Z_2$, $S_2 = Z_2Z_3$ and $S_3 = Z_3Z_1$ can each be measured, always yielding ± 1 . An incorrect measurement result is obtained with probability p_m . The starting state (chosen arbitrarily in the code subspace) is $|000\rangle$; after a certain time 1 or more bits may flip and we measure a set of stabilizers, perhaps repeatedly. We define an event e to be the final state of the qubits together with the measurement results. Each event e has a probability $P(e)$ with $0 \leq P(e) \leq 1$ and a success factor $s(e) = 0$ or $s(e) = 1$ when the event is respectively uncorrectable or correctable. For example, if the textbook procedure of measuring a minimal set of generators S_1 and S_2 is used, a possible event is $e_0 = \{|001\rangle, +1, -1\}$. This can be made fault-tolerant by repeating the measurements and using majority rules on the measurement results. The probability of this event is $P(e_0) = p_q(1 - p_m)^2(1 - p_q)^2$ since there is 1 qubit error and 0 measurement errors. $s(e_0) = 1$ since the information obtained from the measurements allows us to correct the error. The total failure probability of an error correction protocol, including possible RSE, is $F = 1 - \sum_e P(e)s(e)$. In addition, we define the cost C of

Protocol	Failure Rate	Cost
Minimal QEC	$2p_m + p_m^2 + 3p_q^2$	2
Fault-tolerant QEC	$15p_m^2 + 3p_q^2$	$4 + 2p_m$
RSE	$3p_m^2 + 3p_q^2 + 9p_m p_q$	3

Table II.1. Failure rate and cost for 3 error-correction protocols for the 3-qubit bit-flip code.

a protocol to be the expected total number of stabilizer measurements in a correction cycle.

The RSE protocol differs from both the simple protocol and its fault-tolerant extension in that one measures *the complete set of stabilizer group generators* S_1, S_2 and S_3 . This already builds in redundancy; if there is one measurement error then exactly one of the S_i is equal to -1 . If 2 of the S_i is equal -1 then there is a unique instruction as to which bit to flip back. (Here and henceforth we use S_i both for the operators and for the result of measuring the operators.) The key point is that there is a unique signal even if there is a measurement error.

Once protocols are established, then it is straightforward to sum over the events and compute the failure rates and costs. In Table II.1 we tabulate the results to quadratic order in p_q and p_m and the cost to linear order.

The fact that minimal QEC has a linear term in p_m is the signature that it is not fault-tolerant and is therefore not a candidate for a working computer. More importantly, the fault-tolerant version of conventional QEC is always more costly than RSE and the failure rate for conventional QEC exceeds that of RSE whenever $15p_m^2 + 3p_q^2 > 3p_m^2 + 3p_q^2 + 9p_m p_q$. This reduces to $p_m > 3p_q/4$, which is likely to happen in many implementations. It is interesting that RSE is superior even for $p_m = p_q$, a case often considered.

III. 2-DESIGNS

The crucial feature of RSE for the bit flip code is that the syndrome possesses a unique signature when there is a measurement error. This feature can be generalized to more complex codes that can correct phase flip as well as bit flip errors. Consider an $[[n, k, d]]$ stabilizer code with n the number of physical qubits, k the number of logical qubits and d the distance; the code can correct errors on up to $(d-1)/2$ physical qubits. We will focus on $k=1$ and the logical operators are $X_L = \otimes_{i=1}^n X_i$ and $Z_L = \otimes_{i=1}^n Z_i$, as in the Steane $[[7, 1, 3]]$ code. Our notation in this paper extends the usual one slightly, since we wish also to detect up to s syndrome measurement errors - hence we refer to $[[n, k, d, s]]$ codes. Standard quantum error correction without repetitions has $s=0$.

In RSE for a CSS code we measure $m = C/2$ stabilizer operators of the form $S = X_{i_1} X_{i_2} \cdots X_{i_w}$ and $m = C/2$ stabilizer operators of the form $S = Z_{i_1} Z_{i_2} \cdots Z_{i_w}$. Each stabilizer has weight w . Here $\{i_1, i_2, \dots, i_w\}$ are chosen from the set $\{1, 2, \dots, n\}$, and any given S is completely

defined by this choice. Thus for CSS codes X and Z errors are handled separately, so we simply use 2 copies of a single design, and this gives a particularly economical and effective RSE protocol. The measurement result of the Z -type stabilizers is different for any bit flip. Tabulating these possible syndrome results yields an $m \times (n+1)$ matrix E whose entries are ± 1 . The entry E_{ij} is the result of correctly extracting the value of S_i for a bit flip on the j -th physical qubit. At a minimum, the rows of E must all be distinct in order to diagnose an error uniquely. We wish to go beyond this. *Fault tolerance in RSE is achieved not by repetition but by choosing our measurements so that the results differ by as much as possible.* This motivates the use of 2-designs for our choice of measurements.

A 2-design is a family of subsets of a larger set. This family must fulfill certain conditions. For present purposes there is a set of n qubits and the indices on each Z -type stabilizer to be measured defines a subset of the qubit indices. Thus the family of subsets is determined by the choice of Z -type stabilizers. There are m subsets. The conditions for this choice to be a 2-design are: (1) each subset has the same size w ; (2) every index must appear in exactly ρ subsets; (3) every pair of indices appears in exactly λ subsets. The parameters are not all independent. They satisfy the basic 2-design relations $mw = n\rho$ and $\lambda(n-1) = \rho(w-1)$. These equations are proved using counting arguments.

Let us define the Hamming-like distance D between any two Z -type stabilizers S_i and $S_{i'}$ as $D(S_i, S_{i'}) = \sum_{j=1}^n |E_{ij} - E_{i'j}|$, where E_{ij} is the result when the j th qubit has flipped. Then if the choice of the S_i is a 2-design we have that $D(S, S') = 2(\rho - \lambda)$ for all S and S' . This may be shown by arguments similar to those in [12]. This the key feature of 2-designs for error correction purposes: it enables us to systematically maximize $\rho - \lambda$.

To illustrate the definition we give the example of a simple 2-design known as the order-2 biplane. It applies to a system of $n = 7$ qubits. The stabilizers are $S_1 = Z_1 Z_5 Z_6 Z_7$, $S_2 = Z_2 Z_4 Z_6 Z_7$, $S_3 = Z_3 Z_4 Z_5 Z_7$, $S_4 = Z_1 Z_2 Z_4 Z_5$, $S_5 = Z_1 Z_3 Z_4 Z_6$, $S_6 = Z_2 Z_3 Z_5 Z_6$, $S_7 = Z_1 Z_2 Z_3 Z_7$. It is not hard to verify that this choice satisfies the constraints for a 2-design with $w = 4$, $m = 7$, $\rho = 4$ and $\lambda = 2$. We will use this 2-design below.

The fundamental criterion for the choice of stabilizers is the minimization of the failure rate F and the cost C . We have seen that the natural arena for this is the 2-design. However, not all 2-designs can be used in conjunction with stabilizer quantum error correction. There is one constraint for all RSE schemes based on 2-designs.

Constraint 1. The definition of a stabilizer requires that it must commute with the logical operators, *i.e.*, $[S, \otimes_{i=1}^n X_i] = [S, \otimes_{i=1}^n Z_i] = 0$ for all S . A short calculation shows that this is true if and only if w is even.

Constraint 2. (CSS codes only.) The use of two copies of a design generates an additional constraint. The stabilizer group is commutative. All X -type stabilizers trivially commute with each other; the same is true for the Z -type stabilizers. An X -type stabilizer

commutes with a Z -type stabilizer if and only if the intersection of the set of indices of the X -type stabilizer with the set of indices of the Z -type stabilizer has even cardinality. This happens for all such pairs of stabilizers if and only if λ is even.

These two constraints rule out a majority of 2-designs for CSS-RSE. The order-2 biplane with $w = 4$ and $\lambda = 2$ is allowed, but the natural successor is the order-3 biplane with $w = 5$: it cannot serve as the basis for an RSE scheme.

IV. RESULTS

A. 5-qubit code

The $[[5,1,3]]$ perfect code is not a CSS code, so only a single 2-design is used for all errors. We take the stabilizer group generated by $S_1 = X_1Z_2Z_3X_4$, $S_2 = X_2Z_3Z_4X_5$, $S_3 = X_1X_3Z_4Z_5$, and $S_4 = Z_1X_2X_4Z_5$, which is then a $[[5,1,3,1]]$ code. The stabilizer subscripts are an instance of the 2-design known as ????. Once the stabilizer set is chosen we can compute the failure rate F_{RSE} as a function of p_m and p_q . For the 5-qubit code it is also of interest to compare standard repeated quantum error correction to an abbreviated version of RSE in which a single additional stabilizer $S_1S_2S_3S_4$ is added to the minimal set. We abbreviate this protocol as PC . This is somewhat analogous to a single parity check in classical error correction. Analytical results for F_{QEC} , F_{PC} , and F_{RSE} are given in the supplementary material. Choosing F_{QEC} as a baseline, we plot the relative failure rates in Fig. 1 for a range of error probabilities relevant to near-term quantum information processing. See that PC has an advantage over QEC for $p_m > XXXp_q$. However, RSE is superior to both QEC and PC for all p_m, p_q in the appropriate regime. This can be traced back to the fact that $F_{RSE} \sim p_m^4$ for small p_m , while $F_{QEC}, F_{PC} \sim p_m^2$, a qualitative difference. In Fig. 1a we compare the failure rate F_{QEC} for fault-tolerant QEC to F_{PC} , the parity-check protocol. We see that

B. Steane code

In our notation, the Steane code is a $[[7,1,3,0]]$ code. When syndrome measurements errors occur, it is not fault-tolerant. 3-fold repetition of its measurement sequence with majority rules gives a $[[7,1,3,1]]$ code. The order-2 biplane RSE procedure utilizes 14 stabilizers: those given in the previous section and another 7 with $Z_i \rightarrow X_i$. It is a fault tolerant $[[7,1,3,1]]$ code. We again give the comparison of failure rates for 3 protocols: the repeated Steane code, denoted QEC; a PC code with two additional stabilizers, one of the X type and one of the Z type, in both cases a product of the usual gener-

ators; and the RSE approach measuring the full stabilizer group. This final set of stabilizers corresponds to 2 copies of the order-2 biplane. The results demonstrate

Protocol	Failure Rate	Cost
Minimal QEC	$3p_m - 3p_m^2 + 21p_q^2$	3
Fault-tolerant QEC	$9p_m^2 + 21p_q^2$	$6 + 3p_m$
RSE with S_7	$6p_m^2 + 21p_q^2 + 28p_mp_q$	4
RSE	$21p_q^2$	7

Table IV.1. Failure rate and cost for 4 error-correction protocols for the Steane $[[7,1,3]]$ and $[[7,1,3,1]]$ codes.

that RSE has a distinct advantage over the other 2 protocols. It is even more dramatic than in the 5-qubit case. This combination of RSE with a CSS code is particularly effective in repairing measurement errors.

V. CONCLUSION

In this paper we have focused on 2-designs that appear in straightforward modifications of well-known codes. The long-term goal is to use known 2-designs to improve syndrome extraction by using known 2-designs to construct new quantum error-correction schemes. This not straightforward, since there is no general classification theorem for 2-designs, though a large number of special cases and some infinite families are known [13]. This is a promising line of research.

Once a quantum processor is characterized and p_q, p_m are known, we can look at the failure rates to determine which approach to take. The next consideration is cost. In a Shor-style extraction protocol each stabilizer measurement requires a number of ancilla qubits one greater than the weight of the operator itself [1]. In fault-tolerant QEC ancilla qubits can be reused on subsequent cycles of syndrome extraction. Thus, even though the number of QEC measurements may exceed that of RSE for a given code, the size of the quantum register required may in fact be larger for RSE. Recent ideas for using fewer ancilla qubits could be used to bring down the potential cost disparity between QEC and RSE [14]. This comes at the price of adding more gates, so an appraisal of which is the most fruitful approach involves a balancing act between number of qubits and circuit depth.

In the near term, we may expect the development of machines with 50-100 fairly noisy qubits and gates (the "NISQ" era). One important goal for this era is the development of a single fault-tolerant error-corrected logical qubit. The correction process involves multiple gates while the data qubits will often have reasonably long coherence times. In this situation, probably the most common one, we expect $p_m > p_q$. This means that the strategies outlined in this paper will be very relevant for this important goal.

-
- [1] P. W. Shor. Fault-tolerant quantum computation. In *Proceedings of 37th Conference on Foundations of Computer Science*, pages 56–65, Oct 1996.
 - [2] John Preskill. Fault-tolerant quantum computing. In Hoi-Kwong Lo, Tim Spiller, and Sandu Popescu, editors, *Introduction to Quantum Computation and Information*. World Scientific, 1999.
 - [3] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77:793–797, Jul 1996.
 - [4] David P. DiVincenzo and Peter W. Shor. Fault-tolerant error correction with efficient quantum codes. *Phys. Rev. Lett.*, 77:3260–3263, Oct 1996.
 - [5] Yuichiro Fujiwara. Ability of stabilizer quantum error correction to protect itself from its own imperfection. *Phys. Rev. A*, 90:062304, Dec 2014.
 - [6] Y. Fujiwara, A. Gruner, and P. Vandendriessche. High-rate quantum low-density parity-check codes assisted by reliable qubits. *IEEE Transactions on Information Theory*, 61(4):1860–1878, April 2015.
 - [7] A. Ashikhmin, C. Lai, and T. A. Brun. Robust quantum error syndrome extraction by classical coding. In *2014 IEEE International Symposium on Information Theory*, pages 546–550, June 2014.
 - [8] Daniel Crow, Robert Joynt, and M. Saffman. Improved error thresholds for measurement-free error correction. *Phys. Rev. Lett.*, 117:130503, Sep 2016.
 - [9] 2-designs are also known balanced incomplete block designs. Our sense of the word 2-design is not related to quantum 2-designs, which are probability distributions over quantum states.
 - [10] Daniel Gottesman. Class of quantum error-correcting codes saturating the quantum hamming bound. *Phys. Rev. A*, 54:1862–1868, Sep 1996.
 - [11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.
 - [12] Vera Pless. *Introduction to the Theory of Error-Correcting Codes*. Wiley-Interscience, New York, NY, USA, 3rd edition, 1982.
 - [13] Rudolf Mathon and Alexander Rosa. Tables of parameters of bibds with $r \leq 41$ including existence, enumeration and resolvability results: An update. *North-Holland Mathematics Studies*, 30:65–96, 12 1985.
 - [14] Rui Chao and Ben W. Reichardt. Quantum error correction with only two extra qubits. *Phys. Rev. Lett.*, 121:050502, Aug 2018.