



Optimally combining dynamical decoupling and quantum error correction

Gerardo A. Paz-Silva^{1,4} & D. A. Lidar^{1,2,3,4}

¹Department of Chemistry, University of Southern California, Los Angeles, California 90089, USA, ²Department of Electrical Engineering, University of Southern California, Los Angeles, California 90089, USA, ³Department of Physics, University of Southern California, Los Angeles, California 90089, USA, ⁴Center for Quantum Information Science & Technology, University of Southern California, Los Angeles, California 90089, USA.

Quantum control and fault-tolerant quantum computing (FTQC) are two of the cornerstones on which the hope of realizing a large-scale quantum computer is pinned, yet only preliminary steps have been taken towards formalizing the interplay between them. Here we explore this interplay using the powerful strategy of dynamical decoupling (DD), and show how it can be seamlessly and optimally integrated with FTQC. To this end we show how to find the optimal decoupling generator set (DGS) for various subspaces relevant to FTQC, and how to simultaneously decouple them. We focus on stabilizer codes, which represent the largest contribution to the size of the DGS, showing that the intuitive choice comprising the stabilizers and logical operators of the code is in fact optimal, i.e., minimizes a natural cost function associated with the length of DD sequences. Our work brings hybrid DD-FTQC schemes, and their potentially considerable advantages, closer to realization.

The nemesis of quantum information processing is decoherence, the outcome of the inevitable interaction of a quantum system with its environment, or bath. Several methods exist that are capable of mitigating this undesired effect. Of particular interest to us here are quantum error correction (QEC)^{1–4} and dynamical decoupling (DD)^{5–8}. QEC is a closed-loop control scheme which encodes information and flushes entropy from the system via a continual supply of fresh ancilla qubits, which carry off error syndromes. DD is an open-loop control scheme that reduces the rate of entropy growth by means of pulses applied to the system, which stroboscopically decouple it from the environment. QEC and DD have complementary strengths and weaknesses. QEC is relatively resource-heavy, but can be extended into a fully fault-tolerant scheme, complete with an accuracy threshold theorem^{9–14}. DD demands significantly more modest resources, can theoretically achieve arbitrarily high decoherence suppression^{15–22}, but cannot by itself be made fully fault-tolerant²³.

A natural question is whether a hybrid QEC-DD scheme is advantageous relative to using each method separately in the setting of fault-tolerant quantum computing (FTQC). Typically, improvements in gate accuracy achieved by DD mean that more noise can be tolerated by a hybrid QEC-DD scheme than by QEC alone, and that invoking DD can reduce the overhead cost of QEC. While early studies identified various advantages^{24–26}, they did not address fault tolerance. A substantial step forward was taken in Ref. 27, which analyzed “DD-protected gates” (DDPGs) in the FTQC setting. Such gates are obtained by preceding every physical gate (i.e., a gate acting directly on the physical qubits) in a fault tolerant quantum circuit by a DD sequence. DDPGs can be less noisy than the bare, unprotected gates, since DD sequences can substantially reduce the strength of the effective system-environment interaction just at the moment before the physical gate is applied. The gains can be very substantial if the intrinsic noise per gate is sufficiently small, and can make quantum computing scalable with DDPGs, where it was not with unprotected gates²⁷.

The analysis in Ref. 27 assumed a “local” perspective. Rather than analyzing the complete FT quantum circuit, each single- or multi-qubit gate was separately DD-protected. This required a strong locality constraint limiting the spatial correlations in the noise, known as the “local bath” assumption. Unfortunately, many physically relevant error models violate this assumption^{12–14}.

Here we aim to integrate DD with FTQC using a *global* perspective. This appears to be necessary in order to achieve high order decoupling in a multi-qubit setting, under general noise models. Rather than protecting individual gates we shall show how an entire FT quantum register, including data and ancilla qubits, can be enhanced using DD. This will allow us to relax the restrictive local bath assumption. Along the way, we identify a DD strategy that takes into account the basic structure and building blocks of FT quantum circuits, and identify optimal DD pulse sequences compatible with this structure, that drastically reduce the number of pulses required

SUBJECT AREAS:

QUANTUM MECHANICS
INFORMATION THEORY AND
COMPUTATION
QUANTUM INFORMATION
THEORETICAL PHYSICS

Received
13 December 2012

Accepted
7 February 2013

Published
5 April 2013

Correspondence and
requests for materials
should be addressed to
G.A.P.-S. (pazsilva@
usc.edu)



compared with previous designs. Such a reduction is crucial in order to reap the benefits of DD protection, for if a DD sequence becomes too long, noise can accumulate to such an extent as to outweigh any DD enhancements.

Results

The noise model. We assume a completely general noise Hamiltonian H acting on the joint system-bath Hilbert space, the only assumption being that $\|H\| < \infty$, where $\|\cdot\|$ denotes the sup-operator norm (the largest singular value, or largest eigenvalue for positive operators). Some noise models, such as bosonic baths, violate the $\|H\| < \infty$ assumption. In this case our analysis still applies, but operator norms must be replaced by frequency cut-offs^{5,14,27}. Informally, H contains a “good” and a “bad” part, the latter being the one we wish to decouple. H is k -local, i.e., involves up to k -body interactions, with $k \geq 1$. We allow for arbitrary interactions between the system and the bath, as well as between different parts of the system or between different parts of the bath. See Fig. 1.

Dynamical decoupling. DD pulse sequences comprise a series of rapid unitary rotations of the system qubits about different axes, separated by certain pulse intervals, and generated by a control Hamiltonian $H_C(t)$. They are designed to suppress decoherence arising from the “bad” terms in H . This is typically manifested in the suppression or even vanishing of the first N orders, in powers of the total evolution time T , of the time-dependent perturbation expansion (Dyson or Magnus series²⁸) of the evolution operator $U(T) = \mathcal{T} \exp\left(-i \int_0^T H(t) dt\right)$, where $H(t)$ is H in the “toggling frame” (the interaction picture generated by the DD pulse sequence Hamiltonian $H_C(t)$)⁸, and \mathcal{T} denotes time-ordering. When the first non-identity system-term of $U(T)$ appears at $O(T^{N+1})$ one speaks of *Nth order decoupling*. Such DD sequences are now known and well understood.

Most DD sequences can be defined in terms of pulses chosen from a mutually orthogonal operator set (MOOS), i.e., a set of unitary and Hermitian operators $\Omega = \{\Omega_i\}_{i=1}^{|\Omega|}$, $\Omega_i^2 = \mathbf{I}$ (identity) $\forall i$, and such that any pair of operators either commute or anticommute²⁰. The

generator set of a MOOS (gMOOS), $\hat{\Omega} = \{\Omega_i\}_{i=1}^{|\hat{\Omega}|}$, is defined as the minimal subset $\hat{\Omega} \subseteq \Omega$ such that every element of Ω is a product of elements of $\hat{\Omega}$ but no element in $\hat{\Omega}$ is itself a product of elements in $\hat{\Omega}$ (throughout this work we denote the generator set of a set S by \hat{S} and the cardinality of a set S by $|S|$). All deterministic DD sequences are finitely generated, meaning that the pulses are elements, or products of elements, of a finite DD generator set (DGS), which we identify with the gMOOS $\hat{\Omega}$.

The centralizer of the MOOS Ω is $\mathcal{C}_\Omega := \{A | [A, \Omega] = 0\}$, i.e., the set of operators which commute with all MOOS elements. A good example of a gMOOS is the generator set $\hat{P}_n = \{X^{(i)}, Z^{(i)}\}_{i=1}^n$, where $X^{(i)}$ ($Z^{(i)}$) denotes the Pauli- x (z) matrix acting on the i th qubit, of the Pauli group $P_n = P_1^{\otimes n}$ on n qubits (the group of all n -fold tensor products of the standard Pauli matrices $P_1 = \{1, X, Y, Z\}$, modulo \mathbb{Z}_2). For simplicity, since we will be dealing with qubits and are particularly interested in decoupling sequences that allow for bitwise pulses, we shall assume henceforth that $\hat{\Omega} \subseteq P_n$. It is necessary to recast the notion of decoupling order in the MOOS scenario, since the previously mentioned notion turns out to be too strong for our purposes.

Note that any operator A can be decomposed as $A = A_0 + A_r$, where A_0 (A_r) denotes the component that commutes (does not commute) with all elements of a MOOS, i.e., $A_0 \in \mathcal{C}_\Omega$. We shall say that a pulse sequence with generator set $\hat{\Omega}$ lasting total time T achieves “ N th order $\hat{\Omega}$ -decoupling” if the joint system-bath unitary evolution operator at the conclusion of the sequence becomes

$$U^{[N]}(T) = e^{iTH^{\text{eff},N}(T)}, \quad (1)$$

where the effective Hamiltonian is

$$H^{\text{eff},N}(T) \equiv H_0^{\text{eff},N}(T) + H_r^{\text{eff},N}(T) \quad (2a)$$

$$T \|H_r^{\text{eff},N}(T)\| \sim O[(T\|H\|)^{N+1}] \quad (2b)$$

$$H_0^{\text{eff},N}(T) \in \mathcal{C}_\Omega. \quad (2c)$$

When this holds we likewise say that the subspace invariant under \mathcal{C}_Ω and the subgroup \mathcal{C}_Ω have been decoupled to order N , in the sense

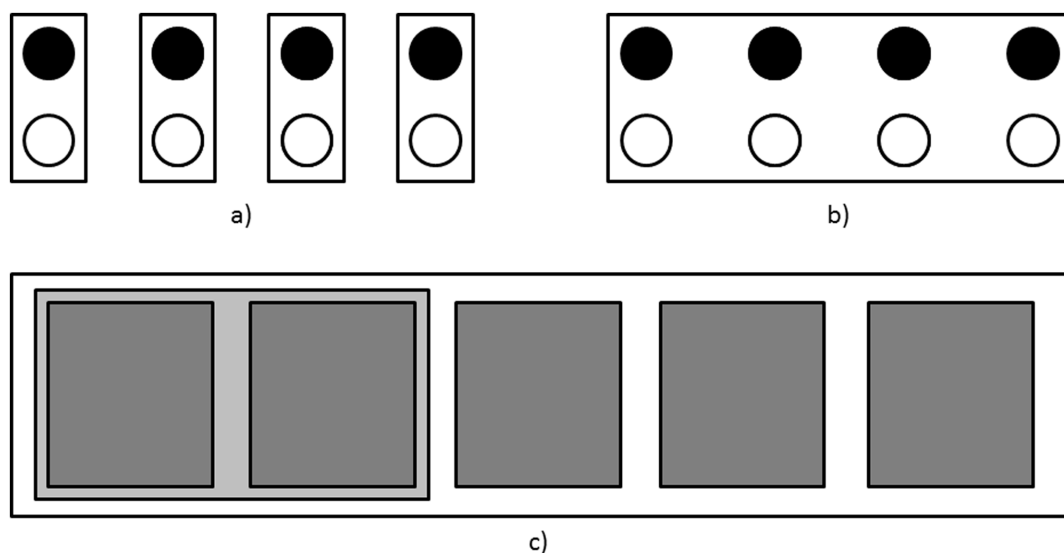


Figure 1 | Qubits and corresponding baths represented as white and black circles respectively. Bath operators corresponding to different operators inside a box do not necessarily commute, while they do if the baths are in different boxes. The Hamiltonians considered are general within each box, but not between them. In (a) a diagram of the “local bath assumption” used in Ref. 27 is shown, while (b) represents the general scenario considered in fault-tolerance^{12–14}. In (c) we illustrate one of our key results: domains are allowed to grow logarithmically in the size of the problem the FTQC is solving. The dark grey boxes represent such domains, each containing $O[\log(k_{\text{tot}})]$ physical qubits at the highest level of concatenation, where k_{tot} is the total number of logical qubits. When two domains need to interact (light grey box), then the joint DD generator set is used and the locality of the bath is updated accordingly.



that any operator not in C_Ω appears only in $O(T^{N+1})$. Thus the choice of the pulse generator set $\hat{\Omega}$ determines what subspace(s) can be decoupled, and conversely a subspace one is interested in decoupling to arbitrary order implies a choice of $\hat{\Omega}$.

Optimization of the DGS. We define the cost of a DD sequence as the total number of pulse intervals it uses to achieve N th order $\hat{\Omega}$ -decoupling. While this definition is motivated by the bang-bang limit of DD, i.e., zero-width pulses with finite pulse intervals, it can be modified to accommodate other types of constraints, such as finite bandwidth. The core of the arguments we develop here is unchanged for different cost functions, as long as there is an underlying group structure. For all known DD sequences (even those optimized for multiple qubits²⁹), the cost is at least

$$c_{\hat{\Omega}} = f(N)^{|\hat{\Omega}|}, \quad (3)$$

and $f(N)$ depends on the particular DD sequence. Pulse interval optimization has already reduced $f(N)$ from 2^N for CDD to $N + 1$ for NUDD. Here we are concerned instead with the optimization of the cost exponent $|\hat{\Omega}|$, to which end the following theorem will prove to be crucial:

THEOREM 1: *Let B be a subgroup of the Pauli group P_m generated by \hat{B} . Consider a DGS $\hat{\Omega} \subseteq P_n$ which decouples $C_\Omega \cap B$. Then $|\hat{\Omega}| \geq |\hat{B}|$. Moreover, the DGS $\hat{\Omega} = \hat{B}$ decouples B in the desired sense, and automatically saturates the bound.*

As an immediate application, we reproduce the well-known result that $\hat{\Omega} = \hat{P}_n$, and hence $|\hat{\Omega}| = 2n$, is optimal for n qubits without encoding⁸. Indeed, in this case the most general noise Hamiltonian is spanned by the elements of the “error group” $B = P_m$, so $|\hat{B}| = 2n$ and thus by Theorem 1 for any DGS $\hat{\Omega}$ it must be that $|\hat{\Omega}| \geq 2n$. On the other hand $\hat{\Omega} = \hat{P}_n$ indeed decouples P_n since $C_\Omega = 1$. Note also that Eq. (2c) yields $H_0^{\text{eff},N}(T) \propto 1$. Moreover, since DD sequences are known that achieve N th order $\hat{\Omega}$ -decoupling for $n \geq 1$ qubits (specifically CDD¹⁵ and NUDD²⁰, with explicit \hat{P}_n -based constructions given in Ref. 20), the generating set \hat{P}_n is the smallest one capable of achieving N th order decoupling of a general n -qubit Hamiltonian. However, as we discuss next, there is a better choice for the purpose of protecting a code subspace.

DD generator set for a QEC code. Consider a set of n physical qubits encoding k logical and r gauge qubits via some distance d code, i.e., an $[[n, k, r, d]]$ subsystem code^{30–32} (or an $[[n, k, d]]$ stabilizer code⁴ for $r = 0$), subject to the general noise model described above. Let $\hat{S} = \{S_\mu\}_{\mu=1}^Q$ denote the stabilizer generators, where $Q = n - (k + r)$, let $\hat{L} = \{X_L^{(i)}, Z_L^{(i)}\}_{i=1}^k$ denote the logical-operator generators of the code, and $\hat{G} = \{X_v, Z_v\}_{v=1}^r$ the gauge operator generators. In the $[[n, k, d]]$ code case, each error correctable by the code maps a codeword to a syndrome subspace labelled by an error syndrome, i.e., a sequence of ± 1 eigenvalues of the stabilizer generators⁴. In order to properly integrate DD with QEC, we require a set of DD generators $\hat{\Omega}$ which preserves the error syndromes to order N , i.e., such that $H_0^{\text{eff},N}$ acts trivially on each of the syndrome subspaces and does not mix them, so that at the conclusion of the sequence the original noise model for which the code was chosen, is preserved (again, to order N). This form of the N th order $\hat{\Omega}$ -decoupling requirement will enable error correction to function as intended. A simple, but important observation is that in light of this, we do not need to protect the complete 2^n -dimensional Hilbert space \mathcal{H} , but rather the 2^{n-k} syndrome subspaces. We seek to minimize the impact of decoupling an encoded state.

An intuitive choice for the DGS is the complete set of stabilizer and logical operator generators, i.e., let $\hat{\Omega} = \hat{S} \cup \hat{L}$. Then $C_\Omega = \hat{S} \subset \hat{\Omega}$. We refer to any DD sequence having a DGS of this type as a

“stabilizer-logical DD” (SLDD) sequence. While this choice is natural it is not obvious that is also optimal, and this is were Theorem 1 will prove to be useful. (One might try instead to choose as a DD sequence generator set the stabilizers only, i.e., let $\hat{\Omega} = \hat{S}^{24}$. However, since the logical operators of the same code commute with these stabilizer DD pulses, they are not decoupled and hence have non-trivial action on the code subspace, thus causing logical errors. Formally, when $\hat{\Omega} = \hat{S}$, $H_0^{\text{eff},N}$ will contain logical operators.) Now note that if $C_\Omega \subseteq \hat{\Omega}$, then the elements in C_Ω commute and they define $|C_\Omega| = 2^{|C_\Omega|}$ subspaces characterized by their eigenvalue under the action of C_Ω . In this case we have independent N th order $\hat{\Omega}$ -decoupling of each of these subspaces. In other words, $H_0^{\text{eff},N}$ leaves each of the syndrome subspaces invariant and does not mix them, as desired. Note that the choice $\hat{\Omega} = \hat{S} \cup \hat{L}$ also applies to subsystem codes^{30–32}. In this case each of the syndrome subspaces can be decomposed as $\mathcal{H}_{\text{logical}} \otimes \mathcal{H}_{\text{gauge}}$, where $\mathcal{H}_{\text{logical}}$ is invariant under $\hat{S} \cup \hat{G} = C_\Omega$, since the gauge operators act non-trivially on $\mathcal{H}_{\text{gauge}}$ only.

Optimal DGS for concatenated QEC codes. Many FTQC constructions are based on concatenated QEC codes³³, so what is the optimal DGS for this case, cost-wise? Suppose an $[[n, k, r, d]]$ code is concatenated R times. A complete generator set for all the stabilizers of such a code is given by $\bigcup_{q=1}^R \hat{S}^{(q)}$, where $\hat{S}^{(q)}$ is the stabilizer generator set of concatenation level q . Let $\hat{L}^{(R)}$ denote the set of R th-concatenation level logical generators.

THEOREM 2: *The optimal DGS for decoupling all the syndrome subspaces at concatenation level R is the SLDD set $\hat{\Omega} = \bigcup_{q=1}^R \hat{S}^{(q)} \cup \hat{L}^{(R)}$, where $|\hat{\Omega}| = n^R - (k+r)^R + 2k^R$.*

Note that the above theorem is general in the sense that is not limited to concatenated QEC codes as it only requires a stabilizer structure and a set of logical generators satisfying the MOOS structure. The only thing that will change for other stabilizer codes, such as surface or topological codes³⁴, is the actual expression in terms of n, k . Note also that by setting $R = 1$ Theorem 2 reduces to the optimality of SLDD for subspace or subsystem codes, with $|\hat{\Omega}| = n + k - r$ as claimed above. The subspace case is recovered by setting $r = 0$. Let us now quantify the gain achieved by choosing the optimal DGS for QEC codes.

Relative cost of SLDD. For an $[[n, k, d]]$ code and an SLDD sequence, the number of stabilizer generators $(n - k)$ plus logical operator generators $(2k)$ yields $|\hat{\Omega}| = n + k$, which means that $c_{\hat{S} \cup \hat{L}} = f(N)^{n+k} < c_{\hat{P}_n} = f(N)^{2n}$. Often $n \gg k$, so that $c_{\hat{S} \cup \hat{L}} \sim \sqrt{c_{\hat{P}_n}}$. In the case of $[[n, k, r, d]]$ subsystem codes³² the advantage is more pronounced: the number of stabilizers is $n - k - r$, so $|\hat{\Omega}| = n + k - r$. As an example consider the Bacon-Shor $[[m \times m, 1, (m - 1)^2, m]]$ subsystem code³⁰, which has the highest (analytically) known fault-tolerant threshold for error correction routines with¹² and without measurements³⁵. In this case one would have $c_{\hat{S} \cup \hat{L}} = f(N)^{2m} = (c_{\hat{P}_{m^2}})^{1/m}$, a polynomial advantage that grows with the block size m .

Let us illustrate this using the 9-qubit Bacon-Shor code. This code is defined via the stabilizer generator set $\{XXXXXXXXIII, XXXIIIXXXX, ZZIZZIZZI, IZZIZIZZI\}$ and has logical operators $Z_L = ZIIZIIZII, X_L = XXXIIIIII$. Using the above result we can decouple the relevant subspaces using just the six-element DGS containing

$$\{XXXXXXXXIII, XXXIIIXXXX, ZZIZZIZZI, IZZIZIZZI, X_L, Z_L\},$$

as opposed to the full-decoupling case which would use the eighteen-element DGS containing $\{X_i\}_{i=1}^9 \cup \{Z_i\}_{i=1}^9$, where A_i denotes the operator A acting on qubit i .



Choice of DGS for protecting ancilla states. The protection of certain ancilla states is also an important part of fault tolerance. Such states can be thought of as QEC codes with small stabilizer sets. E.g., $|cat_{m,+}\rangle = (|0\rangle^{\otimes a} + |1\rangle^{\otimes a})/\sqrt{2}$ is often used for fault-tolerant stabilizer measurements or for teleportation of encoded information. The stabilizer is generated by $\{X^{\otimes a}, \{Z_i Z_{i+1}\}_{i=1}^{a-1}\}$, and equals the DGS.

Decoupling multiple subgroups or invariant subspaces. Keeping in mind our goal of integrating DD with FTQC for a complete quantum register, a common scenario is that in which multiple subgroups have to be simultaneously decoupled. While in principle the optimal DGS can be found for any particular subgroup, as we have already done for QEC codes and certain ancillary states, one would like a way to build the optimal DGS for a collection of subgroups. How can this be done optimally? Assume that there are distinct and non-overlapping sets of $\{n_i\}$ physical qubits comprising a quantum register, e.g., a complete register comprising k logical qubits, along with the corresponding ancillas. Assume that they are partitioned into sets of sizes $\{k_i\}_{i=1}^p$, such that $k = \sum_{i=1}^p k_i$, and that each set i is encoded in some subsystem (or subspace) code $[[n_i, k_i, r_i, d_i]]$. For each block of k_i logical qubits we have an SLDD sequence with DGS $\hat{\Omega}_i = \hat{S}_i \cup \hat{L}_i$.

Let the Hamiltonians of the different sets be $\{H_i\}$, and spanned by the error groups $\{B_i \subset P_{n_i}\}$. Using Theorem 1, it follows that if $\hat{\Omega}_i$ is optimal for error group B_i , then $\hat{\Omega}_{\text{tot}} = \cup_i \hat{\Omega}_{B_i}$, optimally decouples the joint Hamiltonian spanned by $\cup_i B_i$. This form of composing a larger DGS out of the union of smaller, independent DGSs guarantees that each term of a general Hamiltonian acting on the whole register must anticommute with at least one element in $\hat{\Omega}_{\text{tot}}$, which in turn implies that $\hat{\Omega}_{\text{tot}}$, used to construct, e.g., a CDD or NUDD sequence, is capable of independent N th order $\hat{\Omega}_{\text{tot}}$ -decoupling of each of the subgroups. This can be formalized as follows:

COROLLARY 1: Let B_i be a of subgroup of the Pauli group P_{n_i} , generated by $\hat{B}^{(i)}$. If $\hat{B}^{(i)} \cap \hat{B}^{(j)} = \emptyset$ and $\cup_i \hat{B}^{(i)}$ satisfies the MOOS conditions, then the DGS $\hat{\Omega}$ which decouples the collection of subgroups $\{B_i\}$ satisfies $|\hat{\Omega}| \geq \sum_i |\hat{B}^{(i)}|$. Moreover, the DGS $\hat{\Omega} = \cup_i \hat{B}^{(i)}$ decouples $\cup_i B_i$ in the desired sense, and automatically saturates the bound.

This result is important since it allows the modular construction of optimal DGSs, such as the one required for decoupling two or more encoded qubits, or an encoded qubit and an ancilla.

Discussion

We have now assembled and described all the ingredients for optimally combining DD with FTQC for protection of a complete quantum register. However, we must ensure that the cost of implementing the DD sequence does not spoil quantum speedups. To this end we consider once more an $[[n, k, r, d]]$ subsystem code concatenated R times, used to encode an entire quantum register, and divide the register into $d(R)$ domains (e.g., a code block along with ancillas) of size $k_D(R) = O(k^R)$ logical qubits, such that the total number of logical qubits in the register is $k_{\text{tot}} = d(R)k_D(R)$. We then optimally decouple the i th domain using an SLDD sequence generated by $\hat{\Omega}_i = \cup_{q=1}^R (\hat{S}_i^{(q)} \cup \hat{L}_i^{(q)})$, $i \in \{1, \dots, d(R)\}$ (where $\hat{S}_i^{(q)}$ and $\hat{L}_i^{(q)}$ act non-trivially only on the qubits in the domain i), and ask for the maximal allowed size of each domain such that the DD sequence cost scales polynomially in k_{tot} , as this will ensure that any exponential quantum speedup is retained.

COROLLARY 2: In a fault tolerant quantum computation the maximal allowed domain size compatible with a DGS having cost $c_{\hat{\Omega}} = f(N)^{|\hat{\Omega}|} = \text{poly}(k_{\text{tot}})$, is $O[\log(k_{\text{tot}})]$.

Corollary 2 means that we can relax the local bath assumption²⁷, an assumption tantamount to assuming constant domain size $k_D \leq 2$; instead we find that domains are allowed to grow logarithmically with problem size. Note that this scaling law for the domain size is

the same as one would obtain in the absence of encoding. I.e., the code structure does not impose a fundamental limit on the profitable combination of DD and QEC. The scaling law is thus a statement regarding known DD sequences, in particular CDD or NUDD, even when the DGS is optimized, as in SLDD. When two domains i and j are required to interact, the joint DGS $\hat{\Omega}_i \cup \hat{\Omega}_j$ should be used [see Fig. 1(c)]. The size of these domains is large enough that they can sustain a full logical qubit, i.e., an encoded logical qubit with all the necessary ancillas for quantum correction and single qubit gates. Moreover, the size of such a joint DGS is compatible with retaining exponential quantum speedups. If the result is that at the highest concatenation level the noise per gate has been reduced (as shown explicitly for the local bath setting in Ref. 27), then a reduction in the number of required concatenation levels is enabled, hence reducing the overall overhead, or the effective noise threshold.

So far we discussed the problem of protecting stored quantum information; what about computation? Quantum logic operations can be combined with DD, e.g., using “decouple while compute” schemes^{36,37}, or (concatenated) dynamically corrected gates [(C)DCGs] for finite-width pulses³⁸, or dynamically protected gates²⁷ in the zero-width (ideal) pulse limit. The optimal SLDD scheme introduced here is directly portable into the latter two schemes, since they use the same DD building blocks and the associated group structure. It is important to emphasize that SLDD sequences require only bitwise (i.e., transversal) pulses, and can be generated by one-local Hamiltonians, thus not altering the assumptions of the CDCG construction. More importantly, the polynomial scaling guaranteed by Corollary 2 also applies in the quantum logic scenario, thus allowing, in principle, a fidelity improvement without sacrificing the speedup of quantum computing.

In conclusion, in this work we identified the optimal decoupling generating set in the general context of protection of subspaces invariant under the action of a group, and showed how this can be applied in the context of information encoded into a quantum error correcting code. This allowed us to show how DD and FTQC can be optimally integrated. In doing so we showed that one can simultaneously protect disjoint domains growing logarithmically with problem size, thus improving over the constant-size domains associated with the local-bath assumption made in earlier work on hybrid DD-FTQC strategies. Future work should focus on demonstrating that DD-enhanced FTQC results in improved resource overheads and lower noise thresholds, and identify, or rule out, multi-qubit DD sequences with sub-exponential scaling in the cardinality of their generating sets.

Methods

Dynamical decoupling background. Concatenated DD (CDD)¹⁵, the first explicit arbitrary order DD method, uses a recursive nesting of elementary pulse sequences and (provided pulse intervals can be made arbitrarily small) can be used to achieve N th order decoupling of n qubits with both N and n arbitrary, but requires a number of pulses that is exponential in both N and n ¹⁵. Pulse-interval optimized sequences are now known for purely longitudinal or purely transversal system-bath coupling, requiring only $N + 1$ pulses for N th order decoupling¹⁶. The Uhrig DD (UDD) sequence that accomplishes this was generalized to the quadratic DD (QDD) sequence for general decoherence of a single qubit¹⁹, which uses a nesting of the transversal and longitudinal UDD sequences to achieve N th order decoupling using $(N + 1)^2$ pulses, an exponential improvement over CDD and concatenated UDD¹⁸. Both UDD and QDD are essentially optimal in terms of the number of pulses required, and are provably universal for arbitrary, bounded baths^{17,21,22}. Generalizing from QDD, nested UDD (NUDD) pulse sequences were proposed for arbitrary system-environment coupling involving n qubits or even higher-dimensional systems²⁰. NUDD requires $(N + 1)^{2n}$ pulses to decouple n qubits to N th order from an arbitrary environment. For more details see, e.g., the recent review³⁹.

Proof of Theorem 1. Let B be generated by $\hat{B} = \{b_i\}_{i=1}^{|B|}$, so that $|B| = 2^{|B|}$, and consider the DD generating set $\{\Omega_x\}_{x=1}^{|\hat{\Omega}|}$. One can associate to each b_i a string $s^{(i)} = \{s_1^{(i)}, \dots, s_{|\hat{\Omega}|}^{(i)}\}$ where $s_x^{(i)}$ encodes the effect the pulse Ω_x has on the error term b_i (commutes or anticommutes), via $s_x^{(i)} = \pm 1$ if $\Omega_x b_i \Omega_x = \pm b_i$, i.e., $\Omega_x b_i \Omega_x = s_x^{(i)} b_i$. The total number of such strings is $|B|$, i.e., $i \in \{1, \dots, 2^{|B|}\}$. Note that if $b \in B$ is associated



with the “identity string” $\{+, \dots, +\}$ then it will not be decoupled since it commutes with all decoupling pulses. Now, we can associate $|\hat{\Omega}|$ bits (over the \pm alphabet) to the $|\hat{\Omega}|$ DD sequence generators. From these $|\hat{\Omega}|$ bits we can construct exactly $2^{|\hat{\Omega}|}$ distinct strings $\{r^{(i)}\}_{i=1}^{2^{|\hat{\Omega}|}}$, where $r^{(i)} = \{r_1^{(i)}, \dots, r_{|\hat{\Omega}|}^{(i)}\}$, and $r_j^{(i)} \in \{-, +\}$. Let us map the $r^{(i)}$ strings, $i \in \{1, \dots, 2^{|\hat{\Omega}|}\}$, to the $s^{(i)}$ strings, $i \in \{1, \dots, 2^{|\hat{B}|}\}$. Clearly, if B has “too many” elements, i.e., if $|\hat{B}| > |\hat{\Omega}|$, then the mapping will be one-to-many, i.e., some of the $r^{(i)}$ strings will have to be repeated, meaning that the set $\{s^{(i)}\}_{i=1}^{2^{|\hat{\Omega}|}}$ will contain duplicates. The product of any two duplicate strings is the identity string $\{+, \dots, +\}$. But since B is a group, this means that the product of the two distinct elements of B associated with a duplicated string is also a group element, and moreover is associated with the identity string. Since the elements of B are in the Pauli group, the product of any two distinct elements cannot be the identity operator. Thus we have shown that there is a non-identity element of B which is associated with the identity-string, and hence is not decoupled. On the other hand, a DD generating set of cardinality $|\hat{B}|$ exists and is just \hat{B} itself.

Theorem 1 can in fact be generalized by allowing B to not be a subgroup of P_n , although we do not require or use this more general version here. The proof is similar: if a DGS $\hat{\Omega}$ satisfying the MOOS properties exists such that the only element of \hat{B} that commutes with all elements in $\hat{\Omega}$ is 1 and, if each element in \hat{B} has a unique inverse then, following an argument similar to the one used in the proof of Theorem 1, such a DGS decoupling B satisfies $|\hat{\Omega}| \geq |\hat{B}|$. This more general result applies to higher dimensional subsystems, such as qudits. The existence of such a DGS is guaranteed, in particular, for subgroups of P_n .

Counting the number of stabilizer generators in a concatenated subsystem code.

Before proving Theorem 2 we explain how to number of stabilizer generators behaves under concatenation. The total number of physical qubits n in an $[[n, k, d]]$ stabilizer subspace code equals the sum of the $Q = n - k$ stabilizer and k logical qubits⁴. After concatenating R times $m \rightarrow n(R) = n^R$, $k \rightarrow L(R) = k^R$, and hence $Q \rightarrow Q(R) = n^R - k^R$. Likewise, the total number of physical qubits n in an $[[n, k, r, d]]$ stabilizer subsystem code equals the sum of the $Q = n - (k + r)$ stabilizer, k logical, and r gauge qubits³². One can always view an $[[n, k, r, d]]$ subsystem code as an $[[n, k', d']]$ subspace code with $k' = k + r$ and distance $d' \leq d$: in a subsystem code only the k qubits designated as logical qubits are associated with the code distance d , whereas the gauge qubits have distance at most d . For example, in the $[[9, 1, 4, 3]]$ Bacon-Shor code⁴⁰ the gauge qubits have distance 2 while the logical qubit has distance 3. Thus, after concatenating an $[[n, k, r, d]]$ stabilizer subsystem code R times, the number of physical qubits is $n(R) = n^R$, which equals the sum of the $Q(R)$ stabilizer qubits, $L(R) = k^R$ logical qubits (with distance d), and $G(R)$ gauge qubits (with distance $\leq d$). Alternatively, viewed as an $[[n, k', d']]$ subspace code concatenated R times, it has $L'(R) = (k')^R$ logical qubits. However, these logical qubits are the logical and gauge qubits of the original code, i.e., $L'(R) = L(R) + G(R)$, so that $L(R) + G(R) = (k + r)^R$.

Proof of Theorem 2. The number of physical qubits after R levels of concatenation of any $[[n, k, r, d]]$ subsystem stabilizer code is $n(R) = n^R$, and the error group for the entire Hilbert space is the Pauli group $P_{n(R)}$. We need to protect the $2^{Q(R)}$ syndrome subspaces, where $Q(R) = |\bigcup_{q=1}^R \hat{S}^{(q)}|$ is the total number of stabilizer generators after the code is concatenated R times. $Q(R) = n(R) - L(R) - G(R)$, where, as shown above, $L(R) = k^R [G(R)]$ is the number of logical (gauge) qubits at level R , and $L(R) + G(R) = (k + r)^R$.

The SLDD sequence generated by $\hat{\Omega} = \bigcup_{q=1}^R \hat{S}^{(q)} \bigcup \hat{L}^{(R)}$ satisfies the requirement of independent N th order $\hat{\Omega}$ -decoupling of the $2^{Q(R)}$ syndrome subspaces since the stabilizers (as DD pulses) remove the errors at each level q , logical included (recall that a logical error at level $q - 1$ anticommutes with at least one level q stabilizer generator), but not the logical errors at the top level, for which we need $\hat{L}^{(R)}$ as DD pulses. Moreover, for this sequence $|\hat{\Omega}| = Q(R) + 2L(R) = n^R - (k + r)^R + 2k^R$ as claimed. Now, any operator in $P_{n(R)}$ which is not a stabilizer or gauge operator acts as an error either within or between syndrome subspaces. Thus our choice of code dictates which elements of $P_{n(R)}$ act as errors, and clearly this error set is precisely $B = P_{n(R)}/C_{\hat{\Omega}}$, where the centralizer generator is $\hat{C}_{\hat{\Omega}} = \bigcup_{q=1}^R \hat{S}^{(q)} \bigcup \hat{G}^{(q)}$. We have $|\hat{C}_{\hat{\Omega}}| = Q(R) + 2G(R)$. On the other hand $|\hat{B}| = 2n(R) - |\hat{C}_{\hat{\Omega}}| = Q(R) + 2L(R)$, so that $|\hat{B}| = |\hat{\Omega}|$ and $B \cap C_{\hat{\Omega}} = 1$, which proves the optimality of $|\hat{\Omega}|$ by virtue of Theorem 1.

This implies that $\hat{\Omega} = \hat{S} \hat{U} \hat{L}$ is not only the natural choice, since it exactly decouple $(\hat{S} \hat{U} \hat{L}) \cup P_{n(R)}$, but is also the optimal choice.

We note that formally, the QEC structure and the corresponding set $\hat{S} \hat{U} \hat{L}$ separate $P_{n(R)}$ into families^{40,41} $O_{\{z_1, \dots, z_{L(R)+Q(R)}\}}$, such that $O_{\{z_1, \dots, z_s = 0, \dots\}}$ commutes with the s th element of the DGS $\hat{S} \hat{U} \hat{L}$, and $O_{\{z_1, \dots, z_s = 1, \dots\}}$ anticommutes with the s th element of the set $\hat{S} \hat{U} \hat{L}$. Operators with $z_s = 1$, for s corresponding to any of the elements in \hat{S} generate transitions between the syndrome subspaces, while operators with $z_s = 1$ for ℓ corresponding to any of the elements in \hat{L} generate transitions within the syndrome subspace. So $\hat{B} = \{O_z\}$ is a subgroup of P_n , with the product rule $H_{z'} H_{z''} = H_{z' \oplus z''}$, where \oplus denotes bitwise sum modulo two, and with $|\hat{S}| + |\hat{L}|$ generators. This

effectively maps the problem into one in which one has to decouple the subspace invariant under elements of $C_{\hat{\Omega}} = O_{\hat{\Omega}} \subseteq P_n$.

Proof of Corollary 2. We assume that the total cost per domain $c_{\hat{\Omega}}$ is Eq. (3) as it captures all known DD sequences. Theorem 2 shows that $|\hat{\Omega}| = O[n^R - (k + r)^R + 2k^R]$ (the O symbol is used since we allow for the presence of ancillas in the domain). We may assume that the code has parameters such that $n \sim r \sim k$, so that $|\hat{\Omega}| = O(k^R) = O[k_D(R)]$. Now recall that $R = O[\log \log(k_{\text{tot}})]$ in a fault-tolerant simulation of a quantum circuit⁴². Therefore $c_{\hat{\Omega}} = f(N)^{|\hat{\Omega}|} = \text{poly}(k_{\text{tot}})$ requires $k_D(R) = O[\log(\text{poly}(k_{\text{tot}}))] = O[\log(k_{\text{tot}})]$.

- Shor, P. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A* **52**, R2493 (1995).
- Calderbank, A. & Shor, P. Good quantum error correcting codes exist. *Phys. Rev. A* **54**, 1098 (1996).
- Steane, A. Multiple particle interference and quantum error correction. *Proc. R. Soc. London Ser. A* **452**, 2551 (1996).
- Gottesman, D. Class of quantum error-correcting codes saturating the quantum hamming bound. *Phys. Rev. A* **54**, 1862 (1996).
- Viola, L. & Lloyd, S. Dynamical suppression of decoherence in two-state quantum systems. *Phys. Rev. A* **58**, 2733 (1998).
- Zanardi, P. Symmetrizing evolutions. *Phys. Lett. A* **258**, 77 (1999).
- Duan, L.-M. & Guo, G. Suppressing environmental noise in quantum computation through pulse control. *Phys. Lett. A* **261**, 139 (1999).
- Viola, L., Knill, E. & Lloyd, S. Dynamical decoupling of open quantum systems. *Phys. Rev. Lett.* **82**, 2417 (1999).
- Aharonov, D. & Ben-Or, M. Fault tolerant quantum computation with constant error rate. *SIAM J. Comput.* **38**, 1207 (2008).
- Knill, E., Laflamme, R. & Zurek, W. Resilient quantum computation: Error models and thresholds. *Proc. R. Soc. London Ser. A* **454**, 365 (1998).
- Terhal, B. & Burkard, G. Fault-tolerant quantum computation for local non-markovian noise. *Phys. Rev. A* **71**, 012336 (2005).
- Aliferis, P., Gottesman, D. & Preskill, J. Quantum accuracy threshold for concatenated distance-3 codes. *Quantum Inf. Comput.* **6**, 97 (2006).
- Aharonov, D., Kitaev, A. & Preskill, J. Fault-tolerant quantum computation with long-range correlated noise. *Phys. Rev. Lett.* **96**, 050504 (2006).
- Ng, H. K. & Preskill, J. Fault-tolerant quantum computation versus gaussian noise. *Phys. Rev. A* **79**, 032318 (2009).
- Khodjasteh, K. & Lidar, D. A. Fault tolerant quantum dynamical decoupling. *Phys. Rev. Lett.* **95**, 180501 (2005).
- Uhrig, G. Keeping a quantum bit alive by optimized π -pulse sequences. *Phys. Rev. Lett.* **98**, 100504 (2007).
- Yang, W. & Liu, R.-B. Universality of Uhrig dynamical decoupling for suppressing qubit pure dephasing and relaxation. *Phys. Rev. Lett.* **101**, 180403 (2008).
- Uhrig, G. S. Concatenated control sequences based on optimized dynamic decoupling. *Phys. Rev. Lett.* **102**, 120502 (2009).
- West, J. R., Fong, B. H. & Lidar, D. A. Near-optimal dynamical decoupling of a qubit. *Phys. Rev. Lett.* **104**, 130501 (2010).
- Wang, Z.-Y. & Liu, R.-B. Protection of quantum systems by nested dynamical decoupling. *Phys. Rev. A* **83**, 022306 (2011).
- Kuo, W.-J. & Lidar, D. A. Quadratic dynamical decoupling: Universality proof and error analysis. *Phys. Rev. A* **84**, 042329 (2011).
- Jiang, L. & Imambekov, A. Universal dynamical decoupling of multiqubit states from environment. *Phys. Rev. A* **84**, 060302 (2011).
- Khodjasteh, K., Erdélyi, T. & Viola, L. Limits on preserving quantum coherence using multipulse control. *Phys. Rev. A* **83**, 020305 (2011).
- Byrd, M. S. & Lidar, D. A. Comprehensive encoding and decoupling solution to problems of decoherence and design in solid-state quantum computing. *Phys. Rev. Lett.* **89**, 047901 (2002).
- Boulant, N., Pravia, M. A., Fortunato, E. M., Havel, T. F. & Cory, D. G. Experimental Concatenation of Quantum Error Correction with Decoupling. *Quant. Inf. Proc.* **1**, 135 (2002).
- Khodjasteh, K. & Lidar, D. A. Quantum computing in the presence of spontaneous emission by a combined dynamical decoupling and quantum-error-correction strategy. *Phys. Rev. A* **68**, 022322 (2003). Erratum: *ibid*, *Phys. Rev. A* **72**, 029905 (2005).
- Ng, H. K., Lidar, D. A. & Preskill, J. Combining dynamical decoupling with fault-tolerant quantum computation. *Phys. Rev. A* **84**, 012305 (2011).
- Blanes, S., Casas, F., Oteo, J. & Ros, J. The Magnus expansion and some of its applications. *Phys. Rep.* **470**, 151 (2009).
- Wocjan, P. Efficient decoupling schemes with bounded controls based on eulerian orthogonal arrays. *Phys. Rev. A* **73**, 062317 (2006).
- Bacon, D. Operator quantum error-correcting subsystems for self-correcting quantum memories. *Phys. Rev. A* **73**, 012340 (2006).
- Kribs, D., Laflamme, R. & Poulin, D. Unified and generalized approach to quantum error correction. *Phys. Rev. Lett.* **94**, 180501–(2005).
- Poulin, D. Stabilizer formalism for operator quantum error correction. *Phys. Rev. Lett.* **95**, 230504–(2005).



33. Gaitan, F. *Quantum Error Correction and Fault Tolerant Quantum Computing* (CRC, Boca Raton, 2008).
34. Kitaev, A. Fault-tolerant quantum computation by anyons. *Ann. of Phys.* **303**, 2 (2003).
35. Paz-Silva, G. A., Brennen, G. K. & Twamley, J. Fault tolerance with noisy and slow measurements and preparation. *Phys. Rev. Lett.* **105**, 100501– (2010).
36. Khodjasteh, K. & Lidar, D. A. Rigorous bounds on the performance of a hybrid dynamical-decoupling quantum-computing scheme. *Phys. Rev. A* **78**, 012355 (2008).
37. West, J. R., Lidar, D. A., Fong, B. H. & Gyure, M. F. High fidelity quantum gates via dynamical decoupling. *Phys. Rev. Lett.* **105**, 230503 (2010).
38. Khodjasteh, K., Lidar, D. & Viola, L. Arbitrarily accurate dynamical control in open quantum systems. *Phys. Rev. Lett.* **104**, 090501 (2010).
39. Yang, W., Wang, Z.-Y. & Liu, R.-B. Preserving qubit coherence by dynamical decoupling. *Front. Phys.* **6**, 2 (2011).
40. Paz-Silva, G. A., RezaKhani, A. T., Dominy, J. M. & Lidar, D. A. Zeno Effect for Quantum Computation and Control. *Phys. Rev. Lett.* **108**, 080501 (2012).
41. Dominy, J. M., Paz-Silva, G. A., RezaKhani, A. T. & Lidar, D. A. Analysis of the quantum Zeno effect for quantum control and computation. *ArXiv e-prints* (2012).
42. Nielsen, M. & Chuang, I. *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

Acknowledgments

This research was supported by the ARO MURI grant W911NF-11-1-0268, by the Department of Defense, by the Intelligence Advanced Research Projects Activity (IARPA) via Department of Interior National Business Center contract number D11PC20165, and by NSF grants no. CHE-924318 and CHE-1037992. The US Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of IARPA, DoI/NBC, or the US Government.

Author contributions

Initial results were obtained by G.P.S. Final results were derived through discussions involving both authors. Both authors contributed equally to the writing of the manuscript.

Additional information

Competing financial interests: The authors declare no competing financial interests.

License: This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/3.0/>

How to cite this article: Paz-Silva, G.A. & Lidar, D.A. Optimally combining dynamical decoupling and quantum error correction. *Sci. Rep.* **3**, 1530; DOI:10.1038/srep01530 (2013).