Symmetry boost of the fidelity of Shor factoring

Y. S. Nam and R. Blümel

Phys. Rev. A **97**, 052311 — Published 8 May 2018

DOI: 10.1103/PhysRevA.97.052311

Symmetry boosts Shor factoring fidelity

Y. S. Nam*

Joint Center for Quantum Information and Computer Science,

Institute for Advanced Computer Studies,

University of Maryland, College Park, MD 20910, USA

**now with IonQ Inc., College Park, MD 20740, USA*

R. Blümel

Department of Physics, Wesleyan University,

Middletown, Connecticut 06459-0155, USA

(Dated: April 17, 2018)

Abstract

In Shor's algorithm quantum subroutines occur with the structure $\mathcal{F}\mathcal{U}\mathcal{F}^{-1}$, where $\mathcal{F}$ is a unitary transform and $\mathcal{U}$ is performing a quantum computation. Examples are quantum adders and subunits of quantum modulo adders. In this paper we show, both analytically and numerically, that if, in analogy to spin echoes, $\mathcal{F}$ and $\mathcal{F}^{-1}$ can be implemented symmetrically when executing Shor's algorithm on actual, imperfect quantum hardware, such that $\mathcal{F}$ and $\mathcal{F}^{-1}$ have the same hardware errors, a symmetry boost in the fidelity of the combined $\mathcal{F}\mathcal{U}\mathcal{F}^{-1}$ quantum operation results when compared to the case in which the errors in $\mathcal{F}$ and $\mathcal{F}^{-1}$ are independently random. Running the complete gate–by–gate implemented Shor algorithm, we show that the symmetry-induced fidelity boost can be as large as a factor 4. While most of our analytical and numerical results concern the case of over- and under-rotation of controlled rotation gates, in the numerically accessible case of Shor's algorithm with a small number of qubits, we show explicitly that the symmetry boost is robust with respect to more general types of errors. While, expectedly, additional error types reduce the symmetry boost, we show explicitly, by implementing general off-diagonal SU(N) errors, $N = 2, 4, 8$, that the boost factor scales like a Lorentzian in δ/σ, where σ and δ are the error strengths of the diagonal over- and underrotation errors and the off-diagonal SU(N) errors, respectively. The Lorentzian shape also shows that, while the boost factor may become small with increasing δ, it declines slowly (essentially like a power law) and is never completely erased. We also investigate the effect of diagonal non-unitary errors, which, in analogy to unitary errors, reduce, but never erase the symmetry boost. Going beyond the case of small quantum processors, we present analytical scaling results that show that the symmetry boost persists in the practically interesting case of a large number of qubits. We illustrate this result explicitly for the case of Shor-factoring of the semiprime RSA-1024, where, analytically, focusing on over/underrotation errors, we obtain a boost factor of about 10. In addition, we provide a proof of the fidelity product formula, including its range of applicability.

PACS numbers: 03.67.Lx, 03.67.Ac

*Electronic address: nam@ionq.co

I. INTRODUCTION

The second half of the 20th century saw the advent of the information technology revolution. There is no doubt about its profound impact on just about every aspect of modern society. The technological innovation in computers and networks enabled us to achieve tasks previously thought to be impossible, such as weather forecast, telecommunication, the Global Positioning System, and online banking.

While the current classical technology is already impressive, yet another revolution has emerged: Quantum information technology [1]. Taking advantage of quantum superposition and entanglement, a quantum information device is expected to be more secure and faster than its classical counterpart. Epitomizing the former is Shor's algorithm [1, 2], which enables us to factor a semiprime $N = pq$, where p and q are prime numbers, exponentially faster than any classical algorithm known to date. Shor's algorithm is often associated with code-breaking, since semiprime factorization is the key technology needed to break the widely-employed Rivest-Shamir-Adleman (RSA) encryption scheme [1, 3].

Despite all the theoretically predicted tremendous powers of quantum information devices, we do encounter major challenges when it comes to a physical realization of these devices: Errors and defects. This is so, because quantum information processors are known to be susceptible to the detrimental effects of inexact gate operations and decoherence, especially for a quantum computer whose workings are based on exquisite control of quantum superposition and interference. An early list of the potentially dangerous physical mechanisms that may destroy the proper functioning of a quantum computer was compiled by Landauer [4], and much progress has been made to fight these adverse mechanisms over the past couple of decades. In particular, broadly speaking, there are four different classes of errors that may occur during the execution of a quantum algorithm on a quantum computer [5–22].

1. *Environmental decoherence errors.* This type of error is caused by unknown and uncontrollable noise sources, originating in the environment outside of the quantum computer. The paradigm here, in terms of quantum circuit terminology, is the bit-flip error, which can largely be handled by sophisticated quantum error correction circuitry. Most studies of quantum error correction, with few exceptions, consider bit-flip errors to occur during qubit idle times, which are then restored by quantum error-correction

circuitry. Excellent reviews of quantum error correction are available in the literature, for instance by Devitt et al. [5], Terhal et al. [6], Gottesman et al. [7], and Raussendorf et al. [8].

2. *Hardware errors.* This type of errors, sometimes called control errors, occur when control signals directed at a physical qubit, such as, e.g., laser pulses acting on a two-level qubit, consistently or randomly over- or under-rotate the phase of this qubit. As a specific example, let us consider a quantum computer represented as a unitary operator $\hat{Q}(\vec{\theta}_1, \vec{\theta}_2, \ldots, \vec{\theta}_M) = \prod_{j=1}^{M} \hat{U}_j^{(\tau_j)}(\vec{\theta}_j)$ in the form of a sequence of M gate applications, where $\hat{U}_j^{(\tau_j)}(\vec{\theta}_j)$ is the unitary operator representing gate type τ_j, j is the sequence number, and $\vec{\theta}_j$ are the ideal (ciruit-specified) control parameters that determine the action of gate number j. Specifying the initial state $|\phi_i\rangle$ of the quantum computer, $\hat{Q}(\vec{\theta}_1, \vec{\theta}_2, \ldots, \vec{\theta}_M)$ takes the initial state $|\phi_i\rangle$ into the final state $|\phi_f(\vec{\theta}_1, \vec{\theta}_2, \ldots, \vec{\theta}_M)\rangle$. Experimentally, because of unavoidable control errors, the control parameters will be different from quantum-computer run to quantum-computer run, i.e., $\vec{\theta}_j \to \vec{\vartheta}_j$, $|\phi_f\rangle \to |\varphi_f\rangle$, and we need to characterize the sensitivity of the output state $|\varphi_f(\vec{\vartheta}_1, \vec{\vartheta}_2, \ldots, \vec{\vartheta}_M)\rangle$ with respect to the perturbed control parameters $\vec{\vartheta}_j$. We do this by computing the fidelity. If we denote by $|\varphi_f^{(n)}\rangle$ the output state obtained after run number n, the fidelity is computed according to $F = \sum_{n=1}^{N} |\langle\varphi_f^{(n)}|\phi_f\rangle|^2/N$, where N is the number of runs. While each run number n yields a pure output state $|\varphi_f^{(n)}\rangle = |\varphi_f(\vec{\vartheta}_1^{(n)}, \vec{\vartheta}_2^{(n)}, \ldots, \vec{\vartheta}_M^{(n)})\rangle$, where the control parameters $\vartheta_j^{(n)}$ are the actual settings for this specific run, the output state of the combined ensemble of states produced by repeated runs of $\hat{Q}$ is a mixed state, best characterized by a density matrix [23] $\rho = \sum_{n=1}^{N} |\varphi_f^{(n)}\rangle\langle\varphi_f^{(n)}|/N$. Using this mixed-state density matrix, the fidelity is computed according to $F = \langle\phi_f|\rho|\phi_f\rangle$ and yields exactly the same result as before. Therefore, generating pure states, and then averaging, or viewing this process as a state-generation machine (a "beam") that generates a mixed state, produces identical results for the fidelity F. The mixed state will show a reduction of the "coherences" of the density matrix [23], i.e., a reduction of the sizes of the off-diagonal matrix elements of ρ with respect to the density matrix corresponding to the ideal settings $\vec{\theta}_j$ of the control parameters. This decoherence, a consequence of hardware errors, and fully included in our simulations, should not be confused with environmental decoherence,

as discussed in point 1 above: In the presence of environmental decoherence, a mixture results even after a single run of the quantum computer. Since, in general, different gate types are implemented with different hardware (for instance different laser pulse sequences), it makes sense to correlate hardware errors with gate types. We define *typed errors* according to $\vec{\vartheta}_j^{(n)} = \vec{\vartheta}_{j'}^{(n)}$ whenever $\tau_j = \tau_{j'}$. Without such correlation we call the hardware errors non-typed. We emphasize that the above discussion applies to typed as well as non-typed errors. Hardware errors, and how to counteract them in quantum processors realized with physical gates, are the main focus of this paper.

3. *Gate approximation errors.* Only a limited set of standard gates can be protected in a straightforward way by quantum error correction circuitry. Gates that cannot be protected easily need to be represented as products of more elementary, protectable gates. The longer the approximation sequence, the better a given gate is approximated by the sequence. However, for sequences of finite lengths, i.e., the only type that exists in an actual, physical realization of a quantum computer, a finite approximation error always remains. That these sequence approximations always converge largely rests on a theorem by Kitaev [24], and excellent reviews of the current state-of-the-art in sequence approximations and their resulting errors are available in the literature [9–11]. While, on the one hand, as mentioned above, longer gate approximation sequences result in smaller gate approximation errors, longer sequences, on the other hand, provide more chances for type-1 errors (decoherece) and type-2 errors (hardware errors) to counteract the desired improvement in the approximation of a specified target gate. Focusing on type-2 errors, it was shown in [25] that the tug-of-war between type-2 and type-3 errors leads to an optimum in the sequence length, i.e., under realistic conditions it is not always true that longer sequences lead to smaller errors. Analytical formulas for the optimal sequence length may also be found in [25].

4. *Loss.* This type of error, discussed, e.g., in [21, 22], occurs when the quantum computer loses information-carrying photons, phonons, or electrons. Thus, this type of error is a non-unitary error.

This list of quantum-error types helps to better contrast the hardware errors that we focus on in this paper with other types of errors not considered in this paper. In particular, in this paper, we focus on errors that most closely resemble type-2 errors, i.e., random over-

and under- rotations of the phases of qubits. As detailed in [25], *no quantum hardware is perfect*. Therefore, every single component of a quantum computer is necessarily flawed. It is impossible to build an ideal, mathematically precise gate. All physical equipment is limited by finite accuracy and precision. Consequently, even when protected by quantum error protection circuitry, as proved in [25], the resulting quantum computer, even if all gates are encoded, still contains random over- and under- rotations of the phases of qubits with certainty. Therefore, hardware errors are an important class of errors that we study in this paper with the help of several error models.

The impossibility of realizing mathematically perfect quantum gates in physical quantum computer implementations is not a trivial observation that can be dismissed without serious investigation. For instance, akin to the existence of exponential sensitivity to errors in classically chaotic systems [26], it may be possible that quantum computers are exponentially sensitive to hardware errors, which would immediately negate their potential exponentially superior performance with respect to classical hardware. While this, because of the linearity of quantum mechanics, may not be so, it may be discounted only after serious investigation. The fundamental fact that it is impossible to eliminate hardware errors provides the motivation. At the very least, the precise law of proliferation and scaling of hardware errors in large-scale quantum processors needs to be investigated in order to provide physicists and engineers with some benchmarks of how precisely particular quantum gates need to be realized to guarantee acceptable quantum computer performance. First steps in this direction, including analytical estimates, valid in the regime of a large number of qubits, have already been taken [25, 27–29].

Apart from their fundamental importance, there is another reason why we chose to focus on type-2 quantum hardware errors. In discussions with experimentalists at the University of Maryland, who are currently engaged in constructing a quantum computer, projected to be capable of demonstrating quantum supremacy [30] over classical computers, we learned that these researchers, for their quantum-computer architecture of choice (trapped-ion architecture [31, 32]), consider decoherence errors as secondary and hardware errors as primary in determining the limits of their quantum computers [33]. This evaluation is supported by the following general arguments. Previously, two-level systems were realized in the optical regime, where the coherence time is small due to the large transition frequency between the two levels. Now, however, moving into the direction of realizing the computational space in

terms of microwave transitions, the coherence time is much longer, of the order of minutes, simply because the frequency is reduced [34–36]. Therefore, for microwave-based implementations of quantum computers, decoherence, so far typically assumed and discussed in the literature as the most detrimental kind of error to occur in a quantum computer, is taking a back seat and the irremovable hardware errors are now the limiting factor that determines whether a quantum computer works or not.

Our paper is structured as follows. In Sec. II, keeping the above discussion in mind, we define our error models. In light of the above discussion, based on fundamental and physical grounds, we reiterate and emphasize the importance and significance of our error models. Then, in Sec. III, we present our results, demonstrating that the effect of hardware errors may be mitigated and counteracted by symmetry. In particular, we present our central result, i.e., symmetry is capable of boosting Shor factoring fidelity by significant factors. In Sec. IV we illustrate the symmetry boost with a concrete example: Shor factorization of the semiprime RSA-1024 [37]. This example illustrates two points. (a) Our analytical methods are powerful enough to cover the case of a large number of qubits and (b) that symmetry boosts of about an order of magnitude can be obtained even for a large quantum processor with qubit numbers in the thousands. While Secs. II - IV focus on the analytically treatable case of over- and under-rotations of the target qubits of controlled rotation gates, we show in Sec. V that the symmetry boost is robust and does not vanish if more general types of errors are considered. We discuss and conclude our paper in Sec. VI. Technical material is relegated to four appendices. In Appendix A, we derive two formulas that serve as the starting point for much of the discussion in Sec. III. In Appendix B, for the benefit of the reader, and to further emphasize why a distinction needs to be made between type-1 and type-2 errors, we constrast type-1 (decoherence) errors with type-2 (hardware) errors and show that they are indeed qualitatively different. In particular, we show that hardware errors *cannot* be treated in the same framework as we treat flip errors. Thus, the machinery available to treat decoherence errors is only of limited applicability when it comes to type-2 errors. We also show that depending on circumstances, hardware errors, as it turned out to be the case in connection with some of the most modern quantum computer implementations [34], may well be larger and more important than decoherence errors. In Appendix C we prove the fidelity product formula, frequently used in the literature (see, e.g., [38, 39]). In particular, we show in Appendix C that the fidelity product formula is only a first-order

result and state explicitly its range of applicability. In Appendix D we prove a formula we used in Sec. III.

II. METHODS

As a testbed algorithm we chose Shor's algorithm, implemented according to Beauregard's architecture [40]. We selected this particular architecture based on the facts that (i) Shor's algorithm is arguably the most interesting and most important quantum algorithm to date, (ii) the algorithm is complex enough to realistically capture the effects of flawed gates, and, most importantly, and exploited in this paper, (iii) Beauregard's architecture allows us to take advantage of symmetry. Whether some other Shor-algorithm architectures, such as those presented in [41] (and references therein), may be exploited in a similar fashion is currently under investigation and the results will be reported elsewhere.

Studies addressing the effects of errors and defects on a quantum computer running Shor's algorithm continue to be of central interest to many scientists. A list of early, notable contributions includes the investigations by Cirac and Zoller [31] studying the effect of errors in interaction time and laser detuning, Miquel *et al.* studying the effects of interactions with a dissipative environment [42] and phase drift errors [38], Wei *et al.* exploring the effects of coherence errors occurring while the quantum computer is idling [43], and García-Mata *et al.* [44] simulating static imperfections in Shor's algorithm. Recent developments in quantum simulation software [45–47] reflect the fact that quantum computers remain at the forefront of research. Our work extends this line of research in that we simulate the entire Shor algorithm, gate–by–gate. Based on this complete implementation of Shor's algorithm, we investigate the effects of errors in its phase-rotation gates.

We emphasize that our error model, to be defined and discussed below, reflects the effects of hardware errors that are unavoidable and guaranteed to occur in any hardware that exists in nature. This is so, because not even in principle does there exist physical equipment that meets mathematically exact circuit specifications. As a consequence, even if the quantum computer is protected with hardware implementing quantum error correction circuitry according to any quantum error correction protocol imaginable, each and every single physical quantum gate of the protection circuit will inevitably contain hardware errors itself. Thus, because hardware errors affect all qubits, including the qubits of the correction

circuitry, there is no type of hardware error that can be perfectly corrected. In fact, it can be shown (see Appendix B) that hardware errors, omnipresent everywhere in a realistic quantum computer, may be more significant than the commonly-addressed locally stochastic errors, often thought to be the most significant sources of instability of quantum computers. Our error model, therefore, includes the effects of physical errors, i.e. hardware errors, that are of prime importance for stable quantum computation and, as shown in Appendix B, may indeed be more important than local stochastic errors.

Since the most frequently used quantum gate in Beauregard's architecture of Shor's algorithm is a phase rotation gate

$$\theta_j^{(\pm)} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pm i\frac{\pi}{2^j}} \end{pmatrix}, \tag{1}$$

which appears $\sim 18L^4$ times throughout the algorithm [27] when using the minimally required number of qubits to factor a semiprime N whose bit-length is L, we tested the sensitivity of this quantum computer running Shor's algorithm with respect to errors in $\theta_j^{(\pm)}$. Specifically, we used a statistical error model of the rotation gate of the form [28]

$${}^{R}\theta_j^{(\pm)} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pm i\frac{\pi}{2^j}[1+\alpha^{(\pm)}]} \end{pmatrix}, \tag{2}$$

in the case where the errors scale according to the size of the gate operation and

$${}^{A}\theta_j^{(\pm)} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pm i\left[\frac{\pi}{2^j}+\alpha^{(\pm)}\right]} \end{pmatrix}, \tag{3}$$

in the case where the errors do not scale according to the size of the gate operation. In both cases $\alpha^{(\pm)}$ is the defect parameter that may or may not be (strongly) correlated with the gate type indexed with j. In case a one-to-one correlation exists, we call the error "typed" and replace $\alpha^{(\pm)}$ with $\alpha_j^{(\pm)}$. The $\pm$ sign corresponds to forward and backward operation.

The reason why we explicitly distinguish these two error models is as follows. First, any physically implemented gate has a finite accuracy, which may be characterized in terms of percentage error with respect to the desired gate operation. Since a rotation gate θ_j is built according to a gate-decomposition sequence (see references in [29]), the approximated rotation gate will contain errors that scale in the size of the operation, for example if θ_j is constructed by applying θ_{j+1} twice. This iteration method, i.e., constructing gates from more

basic, standardized building blocks, is realistic and even desirable from both the technological and economic perspectives. Thus, characterizing a device in terms of relative errors is captured by the ${}^{R}\theta_j^{(\pm)}$ model. However, suppose we characterize our physically implemented gate in terms of its technological limit, say δ. In this case, most likely, all gates will be constructed on the basis of different gate sequences, resulting in an error level $\lesssim \delta$. This is captured by our model ${}^{A}\theta_j^{(\pm)}$.

We now subdivide both models into three categories: (i) typed errors ($\alpha^{\pm} = \alpha_j^{\pm}$), asymmetric ($\alpha^{+} = -\alpha^{-}$); (ii) typed errors ($\alpha^{\pm} = \alpha_j^{\pm}$), symmetric ($\alpha^{+} = \alpha^{-}$); and (iii) non-typed errors, i.e., completely random $\alpha^{\pm}$. The three categories arise as follows. Typing results from using the same sequence, or the same physical device, for the same θ_j that occur multiple times throughout the entire Shor algorithm. Then, depending on the way that the physical device is implemented, since the backward gate is nothing but a unitary inverse of the forward gate, we may assume that the errors of the forward and backward gates are symmetric.

III. GENERAL ANALYTICAL AND NUMERICAL RESULTS

To start with, we simulate the case of factoring $N = 15$. This is the case used in [38], which allows us to compare our results with the results in [38]. Defining the fidelity $F = |\langle\Psi_{\text{actual}}|\Psi_{\text{ideal}}\rangle|^2$ as in [38], we plot, in Fig. 1, F as a function of σ, where the errors $\alpha^{(\pm)}$ are Gaussian-distributed random variables with mean 0 and standard deviation σ. Consistent with the results presented in [38], the fidelity F of Shor's algorithm follows the form $F = \exp(-\gamma\sigma^2)$ for small σ. Figure 1 shows that the performance of the quantum computer improves in the order of asymmetric, random, and symmetric errors. To quantify, we observe that, corresponding to $F = \exp(-\gamma\sigma^2)$, the smaller γ, the larger the fidelity. Numerically, in the case of relative errors, we obtain ${}^{R}\gamma^{(\text{asym})} = 46512$, ${}^{R}\gamma^{(\text{rand})} = 1937$, and ${}^{R}\gamma^{(\text{sym})} = 416$, for asymmetric, random, and symmetric errors, respectively. In the case of absolute errors, we obtain ${}^{A}\gamma^{(\text{asym})} = 20909$, ${}^{A}\gamma^{(\text{rand})} = 664$, and ${}^{A}\gamma^{(\text{sym})} = 184$, respectively. Clearly, for both relative and absolute errors the numerical results follow the progression asymmetric, random, symmetric in terms of fidelity improvement as already noticed graphically in Fig. 1. In order to quantitatively characterize the symmetry boost in

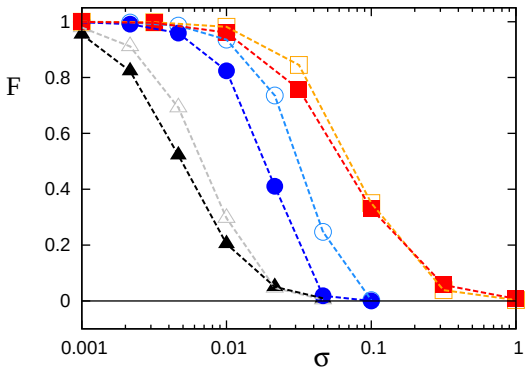

FIG. 1: Fidelity F of a quantum computer factoring $N = 15$ with seed 2 as a function of standard deviation σ of the logical-gate errors. The quantum computer is equipped with adders that are suitable for use in Shor-algorithm factoring of at most 4-bit semiprimes. Shown are the cases of typed, asymmetric errors (triangles), typed, symmetric errors (squares), and non-typed, random errors (circles). Filled plot symbols (red, blue, and black) denote relative errors [see Eq.(2)] and the open plot symbols (orange, cyan, and grey) denote absolute errors [see Eq.(3)]. Dashed lines connecting plot symbols are drawn to guide the eye. The solid, horizontal line corresponds to $F = 0$.

fidelity, we choose the random-error case as our standard and define the boost factor

$$\beta = \gamma^{(\mathrm{rand})}/\gamma^{(\mathrm{sym})}. \tag{4}$$

For the case of relative errors shown in Fig. 1 ($N = 15$), we obtain the boost factor ${}^{R}\beta = {}^{R}\gamma^{(\mathrm{rand})}/{}^{R}\gamma^{(\mathrm{sym})} = 1937/416 = 4.6$. In the case of absolute errors we obtain ${}^{A}\beta = {}^{A}\gamma^{(\mathrm{rand})}/{}^{A}\gamma^{(\mathrm{sym})} = 664/184 = 3.6$. These numbers show that choosing the correct error symmetry class results in an improvement of quantum-computer fidelity. Had we chosen the asymmetric symmetry class for implementing errors, instead of a fidelity boost we would have obtained a fidelity bust of a factor ${}^{R}\tilde{\beta} = {}^{R}\gamma^{(\mathrm{rand})}/{}^{R}\gamma^{(\mathrm{asym})} = 1937/46512 = 0.042$ in the relative-error case and ${}^{A}\tilde{\beta} = {}^{A}\gamma^{(\mathrm{rand})}/{}^{A}\gamma^{(\mathrm{asym})} = 664/20909 = 0.032$ in the absolute-error case. This shows clearly that (i) the fidelity of the quantum computer reacts sensitively to the correct choice of symmetry class and that (ii) for the correct choice of symmetry class an improvement of the performance of the quantum computer is obtained. In particular, in the relative-error case, the factor 4.6 improvement in γ would allow for about a factor 2

larger σ.

The important question to ask now is whether the symmetry-driven fidelity boost will persist as we scale up the quantum circuitry, i.e., in the limit of a large number of qubits. To start with, we compare the expected fidelities from naively multiplying the fidelities of the basic building blocks of Shor's algorithm, i.e., the quantum adders. This product formula of fidelities has been shown in [38] to work well in the non-typed cases (see also Appendix C).

For an $(L+1)$-bit sized quantum adder, capable of executing $s+a$, where s and a are integers of bit lengths $\leq L$, the phase Φ associated with $s+a$ in the *symmetric case* is given by

$$\Phi_{s,a}(l) = \frac{1}{2^{L+1}}\left[1+\exp\left(i\left\{\left[\sum_{\nu=0}^{L-1} k_\nu r_{L-\nu}\right]\right\}\right)e^{2\pi i(s+a-l)/2^{L+1}}\right]W_{s,a}(l), \tag{5}$$

where $k_\nu = s_{[\nu]} + a_{[\nu]} - l_{[\nu]}$ ($s_{[\nu]}$, e.g., denotes the νth binary digit of s),

$$W_{s,a}(l) = \sum_{l'=0}^{2^L-1} \exp\left[i\left(\sum_{m=0}^{L-1} l'_{[L-1-m]}\left\{a_{[m]}r_0 + \left[\sum_{\nu=0}^{m-1} k_\nu r_{m-\nu}\right]\right\}\right)\right]e^{2\pi i(s+a-l)l'/2^L}, \tag{6}$$

r_j may be α_j or $(\pi/2^j)\times\alpha_j$ if the errors are of the absolute kind or of the relative kind, respectively, and l is the output integer. Equations (5) and (6) are derived in Appendix A.

The non-typed error cases are obtained by removing correlations via letting each term in k_ν be associated with individual random terms, followed by removing typing of errors associated with the subscript j of r_j.

Calculating now the fidelity of the quantum adder $F_{\text{adder}} = |\Phi_{s,a}(l=s+a)|^2$, using (5) and (6), and assuming that the central limit theorem holds, we find, in the limit that L is large and σ is small,

$${}^R\beta_{\text{adder}} = \frac{\langle \ln {}^R F_{\text{adder}}^{(\text{rand})}\rangle_{s,a}}{\langle \ln {}^R F_{\text{adder}}^{(\text{sym})}\rangle_{s,a}} = 1.35, \qquad {}^A\beta_{\text{adder}} = \frac{\langle \ln {}^A F_{\text{adder}}^{(\text{rand})}\rangle_{s,a}}{\langle \ln {}^A F_{\text{adder}}^{(\text{sym})}\rangle_{s,a}} = 1.20, \tag{7}$$

where, assuming $F\sim\exp(-\gamma\sigma^2)$, the logarithm extracts the γ value, and, in analogy to the boost-factor definitions above, we defined ${}^R\beta_{\text{adder}}$ and ${}^A\beta_{\text{adder}}$ as the adder boost factors for relative errors and absolute errors, respectively. $F_{\text{adder}}^{(\text{rand})}$ is the adder fidelity in the random, non-typed case, and $F_{\text{adder}}^{(\text{sym})}$ is the adder fidelity in the case of symmetric errors.

We see from (7) that exploiting symmetry in our circuitry improves the fidelity of the quantum computer. In particular, the symmetry-driven boost always exists, outperforming the average fidelity of the non-typed, random cases in all cases, even for large numbers of

qubits. The complete Shor algorithm contains many adders. However, since the fidelity of successive applications of adders is approximately given by the product of the individual adders (see Appendix C), the Shor fidelity inherits the symmetry boost of the individual adders and we expect that the symmetry-driven fidelity boost persists in large-scale quantum circuits that are of practical interest. This is indeed confirmed explicitly in Sec. IV, where we obtain large symmetry boosts in the case of RSA-1024 factoring.

Now, the observed boost factors of 4.6 in the relative error case and 3.6 in the absolute error case in Fig. 1 are larger than what is expected from (7). This motivates us to find additional boost mechanisms that are not cpatured by the naïve adder-fidelity product approximation of the Shor processor fidelity. While we were not able to pin down all boost mechanisms, we present in the following the one that is based on the next-level-up building blocks, namely the modulo addition gates.

To start, we point out that a modulo-addition gate consists of five adders and an auxiliary qubit (see, e.g., Fig. 5 of [40]). For an input integer value of s, a quantum modular addition of $s + a \bmod N$ may be performed by first adding a then subtracting N, followed by a conditional operation of adding back N if $s + a < N$, which may be done with the help of an auxiliary qubit. This completes the computational part of the modular addition. In order to now unitarily restore and decouple the auxiliary qubit that is at this point in its conditional state (depending on the relation between $s + a$ and N), two additional adders that subtract and add a, respectively, are used. We refer to this step as the recovery part of the modular addition.

According to whether the conditional addition of N is triggered or not, we consider two cases, i.e., (i) $s + a < N$ and (ii) $s + a \geq N$. In the former case, because of the triggering, the modulo-addition circuit attains a symmetric substructure, denoted by the solid lines in Fig. 2. Thus, motivated by the existence of the highly organized structure and in the limit of small errors, we write the fidelity of a modulo-addition gate in case (i) as $F^{(\mathrm{i})} \approx F_{\mathrm{s.s.}} F^{(a)}_{\mathrm{adder}}$, where $F_{\mathrm{s.s.}}$ denotes the fidelity associated with the symmetric substructure and $F^{(a)}_{\mathrm{adder}}$ denotes the fidelity of the last adder with addend a in Fig. 2, all equipped with symmetric noise. In the latter case, the auxiliary qubit is not turned on, resulting in the modulo addition gate fidelity of case (ii) $F^{(\mathrm{ii})} \approx F^{(-N)}_{\mathrm{adder}} F^{(a)}_{\mathrm{adder}}$, assuming that, in the limit of small errors, the errors commute and thus the errors associated with the first adder of the computational part of the modulo addition gate approximately cancel those associated with the first adder

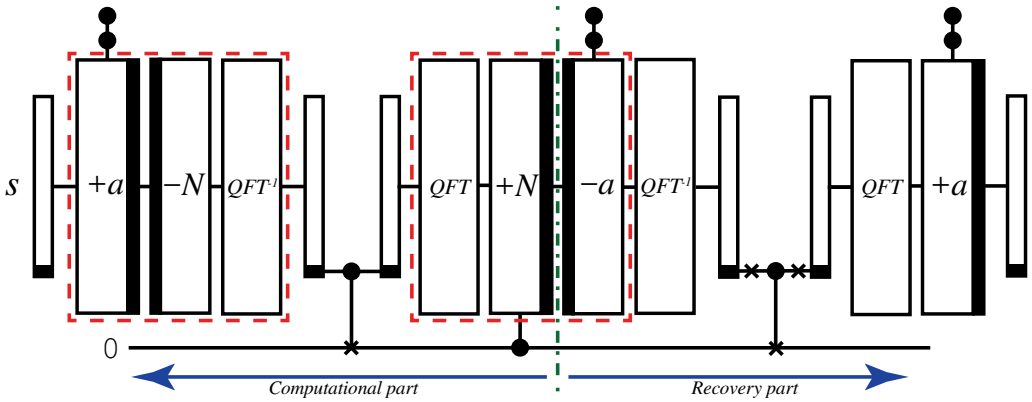

FIG. 2: Modulo addition gate circuit diagram, inspired by Fig. 5 of [40]. Circles denote controlling qubits and Xs denote NOT gates. Thick black bars identify adders and subtractors, i.e., bar-right for adders and bar-left for subtractors. Black solid squares in the qubit registers (denoted by thin rectangles), denote the most significant digit qubit of the register. All additions and subtractions are performed in the Fourier space. Dashed, red boxes enclose the symmetric parts used in the derivation of $F_{\text{s.s.}}$ discussed in the text. The vertical dash-dot, green line denotes the border between computational and recovery parts of the modulo addition circuit.

(subtractor) of the recovery part of the modulo addition gate.

At this point we notice that the only unknown term is $F_{\text{s.s.}}$, since the fidelity of the quantum adder has already been discussed earlier in this paper. Therefore, we now focus on $F_{\text{s.s.}}$.

Defining P_{remain} as the probability of obtaining the ideal bit value of the most significant qubit right after the first box in Fig. 2, one may show (see Appendix D)

$$F_{\text{s.s.}} = P_{\text{remain}}^2. \tag{8}$$

Now, $P_{\text{remain}} = \sum_{l>2^L} |\Phi_{s,a-N}(l)|^2$, where $\Phi_{s,a-N}$ is nothing but (5) with $a_{[\nu]} \to a_{[\nu]} - N_{[\nu]}$ and $a \to a - N$. In fact, we may, up to a phase, write $\Phi_{s,a-N}(l)$ as $\cos[\pi(s + a - N - l)/2^{L+1} + \sigma^{(\nu)}/2]|W_{s,a-N}|/2^L$, where $\sigma^{(\nu)}$ is the sum in the exponent in (5). The remaining term is $|W_{s,a-N}|$, which we analyze next.

In order to gain analytical insight, we consider $s = 0$, $a = 0$, and $l = -N$. In this case, W has a structure where aligned phasors add up with small phase-angle perturbations of the form $\sum_m -l'_{[L-2-m]} N_{[m]} \pi r_0$. In all other cases ($l \neq -N$), the phasors interfere destructively

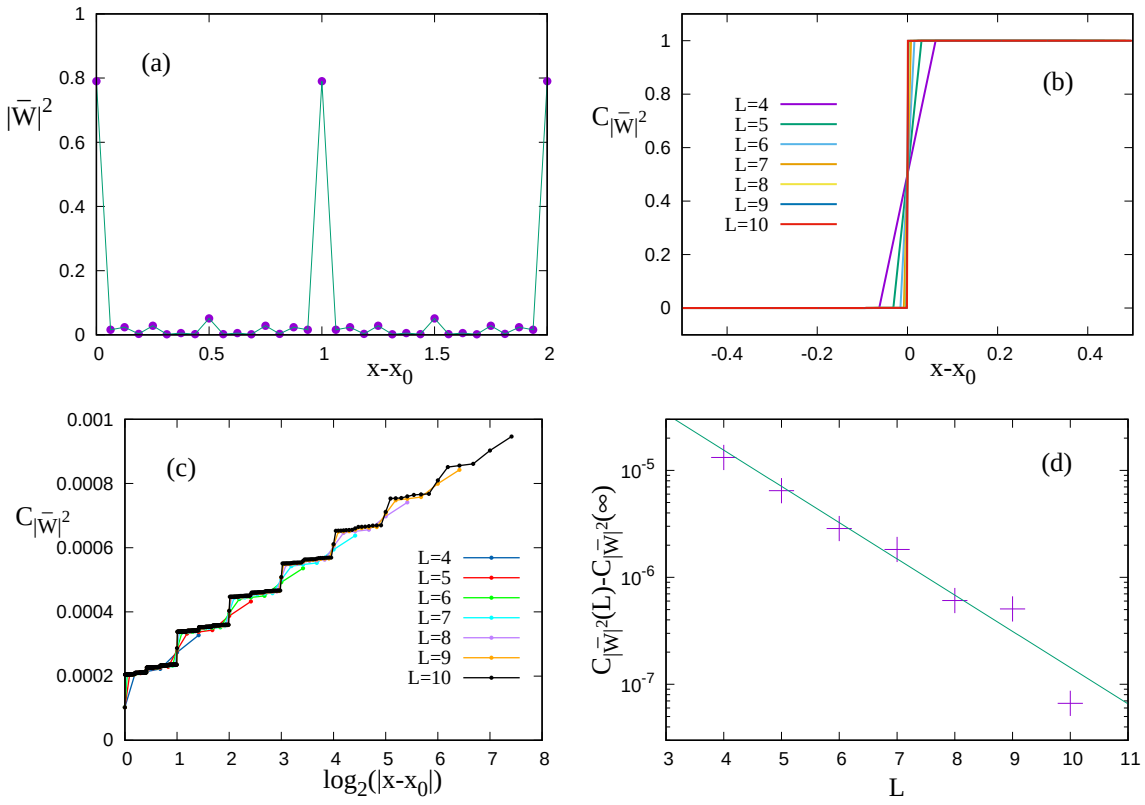

FIG. 3: Various quantities related to $|\bar{W}|^2 = \langle |W_{s,a}|^2 \rangle_{s,a}$, i.e., the average over the amplitudes squared of $W_{s,a}$, defined in (6), over all possible 4-bit computations $s+a$, $0 \leq s \leq 15$, $0 \leq a \leq 15$. (a) shows $|\bar{W}|^2$ as a function of $x - x_0 = (l - l_0)/16$ for $\sigma = 0.2$. (b) shows the corresponding cumulatives of $|\bar{W}|^2$, i.e., $C_{|\bar{W}|^2}(x = l/2^L) = \sum_{l'<l}[|\bar{W}(l')|^2 + |\bar{W}(l'+1)|^2]/2$, for various different L, ranging from $L = 4$ to $L = 10$. The steeper the slope of the lines at the transition point $x - x_0 = 0$, the larger L. (c) shows $C_{|\bar{W}|^2}$ for $\sigma = 0.01$ as a function of $|\log_2[|x - x_0|]|$ for the same range of L values as in (b), i.e., $L = 4, \ldots, 10$. The better the agreement with the steps, the larger L. (d) Exponential convergence of $C_{|\bar{W}|^2}$ in L for all x is illustrated here for the special case $\log_2[|x - x_0|]| = 1$. Purple plot symbols: Numerical simulations. Solid, green line: Exponential fit to the numerical results.

with the additional perturbation of the ν-sum in (6). Now, because the interference without noise is perfect, the existence of the perturbation gives rise to an imperfect interference with nonzero result. Thus, the nature of the imperfection determines $|W|$. We find that [see Fig. 3 (a)-(c) for sample cases with $N = 2^L - 1$ and relative errors] whenever the Hamming

distance between $-N$ and l is 1 (or small), i.e., $|l-(-N)| = 2^{\mu}$, where μ is an integer, the magnitude $|W_{l,N}|$ is relatively large (compared to $|l-(-N)| \neq 2^{\mu}$). This is consistent with our analytical understanding that the more k_{ν}'s become non-zero, the more randomness is introduced to the perturbation angle, resulting once again in destructive interference, but this time of a statistical nature. In fact, we confirm its manifestation in the modulo addition $0+0 \bmod N$ fidelity F for all odd semiprimes $N < 2^{13}$, as shown in Figs. 4 (a) and (b). Semiprimes N between 2^j and 2^{j+1} are sectioned into different F-bands, arising from the bit-spectra of different N values, i.e., the binary digit 1 in the digit spectrum of N triggers the corresponding noisy rotation gate operation.

We also notice that, based on Fig. 3 (c), $|W|$ is localized in l. This is expected, since the form of W in (6) remains the same as a function of L, while the associated cumulative errors are bounded due to the exponential scaling of the error terms in L. In fact, the sum of $|W|^2$ for $|l-N| < 2^L$ equals 1 [see Fig. 3 (b)], where $W(l) = W(l+2^L)$. We explicitly confirm numerically that the convergence toward the limiting, localized distribution is exponentially better for increasing L [see Fig. 3 (d)].

Together with the observed localization, we find P_{remain} to be constant as a function of increasing L ($\sigma^{(\nu)}$ is bounded). This is consistent with the plateau behavior observed in Fig. 4 (c), in which, to highlight the result shown in Fig. 4 (a), we averaged F over N in logarithmic scale, i.e., $2^j < N < 2^{j+1}$ for $j = 3, 4, \ldots, 12$, and plot the results [see Fig. 4 (d) for the average results for Fig. 4 (b)]. In contrast to the relative kind of errors, the case of absolute errors is known to have a fidelity scaling that is one power less favorable in L in the exponent of fidelity (see, e.g., [48]), and this is manifestly visible in Fig. 4 (d). In addition, Fig. 4 shows that the fidelity does not monotonically increase with the number of extra qubits. This is surprising and may be relevant to circuit design.

Following the localization result demonstrated in Figs. 3 (c) and (d), assuming the fidelity F_{adder} of a quantum adder predicts the limiting distribution to a very good approximation, we may write

$$|D(x;x_0)|^2 \approx \frac{\eta}{2\ln(2)|x-x_0|} e^{\eta+\eta\log_2(|x-x_0|)}. \tag{9}$$

Here, $x = l/2^L$ and $x_0 = l_0/2^L$, where l_0 is the ideal output. We used $F_{\text{adder}} = e^{-\eta L}$ from [48], where η is a constant. Approximating now the sum over $l > 2^L$ in P_{remain} as an integral,

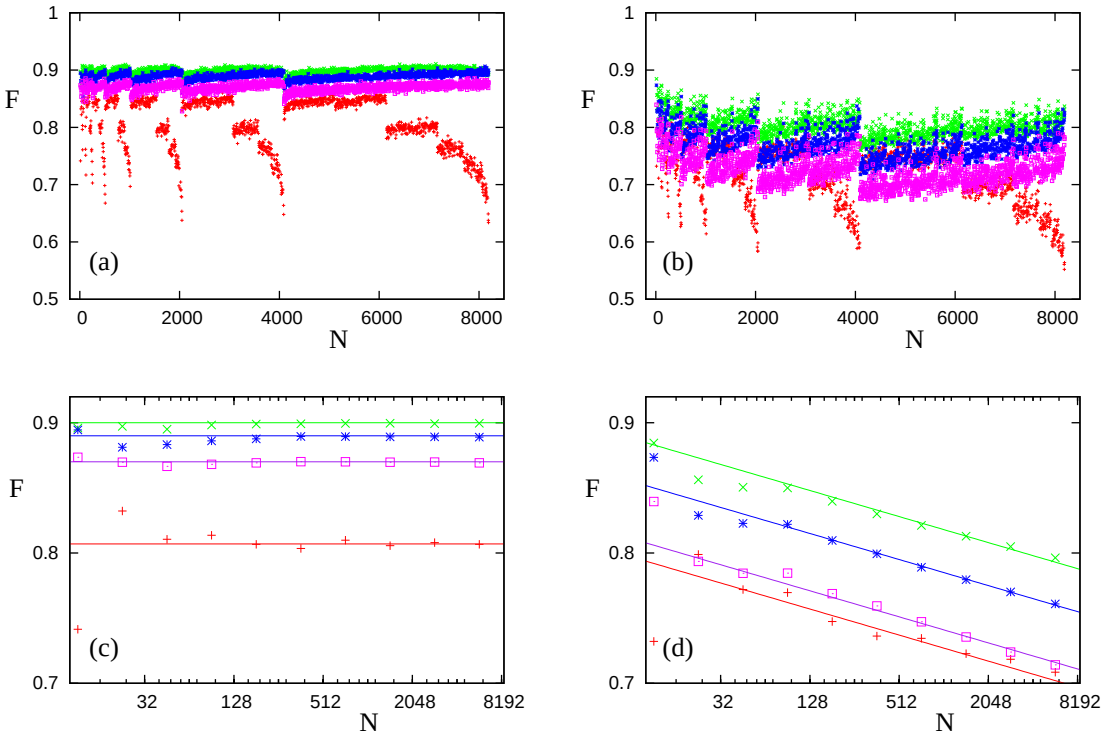

FIG. 4: Fidelity F of a modulo-addition gate performing $0 + 0 \bmod N$, where N is a semiprime. Frames (a) and (b) show F as a function of all odd semiprimes $N < 2^{13}$ for relative and absolute symmetric errors, respectively. The error strength used is $\sigma = 0.2$. In the order of pluses (red), crosses (green), asterisks (blue), and squares (purple), the adders are equipped with 0, 1, 2, and 3 additional qubits than minimally required. Frames (c) and (d) show logarithmically averaged F, i.e., each point plotted at $2^{j+1/2}$ is the result of averaging over N from 2^j to 2^{j+1}, where $3 \leq j \leq 12$. Notice that for $j = 3$ and $j = 4$, there is only one semiprime each, namely, 15 and 21, respectively, resulting in larger fluctuations due to insufficient statistics. Solid lines in Frame (c), with corresponding color symbols, are the tail-region fit lines $F = 0.807$ [red pluses; bottom solid (red) line], $F = 0.9$ [green crosses; top solid (green) line], $F = 0.89$ [blue asterisks; second solid (blue) line from the top], and $F = 0.87$ [purple squares; third solid (purple) line from the top]. Solid lines in Frame (d), with corresponding color symbols, are the tail-region fit lines (to first order) $F = -0.01 \log_2(N) + k$, where $k = 0.827$ [red pluses; bottom solid (red) line], $k = 0.918$ [green crosses; top solid (green) line], $k = 0.885$ [blue asterisks; second solid (blue) line from the top], and $k = 0.841$ [purple squares; third solid (purple) line from the top] for the four cases shown.

together with $|D(x;x_0)|$ in (9), we obtain

$$P_{\text{remain}} \approx \int_0^1 \cos^2\left[\frac{\pi(x-x_0)}{2}\right] |D(x;x_0)|^2 dx, \tag{10}$$

where we assumed $\sigma^{(\nu)}$ is small. This completes our analytical calculation for the only unknown term $F_{\text{s.s.}}$.

Equipped with our analytical fidelity scaling formulas, we once more check for the symmetry-driven fidelity boost. For a sufficiently large quantum circuit, such as Shor's algorithm factoring large semiprimes that are of practical interest, the input s of a modulo addition gate performing $s + a \bmod N$ may range anywhere between 0 and $N-1$. This results in an approximately 50/50 chance of (i) $s + a < N$ and (ii) $s + a \geq N$, assuming a random s and a uniformly distributed between 0 and $N-1$. Thus, we expect the average fidelity $F_{\text{add-mod}}$ of a modulo addition gate to be $0.5[F^{(\text{i})} + F^{(\text{ii})}]$. Now, the addition of the addend a of the modulo addition $s + a \bmod N$ occurs with probability 1/4, assuming random bit values of the two controlling qubits of the addition (see Fig. 5 of [40] for detail). Therefore, assuming once again that the product formula of fidelity holds, this time applied to the modulo addition gate, of which there are $4L^2$ in one complete run of Shor's algorithm, we obtain the symmetric-noise Shor fidelity

$$F_{\text{Shor}}^{(\text{Sym})} = F_{\text{add-mod}}^{4L^2} = \left(\frac{3}{4}F_{\text{s.s.}} + \frac{1}{4}\left[\frac{F_{\text{s.s.}}F_{\text{adder}} + F_{\text{adder}}^2}{2}\right]\right)^{4L^2}. \tag{11}$$

This may be compared to

$$F_{\text{Shor}}^{(\text{rand})} = \left[\frac{3}{4}(F_{\text{adder}})^2 + \frac{1}{4}(F_{\text{adder}})^5\right]^{4L^2} \tag{12}$$

for the non-typed error counterpart. The two estimates (11) and (12) do not include the period finding part, since, in the regime where the modulo exponentiation part works with acceptable performance, the fidelity decrease caused by the period finding part of Shor's algorithm is negligible [27, 28, 48, 49]. Importing F_{adder} from Equation (19) of [48], we obtain, for instance, ${}^{R}F_{\text{Shor}}^{(\text{rand})} = 79\%$ for $\sigma = 0.01$ and $L = 4$ to leading order in L in the exponent of F_{adder}, in excellent agreement with Fig. 1. An equivalent computation for the symmetric case based on (11), together with a proper normalization of (9), i.e., $\int |D|^2 dx = 1$, results in 89%, which is in satisfactory agreement with the simulation results shown in Fig. 1.

We also note that we observe an extra boost of fidelity when we introduce more qubits to the quantum circuit than necessary (see Fig. 5). We find the smallest subcircuit that

exhibits such an extra boost to be the modulo addition gate, whose fidelity as a function of the number of extra qubits ΔL appears in Figs. 5 (c) and (d). In fact, in Fig. 3, different color symbols represent different numbers of extra qubits used in the modulo-addition gate, clearly indicating the presence of this extra boost.

A simple analytical analysis may be performed on the modulo-addition gate based on our previous results, in order to show this extra boost exhibited in Figs. 5 (c) and (d). To a good approximation, the limiting distribution $|D(x;x_0)|^2$ in (9), in the limit of small σ, may be approximated as a delta-peak centered at the ideal output x_0 with a uniform distribution throughout the rest of the domain of the integral in (10), such that $\int |D(x;x_0)|^2 dx = 1$. Now, W in (6) shows that increasing L, while keeping addends the same, does not change W for an ideal output. Thus, together with $|D(x,x_0)|^2 \approx F_{\text{adder}}\delta(x-x_0) + (1-F_{\text{adder}})$ for $x \in [0,1)$, we obtain $P_{\text{remain}} \approx F_{\text{adder}} + (1-F_{\text{adder}})[0.5+\sin(\pi x_0)/\pi]$, where $x_0 = N/2^{L_{\min}+\Delta L}$. Using this formula for P_{remain} in $F_{\text{s.s.}} = P_{\text{remain}}^2$, the fidelity shows a clear extra-boost behavior as a function of ΔL, demonstrating the power of our analytical model.

IV. SPECIFIC EXAMPLE: FACTORING RSA-1024

In this section we present a specific example, illustrating the symmetry boost for a large-scale quantum processor consisting of about 1,000 qubits. In particular, we use Shor factorization of the semiprime RSA-1024 [37], applying our analytical formulas derived in the preceding section to predict processor fidelities and boost factors in the regime of a large number of qubits. RSA-1024, to our knowledge, has not been factored yet, and the following estimates concerning necessary hardware accuracy and obtainable symmetry boost factors may provide guidance as to the feasibility of factoring this semiprime with a quantum computer.

For relative errors, the symmetry boost factor, ${}^R\beta$, is given by [see (7)]

$$ {}^R\beta = \frac{\ln\langle {}^R F_{\text{Shor}}^{(\text{rand})} \rangle_{s,a}}{\ln\langle {}^R F_{\text{Shor}}^{(\text{sym})} \rangle_{s,a}}, \tag{13} $$

where, according to (11) and (12),

$$ {}^R F_{\text{Shor}}^{(\text{sym})} = {}^R F_{\text{add-mod}}^{4L^2} = \left[\frac{3}{4} {}^R F_{ss} + \frac{1}{8} \left({}^R F_{ss} \, {}^R F_{\text{adder}}^{(\text{sym})} + {}^R F_{\text{adder}}^{(\text{sym})^2} \right) \right]^{4L^2} \tag{14} $$

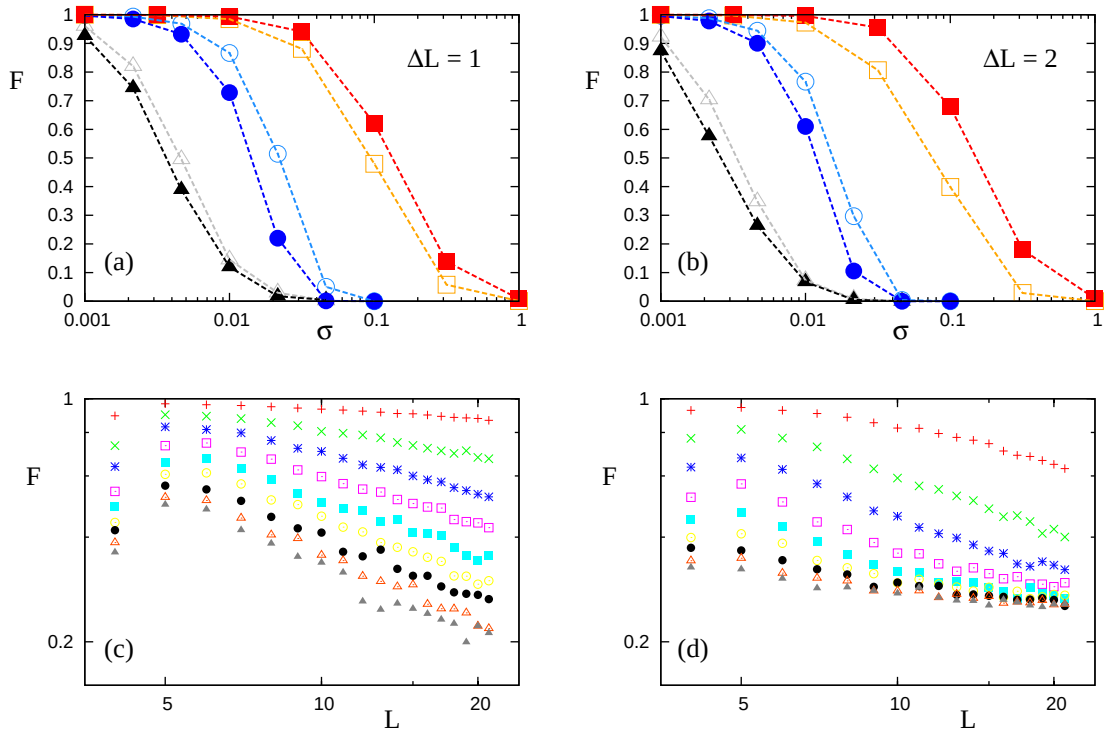

FIG. 5: Fidelity F of quantum computers running Shor's algorithm [(a) and (b)], and a modulo addition gate [(c) and (d)]. In the order of (a) and (b), the quantum computer is equipped with adders that are capable of being used in Shor-algorithm factoring of 5- and 6-bit semiprimes. Compared to Fig. 1, the boost from symmetrized errors is more significant when factoring 15, as shown. Frames (c) and (d) show F as a function of the bit-length L of the maximal semiprime that may be factored using a modulo-addition gate, equipped with relative and absolute symmetric errors, respectively. All cases were performed with $N = 15$. In decreasing order of F, different plot symbols refer to $\sigma = 0.1, 0.2, \ldots, 0.9$.

and

$$ {}^{R}F_{\text{Shor}}^{(\text{rand})} = \left[\frac{3}{4}\left({}^{R}F_{\text{adder}}^{(\text{rand})}\right)^2 + \frac{1}{4}\left({}^{R}F_{\text{adder}}^{(\text{rand})}\right)^5\right]^{4L^2}. \tag{15} $$

The fidelity ${}^{R}F_{\text{adder}}^{(\text{rand})}$ in (15) is given by [see [48], equation (19)]

$$ {}^{R}F_{\text{adder}}^{(\text{rand})} = \exp\left\{-\left[\frac{6\pi^2(3n-4)}{144} + \frac{\lambda_r n\pi^2}{4}\right]\sigma^2\right\}, \tag{16} $$

where $n = L + 1$ and L is the bit length of the semiprime to be factored. In our case, factoring RSA-1024, we have $L = 1024$. Using $n = 1025$ and $\lambda_r = 0.6$ [48] in (16), we arrive

at

$$ {}^{R}F_{\text{adder}}^{(\text{rand})} = \exp\left[-\left({}^{R}\gamma_{\text{adder}}^{(\text{rand})}\right)\sigma^2\right], \tag{17} $$

where

$$ {}^{R}\gamma_{\text{adder}}^{(\text{rand})} \approx 2778. \tag{18} $$

At this point a crucial question arises: What is the minimum harware accuracy required to factor RSA-1024 with reasonable fidelity? If it turns out that the required accuracy is orders of magnitude smaller than can possibly be realized with the most sophisticated equipment, we would have proved right here that Shor factoring of semiprimes of practical significance is impossible in practice. This statement would be independent of considering decoherence as an additional effect, since decoherece would only make matters worse. Fortunately, this is not so, and we can prove instead that hardware errors are a significant, but not an insurmountable obstacle to Shor factoring of RSA-1024.

In order to obtain a reasonably large fidelity for ${}^{R}F_{\text{Shor}}^{(\text{rand})}$, we need a reasonably large fidelity of ${}^{R}F_{\text{adder}}^{(\text{rand})}$, and therefore, according to (17), we necessarily need that ${}^{R}\gamma_{\text{adder}}^{(\text{rand})}\sigma^2$ is small. In this case we may linearize ${}^{R}F_{\text{adder}}^{(\text{rand})}$ to obtain

$$ {}^{R}F_{\text{adder}}^{(\text{rand})} = 1 - {}^{R}\gamma_{\text{adder}}^{(\text{rand})}\sigma^2. \tag{19} $$

Using this in (15), and once more expanding to linear order, we obtain

$$ {}^{R}F_{\text{Shor}}^{(\text{rand})} \approx 1 - 11\,{}^{R}\gamma_{\text{adder}}^{(\text{rand})}L^2\sigma^2 = 1 - 3.2\times 10^{10}\sigma^2. \tag{20} $$

Apparently, in order to obtain ${}^{R}F_{\text{Shor}}^{(\text{rand})}$ close to 1, we need

$$ \sigma < 6\times 10^{-6}. \tag{21} $$

This is a demanding accuracy to achieve in practice, but it is not impossible (much better accuracies are achieved, e.g., in atomic and ionic clock applications [50]). Therefore, we conclude that Shor factorization, as far as hardware errors are concerned, is certainly possible.

At this point we have computed ${}^{R}F_{\text{adder}}^{(\text{rand})}$ and ${}^{R}F_{\text{Shor}}^{(\text{rand})}$ together with the required hardware accuracy σ. To complete the computation of the symmetry boost factor ${}^{R}\beta$, we now need to compute ${}^{R}F_{\text{Shor}}^{(\text{sym})}$ in (14). This computation requires knowledge of ${}^{R}F_{ss}$ and ${}^{R}F_{\text{adder}}^{(\text{sym})}$.

The fidelity ${}^{R}F_{ss}$ in (14), according to (8), is given by

$$ {}^{R}F_{ss} = {}^{R}P_{\text{remain}}^{2}, \tag{22} $$

where, according to (10),

$$ {}^{R}P_{\text{remain}} \approx \int_0^1 \cos^2\left[\frac{\pi(x-x_0)}{2}\right] |{}^{R}D^{(\text{sym})}(x;x_0)|^2 dx, \tag{23} $$

and ${}^{R}D^{(\text{sym})}(x;x_0)$, according to (9), is given by

$$ {}^{R}D^{(\text{sym})}(x;x_0) \approx \frac{\eta e^{-\eta}}{2\ln(2)|x-x_0|} e^{\eta \ln(|x-x_0|)/\ln(2)}, \tag{24} $$

where η is defined according to

$$ {}^{R}F^{(\text{sym})}_{\text{adder}} \approx e^{-\eta L}. \tag{25} $$

We expect that ${}^{R}F^{(\text{sym})}_{\text{adder}}$ will be very close to 1, in which case $\eta L \ll 1$, which means that $\eta \ll 1/L \approx 10^{-3}$. In this case, we can use the fact that

$$ \lim_{\eta\to 0} {}^{R}D^{(\text{sym})}(x;x_0) = \delta(x-x_0), \tag{26} $$

perform the integral in (23), and obtain ${}^{R}P_{\text{remain}} = 1$, which implies ${}^{R}F_{ss} = 1$. The only remaining term in (14) is ${}^{R}F^{(\text{sym})}_{\text{adder}}$, explicitly given by

$$ {}^{R}F^{(\text{sym})}_{\text{adder}} = \exp\left\{-\left[\frac{5\pi^2(3n-4)}{144} + \frac{\lambda_s n \pi^2}{4}\right]\sigma^2\right\}. \tag{27} $$

Linearizing with $n = L+1 = 1025$ and $\lambda_s = 0.4$, we obtain

$$ {}^{R}F^{(\text{sym})}_{\text{adder}} = \exp\left[-\left({}^{R}\gamma^{(\text{sym})}_{\text{adder}}\right)\sigma^2\right], \tag{28} $$

where

$$ {}^{R}\gamma^{(\text{sym})}_{\text{adder}} = 2064. \tag{29} $$

With this result, and using ${}^{R}F_{ss} = 1$ in (14), we now obtain, in linear order,

$$ {}^{R}F^{(\text{sym})}_{\text{Shor}} = 1 - \frac{3}{2}{}^{R}\gamma^{(\text{sym})}_{\text{adder}} L^2\sigma^2. \tag{30} $$

With this result, together with (29), we now obtain the boost factor in the case of relative errors in linear order according to

$$ {}^{R}\beta = \frac{\ln\left[1 - 11\,{}^{R}\gamma^{(\text{rand})}_{\text{adder}} L^2\sigma^2\right]}{\ln\left[1 - \frac{3}{2}{}^{R}\gamma^{(\text{sym})}_{\text{adder}} L^2\sigma^2\right]} \approx \left(\frac{22}{3}\right)\frac{{}^{R}\gamma^{(\text{rand})}_{\text{adder}}}{{}^{R}\gamma^{(\text{sym})}_{\text{adder}}} \approx 10, \tag{31} $$

where we used the numerical values of ${}^{R}\gamma^{(\text{rand})}_{\text{adder}}$ and ${}^{R}\gamma^{(\text{sym})}_{\text{adder}}$ from (18) and (29), respectively. This result is important. It shows that even in the large-qubit limit we obtain a boost factor of about one order of magnitude.

We now turn to the case of absolute errors. In this case we have

$$ {}^{A}F_{\text{Shor}}^{(\text{sym})} = \left[\frac{3}{4}{}^{A}F_{ss} + \frac{1}{8}\left({}^{A}F_{ss}\,{}^{A}F_{\text{adder}}^{(\text{sym})} + {}^{A}F_{\text{adder}}^{(\text{sym})^2}\right)\right]^{4L^2} \tag{32} $$

and

$$ {}^{A}F_{\text{Shor}}^{(\text{rand})} = \left[\frac{3}{4}\left({}^{A}F_{\text{adder}}^{(\text{rand})}\right)^2 + \frac{1}{4}\left({}^{A}F_{\text{adder}}^{(\text{rand})}\right)^5\right]^{4L^2}. \tag{33} $$

According to [48] [equation (20)], we have

$$ {}^{A}F_{\text{adder}}^{(\text{rand})} = \exp\left\{-\left[\frac{6n(n-1)}{32} + \frac{\mu n}{4}\right]\sigma^2\right\}, \tag{34} $$

where μ is given by $\mu = 1.75$ [48]. With $n = L + 1 = 1025$, we obtain

$$ {}^{A}F_{\text{adder}}^{(\text{rand})} = \exp\left[-\left({}^{A}\gamma_{\text{adder}}^{(\text{rand})}\right)\sigma^2\right], \tag{35} $$

where

$$ {}^{A}\gamma_{\text{adder}}^{(\text{rand})} = 1.97 \times 10^5. \tag{36} $$

Linearizing ${}^{A}F_{\text{adder}}^{(\text{rand})}$, using the result in (33), and linearizing again, we obtain

$$ \begin{aligned} {}^{A}F_{\text{Shor}}^{(\text{rand})} &= \left[\frac{3}{4}\left(1 - {}^{A}\gamma_{\text{adder}}^{(\text{rand})}\sigma^2\right)^2 + \frac{1}{4}\left(1 - {}^{A}\gamma_{\text{adder}}^{(\text{rand})}\sigma^2\right)^5\right]^{4L^2} \\ &= 1 - 11L^2\ {}^{A}\gamma_{\text{adder}}^{(\text{rand})}\sigma^2. \end{aligned} \tag{37} $$

For acceptable quantum computer performance, similar to the case of relative errors, we need to require

$$ 11L^2\ {}^{A}\gamma_{\text{adder}}^{(\text{rand})}\sigma^2 < 1, \tag{38} $$

which implies

$$ \sigma < 6.6 \times 10^{-7}. \tag{39} $$

This is one order of magnitude more demanding than in the case of relative errors, but not unrealistic.

In order to capture the symmetry boost, we need to compute ${}^{A}F_{\text{Shor}}^{(\text{sym})}$ [see (32)]. Similar to the case of relative errors, we set ${}^{A}F_{ss} = 1$. We also need ${}^{A}F_{\text{adder}}^{(\text{sym})}$, for which we obtain

$$ {}^{A}F_{\text{adder}}^{(\text{sym})} = \exp\left\{-\left[\frac{5n(n-1)}{32} + \frac{\mu_s n}{4}\right]\sigma^2\right\} = \exp\left[-{}^{A}\gamma_{\text{adder}}^{(\text{sym})}\sigma^2\right], \tag{40} $$

where, with $n = L + 1 = 1025$ and $\mu_s = -0.1$, we obtain

$$ {}^{A}\gamma_{\text{adder}}^{(\text{sym})} = 1.64 \times 10^5. \tag{41} $$

Using (40) in (32) and linearizing, we obtain

$$ {}^{A}F_{\text{Shor}}^{(\text{sym})} = \left[\frac{3}{4} + \frac{1}{8}\left(1 - {}^{A}\gamma_{\text{adder}}^{(\text{sym})}\sigma^2 + 1 - 2{}^{A}\gamma_{\text{adder}}^{(\text{sym})}\sigma^2\right)\right]^{4L^2} = 1 - \frac{3L^2}{2}\,{}^{A}\gamma_{\text{adder}}^{(\text{sym})}\sigma^2. \tag{42} $$

We are now ready to compute the boost factor ${}^{A}\beta$ for absolute errors. With (36) and (41) we obtain

$$ \begin{aligned} {}^{A}\beta &= \frac{\ln\langle {}^{A}F_{\text{Shor}}^{(\text{rand})}\rangle_{s,a}}{\ln\langle {}^{A}F_{\text{Shor}}^{(\text{sym})}\rangle_{s,a}} = \\ &= \left(\frac{22}{3}\right)\left(\frac{{}^{A}\gamma_{\text{adder}}^{(\text{rand})}}{{}^{A}\gamma_{\text{adder}}^{(\text{sym})}}\right) = \left(\frac{22}{3}\right)\left(\frac{1.97\times 10^5}{1.64\times 10^5}\right) = 8.8. \end{aligned} \tag{43} $$

Thus, we have shown that the exploitation of symmetry in both the case of absolute and relative errors yields a boost factor of approximately one order of magnitude. But even without making explicit use of the symmetry boost, we have shown in this section that RSA-1024 factoring using Shor's algorithm is realistic. We had shown a similar result (without using a symmetry boost) for RSA-2048 factoring in [49].

Even without performing the detailed calculations presented in this section, we may convince ourselves immediately that a symmetry boost should exist. Qualitatively, according to (13), the boost factor is

$$ \begin{aligned} \beta &= \frac{\ln\langle F_{\text{Shor}}^{(\text{rand})}\rangle_{s,a}}{\ln\langle F_{\text{Shor}}^{(\text{sym})}\rangle_{s,a}} = \frac{\ln\left[\frac{3}{4}\left(F_{\text{adder}}^{(\text{rand})}\right)^2 + \frac{1}{4}\left(F_{\text{adder}}^{(\text{rand})}\right)^5\right]}{\ln\left[\frac{3}{4} + \frac{1}{8}\left(F_{\text{adder}}^{(\text{sym})} + {F_{\text{adder}}^{(\text{sym})}}^2\right)^2\right]} \\ &= \frac{\ln\left[\frac{3}{4}(1-\gamma_{\text{adder}}^{(\text{rand})}\sigma^2)^2 + \frac{1}{4}(1-\gamma_{\text{adder}}^{(\text{rand})}\sigma^2)^5\right]}{\ln\left[\frac{3}{4} + \frac{1}{8}(1-\gamma_{\text{adder}}^{(\text{sym})}\sigma^2 + (1-\gamma_{\text{adder}}^{(\text{sym})}\sigma^2)^2)\right]} \approx 7\left(\frac{\gamma_{\text{adder}}^{(\text{rand})}}{\gamma_{\text{adder}}^{(\text{sym})}}\right). \end{aligned} \tag{44} $$

As can be seen in (18) and (29) [(36) and (41), respectively], we expect $\gamma_{\text{adder}}^{(\text{sym})} \lesssim \gamma_{\text{adder}}^{(\text{rand})}$, which means that, according to the qualitative estimate (44), we should expect a boost factor of about one order of magnitude.

V. ROBUSTNESS OF THE SYMMETRY BOOST

So far, we assumed that hardware errors occur only in the rotation gates in the form of diagonal over- and under-rotation of the desired phase angles. Assuming this type of errors, we were able to show both analytically and numerically that symmetric implementation of

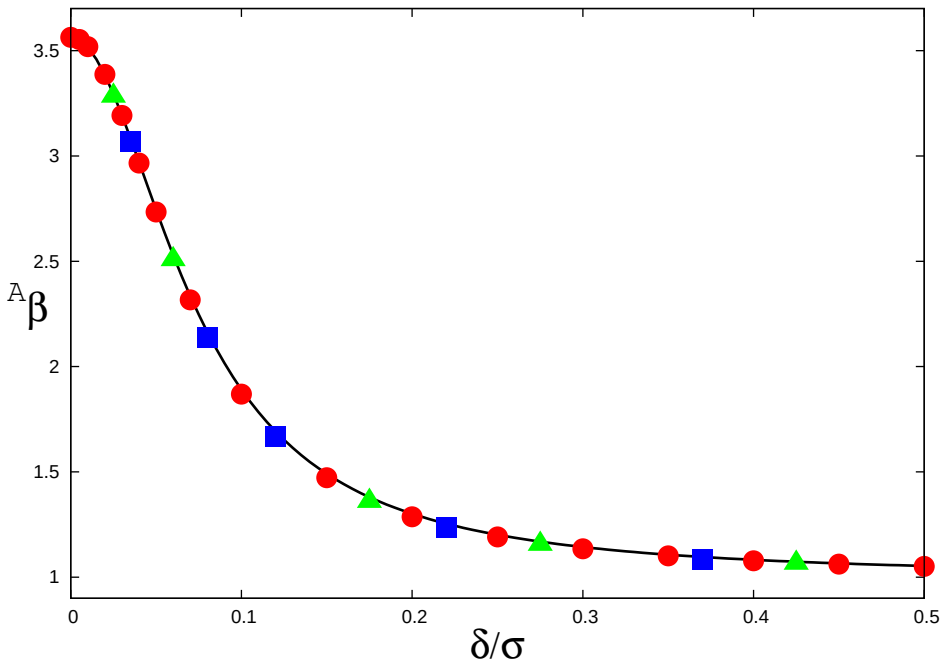

FIG. 6: Boost factor ${}^{A}\beta$ as a function of the scaled off-diagonal error strength δ/σ for $\sigma = 0.01$ (filled red circles), $\sigma = 0.001$ (filled blue squares), and $\sigma = 0.0001$ (filled green triangles). A Lorentzian fit function, $L(\delta/\sigma) = 1 + 2.6/[1 + (\delta/0.073\sigma)^2]$, is also shown.

errors results in a fidelity boost of Shor's quantum factoring algorithm. It is clear that in actual hardware implementations of quantum computers off-diagonal errors also occur, and that all types of gates, not just rotation gates, are affected by this more general class of errors. While, in general, off-diagonal errors are very difficult to treat analytically, we can certainly investigate their effects in numerical simulations. In particular we focus in this section on the question of how more general, non-diagonal errors affect the symmetry boost documented in previous sections.

Introducing general, non-biased, off-diagonal errors into our rotation gates, we computed the boost factor ${}^{A}\beta$ by multiplying the 2×2, 4×4, and 8×8 matrix representations of each of our rotation-, controlled-rotation-, and controlled-controlled-rotation gates by the SU(N) error matrices

$$\mathcal{E}_{N\times N}(v_1, \ldots, v_M; \delta) = \exp(i \sum_{j=1}^{M} v_j \lambda_j), \tag{45}$$

where $N = 2, 4, 8$, respectively, v_j, Gaussian random variables with standard deviation δ,

are the SU(N) error strengths, and λ_j are the $M = N^2 - 1$ generators of SU(N) [51]. The result is shown in Fig. 6 as a function of δ/σ for absolute over/underrotation errors of standard deviation σ, for $\sigma = 0.01$ (filled red circles), $\sigma = 0.001$ (filled blue squares), and $\sigma = 0.0001$ (filled green triangles). We see that the boost factor scales in δ/σ and decreases like a Lorentzian for increasing δ/σ. Thus, Fig. 6 shows that the boost factor is robust with respect to off-diagonal unitary errors and decays relatively slowly (essentially like a power law) for increasing δ/σ.

The simplest model of diagonal non-unitary errors and their effect on the boost factor β is obtained by multiplying each gate by the complex phase factor $\exp(i\omega)$, where ω is a complex number with a positive imaginary part. This results in an exponential reduction of the fidelity by a factor $\exp(-\Omega)$, where Ω is real and positive. Then, according to the definition of the boost factor, we have

$$\beta(\Omega) = \frac{\ln[e^{-\Omega} F^{(\mathrm{rand})}]}{\ln[e^{-\Omega} F^{(\mathrm{sym})}]} = \beta(\Omega = 0) \left\{ \frac{1 + \Omega/[\gamma^{(\mathrm{rand})}\sigma^2]}{1 + \Omega/[\gamma^{(\mathrm{sym})}\sigma^2]} \right\}. \tag{46}$$

This shows that even in the presence of non-unitary errors, the symmetry boost factor is never completely erased. However, in order to obtain a significant boost factor, and since $\gamma^{(\mathrm{sym})} < \gamma^{(\mathrm{rand})}$, we have to require

$$\Omega < \gamma^{(\mathrm{sym})}\sigma^2. \tag{47}$$

VI. DISCUSSION, SUMMARY, AND CONCLUSION

Clearly, our analytical results scale in the number of qubits, demonstrating that the symmetry-driven fidelity boost will persist as we scale up the quantum circuit, i.e., as we go to the limit of large numbers of qubits. We also notice that the analytically predicted fidelity boost underestimates the numerically observed fidelity boost. This is so, because our analytical analyses are based on local estimates of fidelity boosts that are focused on individual building blocks, such as adders and modulo adders. The observed additional boosts may be explained due to long-range coherences that are not currently included in our local analytical estimates.

An important result is the structural stability, i.e., the robustness of the symmetry boost, a result we established in Sec. V. Here we found that adding general SU(2), SU(4), and SU(8) errors of strength δ to the diagonal over/underrotation errors of strength σ reduces

the symmetry boost with a Lorentzian line shape that scales in δ/σ. This shows that the symmetry boost, even in the presence of uniform, non-diagonal errors, is never entirely erased and decays only like a power law in the off-diagonal error strength δ. We note that the isotropic SU(N) simulations conducted in Sec. V correspond to the worst-case scenario of a very badly designed gate that allows the gate to induce phase rotations with statistically equal amplitudes between multiple qubits. If the quantum computer is realized, e.g., as a system of spatially separated trapped ions [32, 34], it is unlikely that a control impulse targeting two specific ions/qubits would induce phase errors in other, not targeted, spatially separated ions with the same strength as induced in the pair of targeted ions. Thus, a special design effort would need to be made to realize the worst-case scenario simulated in Sec. V, whereas in a well-designed gate the largest phase error is expected to manifest in the target state of the target ion/qubit whose phase is intended to be rotated. Thus, we expect that our model of switching on isotropic errors of strength δ in addition to the dominant diagonal errors of strength σ reflects the actual physical situation of realistic gate operation and shows that the symmetry boost is robust with respect to off-diagonal errors.

Investigating the effect of non-unitary errors in a simple model of exponential norm reduction we found that non-unitary errors do reduce the symmetry boost factor without ever completely erasing it. We also found a condition on the strength of the non-unitary errors that, if fulfilled, guarantees that the boost factor is not substantially reduced from its unitary value.

We are certain that our results are useful for quantum experimentalists and engineers as benchmark estimates of necessary hardware accuracy for realizing large-scale quantum computers. Not only are quantum computers already resilient with respect to irremovable hardware errors [25, 27–29], but, as we showed in this paper, exhibit significant performance enhancement just by controlling the symmetry of the errors. We also showed that using symmetry as a method to boost performance is well within engineering capabilities. This is supported by the fact that spin-echoes [52], e.g., already proved useful for practical applications in suppressing the naturally occurring errors in a given physical system. While it is still true that the symmetry needs to be implemented to a high precision, from the engineering perspective, the task of keeping the symmetry should be easier than keeping the error level itself small. Our results are also of interest to theorists. Given that exploiting symmetry is the key for the dramatic fidelity boost at the architectural, surface level, as opposed to

the individual, microscopic, inner-workings of a single-qubit state, we gain the insight that a topologically and structurally robust quantum algorithm may be developed. Given the fact that quantum algorithms, in general, tend to contain a large number of symmetric structures, we expect that designing hardware that results in symmetric errors, as exploited in this paper, may be beneficial for boosting performance in other quantum algorithms as well. Alternative schemes for error reduction exist (see, e.g., [55]). To obtain an additional fidelity boost, our scheme may be used in addition to these schemes.

In summary, we have shown in this paper that by exploiting quantum subroutine structures of the form $\mathcal{F}\mathcal{U}\mathcal{F}^{-1}$ in Shor's algorithm results in a significant fidelity boost that may be as large as one order of magnitude for large quantum computers. Since it is impossible to simulate large-scale quantum computers even with the most advanced classical supercomputers, we present analytical scaling formulas that are capable of predicting the expected symmetry boost for large quantum processors. We illustrated the process with the help of an explicit example: Shor factoring of RSA-1024, in which case we obtain boost factors of about one order of magnitude for both relative an absolute errors. We also showed that the boost factor is robust with respect to off-diagonal unitary and diagonal non-unitary errors.

It would have been lamentable if the irremovable hardware errors proliferated too quickly for a quantum computer to be of any practical use. Fortunately, as we showed in this paper, this is not so. Together with recent advances in quantum error correction and its fault-tolerant implementation, the surprising robustness of quantum computers with respect to errors and noise suggests that large-scale quantum computers may indeed be built. Exploiting symmetry in the subunits of quantum algorithms, as suggested, proved, and illustrated in this paper for the case of Shor's algorithm, provides an additional, powerful tool on the way to the construction of quantum computers of practical importance.

Appendix A: Derivation of (4) and (5)

In this appendix, we derive (5) and (6) in the main text. For the convenience of the reader, we show these two equations again below in the order of (5) and (6):

$$\Phi_{s,a}(l) = \frac{1}{2^{L+1}}\left[1 + \exp\left(i\left\{\left[\sum_{\nu=0}^{L-1} k_\nu r_{L-\nu}\right]\right\}\right) e^{2\pi i(s+a-l)/2^{L+1}}\right] R_{s,a}(l), \tag{A1}$$

and

$$W_{s,a}(l) = \sum_{l'=0}^{2^L-1} \exp\left[i \left(\sum_{m=0}^{L-1} l'_{[L-1-m]} \left\{ a_{[m]} r_0 + \left[\sum_{\nu=0}^{m-1} k_\nu r_{m-\nu} \right] \right\} \right) \right] e^{2\pi i (s+a-l) l'/2^L}. \tag{A2}$$

We note that $k_\nu = s_{[\nu]} + a_{[\nu]} - l_{[\nu]}$, where $s_{[\nu]}$, e.g., denotes the νth binary digit of s, r_j may be α_j or $(\pi/2^j) \times \alpha_j$ if the errors are of the absolute kind or of the relative kind, respectively (see Sec. II), and s, a, and l are the input, addend, and output integers, respectively, of the perturbed adder.

Our starting point is the definition of the $(L+1)$-bit Fourier-based adder. Stating explicitly the definitions of the quantum Fourier transform (QFT), the quantum Fourier adder (QFA) and the inverse quantum Fourier transform (QFT^{-1}), i.e.,

$$\begin{aligned}
\hat{U}^{(\mathrm{QFT})}|s\rangle &= \frac{1}{\sqrt{2^{L+1}}} \sum_{s'=0}^{2^{L+1}-1} \exp\left[\frac{2\pi i s s'}{2^{L+1}} \right] |s'\rangle, \\
\hat{U}_a^{(\mathrm{QFA})}|s'\rangle &= \exp\left[\frac{2\pi i s' a}{2^{L+1}} \right] |s'\rangle, \\
\hat{U}^{(\mathrm{QFT}^{-1})}|s'\rangle &= \frac{1}{\sqrt{2^{L+1}}} \sum_{l=0}^{2^{L+1}-1} \exp\left[-\frac{2\pi i s' l}{2^{L+1}} \right] |l\rangle,
\end{aligned} \tag{A3}$$

we have

$$|s+a\rangle = \hat{U}^{(\mathrm{QFT}^{-1})} \hat{U}_a^{(\mathrm{QFA})} \hat{U}^{(\mathrm{QFT})} |s\rangle. \tag{A4}$$

Equation (A4) shows that the operation of addition has the structure $\mathcal{F}\mathcal{U}\mathcal{F}^{-1}$, which allows the implementation of symmetric errors to obtain a symmetry boost, if we identify $\mathcal{F} = \hat{U}^{(\mathrm{QFT}^{-1})}$, $\mathcal{U} = \hat{U}_a^{(\mathrm{QFA})}$ and $\mathcal{F}^{-1} = \hat{U}^{(\mathrm{QFT})}$. Expressing the integers s, s', a, and l in their binary representations and explicitly writing out the bitwise arithmetic, we may now write

$$\begin{aligned}
\hat{U}^{(\mathrm{QFT})}|s\rangle &= \frac{1}{\sqrt{2^{L+1}}} \sum_{s'=0}^{2^{L+1}-1} \exp\left[i \sum_{m=0}^{L} s'_{[m]} \sum_{\nu=0}^{L-m} s_{[\nu]} \frac{\pi}{2^{L-m-\nu}} \right] |s'\rangle, \\
\hat{U}_a^{(\mathrm{QFA})}|s'\rangle &= \exp\left[i \sum_{m=0}^{L} s'_{[m]} \sum_{\nu=0}^{L-m} a_{[\nu]} \frac{\pi}{2^{L-m-\nu}} \right] |s'\rangle, \\
\hat{U}^{(\mathrm{QFT}^{-1})}|s'\rangle &= \frac{1}{\sqrt{2^{L+1}}} \sum_{l=0}^{2^{L+1}-1} \exp\left[-i \sum_{m=0}^{L} s'_{[m]} \sum_{\nu=0}^{L-m} l_{[\nu]} \frac{\pi}{2^{L-m-\nu}} \right] |l\rangle.
\end{aligned} \tag{A5}$$

We now perturb the rotation angles as specified by our protocols detailed in Sec. II. Denoting $\varphi_{L-m-\nu} = \pi/2^{L-m-\nu}$, this amounts to replacing all occurrences of $\varphi_{L-m-\nu}$ in the

QFT and QFT^{-1} with $\tilde{\varphi}_{L-m-\nu}$, except for the cases with $L-m-\nu=0$, which correspond to the Hadamard gates. The resulting perturbed operations are

$$\begin{aligned}
\hat{\tilde{U}}^{(\mathrm{QFT})}|s\rangle &= \frac{1}{\sqrt{2^{L+1}}}\sum_{s'=0}^{2^{L+1}-1}\exp\left[i\sum_{m=0}^{L}s'_{[m]}\left(s_{[L-m]}\varphi_0+\sum_{\nu=0}^{L-m-1}s_{[\nu]}\tilde{\varphi}_{L-m-\nu}\right)\right]|s'\rangle,\\
\hat{\tilde{U}}_a^{(\mathrm{QFA})}|s'\rangle &= \exp\left[i\sum_{m=0}^{L}s'_{[m]}\sum_{\nu=0}^{L-m}a_{[\nu]}\tilde{\varphi}_{L-m-\nu}\right]|s'\rangle,\\
\hat{\tilde{U}}^{(\mathrm{QFT}^{-1})}|s'\rangle &= \frac{1}{\sqrt{2^{L+1}}}\sum_{l=0}^{2^{L+1}-1}\exp\left[-i\sum_{m=0}^{L}s'_{[m]}\left(l_{[L-m]}\varphi_0+\sum_{\nu=0}^{L-m-1}l_{[\nu]}\tilde{\varphi}_{L-m-\nu}\right)\right]|l\rangle. \qquad \text{(A6)}
\end{aligned}$$

Using $\tilde{\varphi}_{L-m-\nu}=\varphi_{L-m-\nu}+r_{L-m-\nu}$, we obtain

$$\begin{aligned}
\hat{\tilde{U}}^{(\mathrm{QFT}^{-1})}\hat{\tilde{U}}_a^{(\mathrm{QFA})}\hat{\tilde{U}}^{(\mathrm{QFT})}|s\rangle =& \frac{1}{2^{L+1}}\sum_{l=0}^{2^{L+1}-1}\sum_{s'=0}^{2^{L+1}-1}e^{\frac{2\pi i(s+a-l)s'}{2^{L+1}}}\exp\left[i\sum_{m=0}^{L}s'_{[m]}\sum_{\nu=0}^{L-m-1}s_{[\nu]}r_{L-m-\nu}\right]\\
&\exp\left[i\sum_{m=0}^{L}s'_{[m]}\sum_{\nu=0}^{L-m}a_{[\nu]}r_{L-m-\nu}\right]\exp\left[i\sum_{m=0}^{L}s'_{[m]}\sum_{\nu=0}^{L-m-1}l_{[\nu]}r_{L-m-\nu}\right]|l\rangle. \qquad \text{(A7)}
\end{aligned}$$

Inserting

$$\sum_{m=0}^{L}s'_{[m]}\sum_{\nu=0}^{L-m}a_{[\nu]}r_{L-m-\nu}=\sum_{m=0}^{L}s'_{[m]}\sum_{\nu=0}^{L-m-1}a_{[\nu]}r_{L-m-\nu}+\sum_{m=0}^{L}s'_{[m]}a_{[L-m]}r_0 \qquad \text{(A8)}$$

in (A7) and reversing the ordering of the m-sum, i.e., $L-m\to m$, we obtain

$$\begin{aligned}
\hat{\tilde{U}}^{(\mathrm{QFT}^{-1})}\hat{\tilde{U}}_a^{(\mathrm{QFA})}\hat{\tilde{U}}^{(\mathrm{QFT})}|s\rangle =& \frac{1}{2^{L+1}}\sum_{l=0}^{2^{L+1}-1}\sum_{s'=0}^{2^{L+1}-1}e^{\frac{2\pi i(s+a-l)s'}{2^{L+1}}}\\
&\exp\left[i\sum_{m=0}^{L}s'_{[L-m]}\left(a_{[m]}r_0+\sum_{\nu=0}^{m-1}k_\nu r_{m-\nu}\right)\right]|l\rangle. \qquad \text{(A9)}
\end{aligned}$$

At this point we consider two separate cases: s' even and s' odd. In the even case, we have $s'_{[0]}=0$. In the odd case, we have $s'_{[0]}=1$. Writing the two cases out separately, and letting $s'=2l'+s'_{[0]}$, we obtain

$$\begin{aligned}
\hat{\tilde{U}}^{(\mathrm{QFT}^{-1})}\hat{\tilde{U}}_a^{(\mathrm{QFA})}\hat{\tilde{U}}^{(\mathrm{QFT})}|s\rangle =& \frac{1}{2^{L+1}}\sum_{l=0}^{2^{L+1}-1}\left(1+\exp\left[i\sum_{\nu=0}^{L-1}k_\nu r_{L-\nu}\right]e^{\frac{2\pi i(s+a-l)}{2^{L+1}}}\right)\\
&\sum_{l'=0}^{2^{L}-1}\exp\left[i\sum_{m=0}^{L-1}l'_{[L-1-m]}\left(a_{[m]}r_0+\sum_{\nu=0}^{m-1}k_\nu r_{m-\nu}\right)\right]e^{\frac{2\pi i(s+a-l)l'}{2^{L}}}|l\rangle. \qquad \text{(A10)}
\end{aligned}$$

To this end, defining $\Phi_{s,a}(l)$ according to

$$\hat{\hat{U}}^{(\mathrm{QFT}^{-1})}\hat{\hat{U}}_a^{(\mathrm{QFA})}\hat{\hat{U}}^{(\mathrm{QFT})}|s\rangle = \sum_{l=0}^{2^{L+1}-1} \Phi_{s,a}(l)|l\rangle, \tag{A11}$$

the derivation of (5) and (6) is complete.

Appendix B: Hardware errors versus flip errors

There is a fundamental difference between hardware errors and local Pauli errors (spin-flip errors) [25].

(a) *Hardware errors.* Any unitary 2×2 gate acting on a single qubit may be parametrized, up to a global phase, with three real angles, α, β, and ϕ, according to

$$U_{2\times 2} = \begin{pmatrix} e^{i\beta}\cos(\phi) & e^{-i\alpha}\sin(\phi) \\ -e^{i\alpha}\sin(\phi) & e^{-i\beta}\cos(\phi) \end{pmatrix}. \tag{B1}$$

No physical gate is error-free. Therefore, we characterize the strength of the error in the gate by the inexactness of its three parameters α, β, and ϕ. We call these errors hardware errors. Contrary to local Pauli errors (spin-flip errors), to be defined in point (b), hardware errors occur with certainty whenever the gate $U_{2\times 2}$ is executed. This amounts to inexact rotations on the Bloch sphere.

(b) *Flip errors.* We refer to flip errors as the local Pauli errors that occur with probabilities p_x, p_y, and p_z, correspoinding to the three Pauli gates X, Y, and Z.

We now compare the effects of these two types of errors. For hardware errors, we begin with the general unitary gate defined in (B1). For an input state $|\psi\rangle = a|0\rangle + b|1\rangle$, where $|a|^2 + |b|^2 = 1$, we obtain the fidelity F_{Hardware} of the gate according to $F_{\mathrm{Hardware}} = |\zeta|^2$, where

$$\begin{aligned} \zeta = (a^* \quad b^*) & \begin{pmatrix} e^{-i\beta}\cos(\phi) & -e^{-i\alpha}\sin(\phi) \\ e^{i\alpha}\sin(\phi) & e^{i\beta}\cos(\phi) \end{pmatrix} \\ \times & \begin{pmatrix} e^{i(\beta+\Delta\beta)}\cos(\phi+\Delta\phi) & e^{-i(\alpha+\Delta\alpha)}\sin(\phi+\Delta\phi) \\ -e^{i(\alpha+\Delta\alpha)}\sin(\phi+\Delta\phi) & e^{-i(\beta+\Delta\beta)}\cos(\phi+\Delta\phi) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}, \end{aligned} \tag{B2}$$

and the asterisk denotes the complex conjugate. Since ζ is a complex number, we may write

$$F_{\mathrm{Hardware}} \geq [\mathrm{Re}(\zeta)]^2, \tag{B3}$$

where

$$\mathrm{Re}(\zeta) = \cos(\Delta\beta)\cos(\phi)\cos(\phi+\Delta\phi) + \cos(\Delta\alpha)\sin(\phi)\sin(\phi+\Delta\phi) \tag{B4}$$

is the real part of ζ. The equality in (B3) may be obtained in case $|a| = |b| = 1/\sqrt{2}$ and $2a^*b = e^{i\Delta\alpha}$. Assuming a Gaussian distribution with mean 0 and standard deviation σ for the random errors $\Delta\alpha$, $\Delta\beta$, and $\Delta\gamma$, we obtain to second order

$$F_{\mathrm{Hardware}} \geq 1 - \frac{2(\Delta\phi)^2 + (\Delta\beta)^2 + (\Delta\alpha)^2}{2}, \tag{B5}$$

which, upon averaging, leads to

$$\langle F_{\mathrm{Hardware}} \rangle \geq 1 - 2\sigma^2, \tag{B6}$$

where $\langle \ldots \rangle$ denotes the average over the Gaussian ensemble.

For flip errors, the corresponding error model is the depolarizing channel model. Denoting by p the probability of occurrence of the three Pauli errors induced by X, Y, and Z, the fidelity of the single-qubit quantum circuit becomes

$$F_{\mathrm{Flip}} = 1 - 3p. \tag{B7}$$

Comparing (B6) with (B7), we find that for given p, the choice

$$\sigma^2 < 3p/2, \tag{B8}$$

on average, guarantees better fidelity for hardware errors than for flip errors. Conversely, if

$$\sigma^2 > 3p/2, \tag{B9}$$

hardware errors are more important than flip errors, which supports our point that hardware errors may be more detrimental than decoherence errors. The following concrete example illustrates this for an important specific case.

In Fig. 7, we show the fidelity of a [7,1,3] quantum error correction code in the presence of hardware errors (red pluses) or flip errors (green crosses) as a function of σ and p, respectively. We scaled the abscissa in $\sqrt{p}$, but linearly in σ. In this case the inequality (B8) is automatically fulfilled for the same ascissa point $\sigma = \sqrt{p}$ in which case flip errors are expected to result in worse fidelity than hardware errors, i.e., we expect the fidelity curve for flip errors (green crosses) to be below the fidelity curve for hardware errors (red

pluses). For the computations resulting in Fig. 1, and according to the standard convention in the quantum error correction literature, we assumed that errors act in the error-protected region only, and the encoding and decoding circuits are assumed to be error-free. This is entirely in the spirit of quantum error correcting codes whose error-protection capability is restricted to the encoded region. As shown in Fig. 1, and contrary to expectations, the results displayed in Fig. 1 show that hardware errors result in worse fidelity than flip errors. This is despite the fact that, as mentioned above, the fidelity with hardware errors, but without quantum error correction, is, for the same abscissa point, by construction, better than that expected from flip errors. Therefore, our results show that in the presence of quantum error correction, the effect of hardware errors may in fact be more severe, i.e., it reduces the fidelity by a more significant amount, than flip errors. This demonstrates that there are cases in which hardware errors are a more significant problem than flip errors. In these cases error-correction circuitry does more harm than good, and instead of improving the fidelity, the presence of the error-correction circuit worsens the fidelity. This counterintuitive result is a consequence of the fact that, while flip errors occur only *potentially* with some finite probability p per qubit, and may be corrected with high probability with ideal error-correction circuitry, hardware errors occur with *certainty*, i.e., with probability 1, and since error-correction circuitry is designed to consist of replicated gates, and these gates are all imperfect, the errors induced by these gates are imparted on *all* qubits. Thus, multiple errors occur simultaneously, which, overwhelming the error-protection circuit, cannot be corrected, and thus result in $F_{\text{Hardware}} < F_{\text{Flip}}$ *with* quantum error correction, although, by design, $F_{\text{Hardware}} > F_{\text{Flip}}$ for the stand-alone (imperfect) $U_{2\times 2}$ gate *without* quantum error correction. This is a perfect example of how quantum error correction may actually be detrimental instead of being beneficial.

Appendix C: Fidelity Product Formula

We consider the quantum mapping [53]

$$|\psi_N\rangle = U^N|\psi_0\rangle, \quad N = 1, 2, \ldots, \tag{C1}$$

where U is a unitary operator and $|\psi_0\rangle$ is a starting state. Introducing a perturbed operator $\tilde{U}(\epsilon)$, where ϵ is a stochastic perturbation parameter, i.e., a random variable with $\langle\epsilon\rangle_\epsilon = 0$,

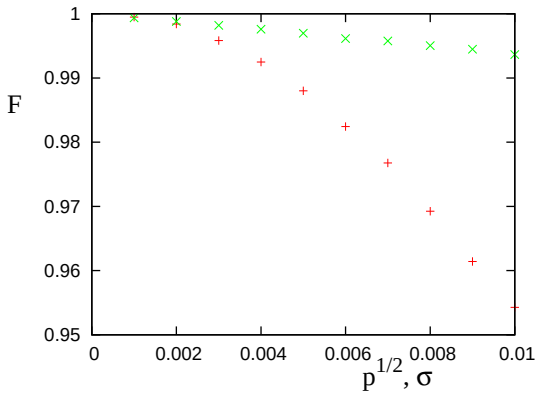

FIG. 7: Fidelity of the [7,1,3] quantum error correction code. Green crosses show the effect of flip errors on the fidelity and correspond to the $p^{1/2}$ scale on the abscissa; red pluses show the effect of hardware errors and correspond to the linear σ scale on the abscissa. For the same abscissa point, i.e., $\sigma = p^{1/2}$, the inequality (B8) is fulfilled, which means that in the absence of quantum error protection the hardware fidelity of the bare gate is better than the fidelity with flip errors. Apparently, in the presence of the [7,1,3] quantum error correction code, hardware errors are a more significant problem than flip errors. Thus, instead of improving the fidelity, the [7,1,3] code *worsened* the fidelity.

$\langle \epsilon^2 \rangle_\epsilon = \sigma^2$ ($\langle \ldots \rangle_\epsilon$ denotes averaging over ϵ), and

$$\tilde{U}(\epsilon) \to U \quad \text{for} \quad \epsilon \to 0, \tag{C2}$$

we define the stochastic quantum mapping

$$|\tilde{\psi}_N\rangle = \tilde{U}(\epsilon_N)\tilde{U}(\epsilon_{N-1}) \ldots \tilde{U}(\epsilon_1)|\psi_0\rangle \tag{C3}$$

and the fidelity

$$F_N = \langle |\langle \tilde{\psi}_N | \psi_N \rangle|^2 \rangle_\epsilon. \tag{C4}$$

Defining

$$F \equiv F_1, \tag{C5}$$

our goal is to motivate and discuss the fidelity product formula

$$F_N \approx F^N, \tag{C6}$$

used in this paper and also extensively used in the literature (see, e.g., [38, 39]). In particular, since this formula holds only approximately, we need to establish its range of validity.

Discussion of the fidelity formula (C6) also serves to illustrate how the deterministic hardware errors discussed in this paper may originate from inaccurate physical implementations of quantum gates.

Suppose we realize a physical qubit as a two-level spin system with states $|\downarrow\rangle$ and $|\uparrow\rangle$, and implement a certain quantum gate G, akin to the phase-rotation gate, with the help of a time-dependent magnetic field B, oriented in the negative z direction and acting on the magnetic dipole moment of the qubit during a time interval Δt. In this case the Hamiltonian of G is given by

$$H = B\mu\sigma_z/2, \quad 0 < t < \Delta t, \tag{C7}$$

where μ is the magnetic moment of the spin and $\sigma_z|\downarrow\rangle = -|\downarrow\rangle$, $\sigma_z|\uparrow\rangle = |\uparrow\rangle$. Then, the unitary operator U executing the gate G is given by

$$U = \exp(iH\Delta t/\hbar) = \exp(i\theta\sigma_z), \tag{C8}$$

where $\theta = B\mu\Delta t/(2\hbar)$ is the rotation angle. We have $U|\downarrow\rangle = \exp(-i\theta)|\downarrow\rangle$ and $U|\uparrow\rangle = \exp(i\theta)|\uparrow\rangle$. Apparently, the action of G is to rotate both $|\downarrow\rangle$ and $|\uparrow\rangle$ by an angle θ, but in opposite directions.

Now, suppose we operate the gate G N times on the starting state $|\psi_0\rangle = A|\downarrow\rangle + C|\uparrow\rangle$, where $|A|^2 + |C|^2 = 1$. Then, as we repeatedly realize the gate G with physical magnetic fields B, we notice immediately that it is impossible to precisely apply identical fields B from pulse to pulse. We take this into account by replacing the mathematical idealization $U = \exp(i\theta\sigma_z)$ with the unitary operator $\tilde{U}(\epsilon_n) = \exp[i(\theta + \epsilon_n)\sigma_z]$ that corresponds to the magnetic field actually applied at the nth application of G, where the random variable ϵ_n represents the error in the magnetic field at gate application number n. Therefore, a physical implementation of G will not produce the ideal state $|\psi_N\rangle$ after N applications of G, but the state $|\tilde{\psi}_N\rangle$, which is different from $|\psi_N\rangle$ and depends on the actual realizations of the magnetic fields from gate application to gate application. The fidelity defined in (C4) measures how well $|\tilde{\psi}_N\rangle$ approximates the ideal state $|\psi_N\rangle$.

For our model gate G we can readily evaluate the fidelity F_N analytically. According to (C4) with (C3), we obtain

$$F_N = 1 - 4|A|^2|C|^2\langle\sin^2(\beta)\rangle_\epsilon, \tag{C9}$$

where

$$\beta = \epsilon_1 + \epsilon_2 + \ldots + \epsilon_N, \tag{C10}$$

and we have to average over all realizations of ϵ_n, $n = 1, 2, \ldots, N$.

The most important assumption for the approximate validity of the fidelity product formula (C6) is that the error parameters ϵ_n are independent random variables. In this case, and for large N, β is a Gaussian distributed random variable with variance $N\sigma^2$. This allows us to evaluate $\langle \sin^2(\beta) \rangle_\epsilon$ analytically. The result is

$$\langle \sin^2(\beta) \rangle_\epsilon = \frac{1}{2}[1 - \exp(-2N\sigma^2)]. \tag{C11}$$

Using this result in (C9), we obtain

$$F_N = 1 - 2|A|^2|C|^2[1 - \exp(-2N\sigma^2)]. \tag{C12}$$

This result shows that not even in the statistical sense is (C6) exact. However, expanding (C12) to linear order in σ^2, we obtain

$$F_N \approx 1 - 4N\sigma^2|A|^2|C|^2 \approx F^N. \tag{C13}$$

Thus, we arrive at the important conclusion that the fidelity product formula holds only to linear order in the error variance σ^2, but is accurate as long as

$$N\sigma^2 \ll 1. \tag{C14}$$

Together with statistical independence of the errors from gate application to gate application, (C14) serves as the criterion for the applicability of the fidelity product formula.

We now turn to the more general case of gate sequences involving different gates, labeled $G_1, \ldots, G_N$. Each of these gates, which are now no longer single-qubit gates, are realized by a unitary transformation U_j, $j = 1, \ldots, N$. A given gate G_j may have a general error in the s-dimensional computational space that may connect all possible computational qubits. Thus, the most general type of error is represented by a hermitian matrix H_j, which we normalize according to

$$V_j = \frac{H_j}{\sum_{k=1}^{s} |\lambda_k^{(j)}|}, \tag{C15}$$

where $\lambda_k^{(j)}$ is the kth eigenvalue of H_j and s is the dimension of our computational space. With the help of the error-type matrix H_j we define the perturbed matrix $\tilde{U}_j$, representing the flawed gate $\tilde{G}_j$, according to

$$\tilde{U}_j = e^{-i\epsilon_j V_j} U_j e^{i\epsilon_j V_j}, \tag{C16}$$

where, because of the normalization of the error matrix V_j, the error parameter ϵ_j now has the physical meaning of an error strength, i.e., it represents the size of the hardware errors. Expanding (C16) to second order in ϵ_j, we obtain

$$\tilde{U}_j \approx U_j - i\epsilon_j C_j - \frac{1}{2}\epsilon_j^2 D_j, \tag{C17}$$

where

$$C_j = [V_j, U_j] \tag{C18}$$

and

$$D_j = [V_j, [V_j, U_j]]. \tag{C19}$$

The fidelity is now defined as

$$F_N = \left|\langle\psi_0|\tilde{U}_1^\dagger(\epsilon_1)\tilde{U}_2^\dagger(\epsilon_2)\ldots\tilde{U}_N^\dagger(\epsilon_N)U_N(\epsilon_N)U_{N-1}(\epsilon_{N-1})\ldots U_1(\epsilon_1)|\psi_0\rangle\right|^2{}_\epsilon, \tag{C20}$$

where the subscript ϵ indicates a statistical average over all error strengths ϵ_j. Using the second-order expansion (C17) in (C20), we obtain

$$\begin{aligned} F_N = \Big|&\langle\psi_0|1 + i\epsilon_1(C_1^\dagger U_1) + i\epsilon_2 U_1^\dagger(C_2^\dagger U_2)U_1 + i\epsilon_3 U_1^\dagger U_2^\dagger(C_3^\dagger U_3)U_2U_1 + \ldots \\ &- \frac{1}{2}\epsilon_1^2(D_1^\dagger U_1) - \frac{1}{2}\epsilon_2^2 U_1^\dagger(D_2^\dagger U_2)U_1 - \frac{1}{2}\epsilon_3^2 U_1^\dagger U_2^\dagger(D_3^\dagger U_3)U_2U_1 - \ldots \\ &- \epsilon_1\epsilon_2 C_1^\dagger(C_2^\dagger U_2)U_1 - \epsilon_1\epsilon_3 C_1^\dagger U_2^\dagger(C_3^\dagger U_3)U_2U_1 - \epsilon_2\epsilon_3 U_1^\dagger C_2^\dagger(C_3^\dagger U_3)U_2U_1 - \ldots|\psi_0\rangle\Big|^2{}_\epsilon, \end{aligned} \tag{C21}$$

This expression has the structure

$$F_N = \left|\langle\psi_0|1 + W_N|\psi_0\rangle\right|^2{}_\epsilon = 1 + 2\Re\langle\psi_0|W_N|\psi_0\rangle_\epsilon + |\langle\psi_0|W_N|\psi_0\rangle|^2_\epsilon, \tag{C22}$$

where $\Re$ denotes the real part. Upon averaging over ϵ_j, the real-part term in (C22) reduces to

$$\Re\langle\psi_0|W_N|\psi_0\rangle_\epsilon = -\frac{1}{2}\Re\langle\psi_0|\left\{\epsilon_1^2(D_1^\dagger U_1) + \epsilon_2^2 U_1^\dagger(D_2^\dagger U_2)U_1 + \epsilon_3^2 U_1^\dagger U_2^\dagger(D_3^\dagger U_3)U_2U_1 + \ldots\right\}|\psi_0\rangle_\epsilon. \tag{C23}$$

Assuming that all ϵ_j have the same variance σ, the remaining ϵ-average turns (C23) into

$$2\Re\langle\psi_0|W_N|\psi_0\rangle_\epsilon = -\sigma^2\Re\langle\psi_0|[(D_1^\dagger U_1) + U_1^\dagger(D_2^\dagger U_2)U_1 + U_1^\dagger U_2^\dagger(D_3^\dagger U_3)U_2U_1 + \ldots]|\psi_0\rangle. \tag{C24}$$

Similarly, for the absolute-square term in (C22), and keeping only terms up to quadratic order, we obtain

$$|\langle\psi_0|W_N|\psi_0\rangle|^2_\epsilon = \sigma^2\Big[|\langle\psi_0|(C_1^\dagger U_1)|\psi_0\rangle|^2 + |\langle\psi_0|U_1^\dagger(C_2^\dagger U_2)U_1|\psi_0\rangle|^2 + |\langle\psi_0|U_1^\dagger U_2^\dagger(C_3^\dagger U_3)U_2U_1|\psi_0\rangle|^2 + \dots\Big]. \tag{C25}$$

At this point we pair corresonding terms in (C24) and (C25). The first such pair is

$$P_1 = -\Re\langle\psi_0|(D_1^\dagger U_1)|\psi_0\rangle + |\langle\psi_0|(C_1^\dagger U_1)|\psi_0\rangle|^2. \tag{C26}$$

Using the explicit versions of the commutators C_1 and D_1 defined in (C18) and (C19), respectively, and defining

$$\Omega_1 = C_1^\dagger U_1 = U_1^\dagger V_1 U_1 - V_1, \tag{C27}$$

we obtain

$$P_1 = -\langle\psi_0|\Omega_1^2|\psi_0\rangle + |\langle\psi_0|\Omega_1|\psi_0\rangle|^2. \tag{C28}$$

We see that $-P_1$ is the fluctuation of a general Hermitian operator Ω_1, which is always ≥ 0 [54], so that P_1 itself is always negative. The general pair is of the form

$$\begin{aligned} P_j =& -\Re\langle\psi_0|U_1^\dagger U_2^\dagger\dots U_{j-1}^\dagger(D_j^\dagger U_j)U_{j-1}U_{j-2}\dots U_1|\psi_0\rangle \\ &+ |\langle\psi_0|U_1^\dagger U_2^\dagger\dots U_{j-1}^\dagger(C_j^\dagger U_j)U_{j-1}U_{j-2}\dots U_1|\psi_0\rangle|^2 \\ =& -\langle\psi_{j-1}|\Omega_j^2|\psi_{j-1}\rangle + |\langle\psi_{j-1}|\Omega_j|\psi_{j-1}\rangle|^2, \end{aligned} \tag{C29}$$

where

$$|\psi_{j-1}\rangle = U_{j-1}\dots U_2U_1|\psi_0\rangle \tag{C30}$$

and

$$\Omega_j = C_j^\dagger U_j. \tag{C31}$$

According to (C22) we now have

$$F_N \approx 1 + \sigma^2\sum_{j=1}^N P_j = \prod_{j=1}^N f_j, \tag{C32}$$

where f_j is the fidelity in step number j, explicitly given by

$$f_j = |\langle\psi_{j-1}|\tilde{U}_jU_j|\psi_{j-1}\rangle|^2_\epsilon \approx 1 + \sigma^2P_j. \tag{C33}$$

In case all f_j are equal, and equal to $f_1 = F$, we obtain the fidelity product formula in its usual form as

$$F_N = F^N. \tag{C34}$$

Apparently, just like in our simple case of qubit rotation above, the fidelity product formula (C32) holds to first order in σ^2. Thus, the criterion of applicability of (C32), as before [see (C14)], is

$$N\sigma^2 \ll 1. \tag{C35}$$

Appendix D: Analytical derivation of $F_{\text{s.s.}}$

We start by defining $U^\dagger$ as the unitary evolution operator represented by the first grey box in Fig. 2 of the main text. Therefore, by symmetry, the second box represents U. Defining the quantum computer state after the first box as

$$|\psi'\rangle = U^\dagger |\psi_{\text{init}}\rangle, \tag{D1}$$

where $|\psi_{\text{init}}\rangle$ denotes the input state, we may write

$$|\psi'\rangle = |\psi_L\rangle + |\psi_U\rangle, \tag{D2}$$

where $|\psi_L\rangle$ and $|\psi_U\rangle$ are two orthogonal states with $|\psi_L\rangle$ denoting the state with the most significant qubit reading 0 and $|\psi_U\rangle$ denotes the state with the most significant qubit reading 1. Because of the CNOT gate between the two boxes, and assuming that the ideal auxiliary qubit state after the two box operations is 0, i.e., the ideal reading of the most significant qubit is 0, we obtain the fidelity of the quantum circuit according to

$$F = |\langle\psi_{\text{init}}|(U|\psi_L\rangle)|^2 = |\langle\psi'|\psi_L\rangle|^2 = |\langle\psi'|\left(|\psi'\rangle - |\psi_U\rangle\right)|^2 = |1 - \langle\psi'|\psi_U\rangle|^2, \tag{D3}$$

where we used (D1) and (D2). Defining the "leakage" probability $P_{\text{leak}} = \langle\psi'|\psi_U\rangle$, we obtain

$$F = |1 - P_{\text{leak}}|^2 = P_{\text{remain}}^2, \tag{D4}$$

which completes the proof.

---

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2000).

[2] Shor, P. W. *Proc. 35th Annual Symp. Foundations of Computer Science* 124-134 (IEEE, 1994).

[3] R. Rivest, A. Shamir, and A. Adleman, *Comm. ACM* **21** (2), 120-126 (1978).

[4] Landauer, R. *Quantum Computing and Communications*, edited by M. Brooks (Springer, 1999), 61.

[5] S. J. Devitt, W. J. Munro, and K. Nemoto, Rep. Prog. Phys. **76** 076001 (2013).

[6] B. M. Terhal, *Rev. Mod. Phys.*, **87**, 307 (2015).

[7] D. Gottesman, An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation, *Proceedings of Symposia in Applied Mathematics*, **68**, 13 (2010).

[8] R. Raussendorf, *Phil. Trans. R. Soc. A*, **370**, 4541-4565 (2011).

[9] N. J. Ross and P. Selinger, Optimal ancilla-free Clifford+T approximation of z-rotations. arXiv:1403.2975v1 [quant-ph] (2014)

[10] V. Kliuchnikov, D. Maslov, and M. Mosca, Quantum Information and Computation **13**, 607 (2013)

[11] V. Kliuchnikov, D. Maslov, and M. Mosca, *IEEE Transactions on Computers* **65**, 161-172 (2016).

[12] F. Gaitan, Quantum Error Correction and Fault Tolerant Computing, (CRC Press, Boca Raton, FL), 2008.

[13] P. W. Shor, *Phys. Rev. A* **52** R2493-R2496 (1995).

[14] A. M. Steane, *Phys. Rev. Lett.* **77**, 793-797 (1996).

[15] A. R. Calderbank and P. W. Shor, *Phys. Rev. A* **54**, 1098-1105 (1996).

[16] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, *Phys. Rev. Lett.* **77** 198 (1996).

[17] P. W. Shor, *Proc. 37th Annual Symp. Foundations of Computer Science* 56-65 (IEEE,1996).

[18] A. M. Steane, *Nature* **399**, 124-126 (1999).

[19] D. Gottesman, *Phys. Rev. A* **57**, 127-137 (1998).

[20] A. Shabani, *Phys. Rev. A* **77**, 022323 (2008).

[21] C.-Y. Lu, W.-B. Gao, J. Zhang, X.-Q. Zhou, T. Yang, and J.-W. Pan, *PNAS* **105**, 11050-11054 (2008).

[22] A. N. Glaudell, E. Waks, and J. M. Taylor, *New J. Phys.* **18**, 093008 (2016).

[23] M. Sargent III, M. O. Scully, and W. E. Lamb, Jr., *Laser Physics* (Addison-Wesley, Reading, MA, 1974).

[24] A. Y. Kitaev, Russ. Math. Surveys **52**, 1191 (1997).

[25] Y. S. Nam and R. Blümel, *Quantum Inf. Process.* **16**, 123 (2017).

[26] R. Blümel and W. P. Reinhardt, *Chaos in Atomic Physics* (Cambridge University Press, Cambridge, 1997).

[27] Y. S. Nam and R. Blümel, *Phys. Rev. A* **88**, 062310 (2013).

[28] Y. S. Nam and R. Blümel, *Phys. Rev. A* **89**, 042337 (2014).

[29] Y. S. Nam and R. Blümel, *Quantum Inf. Comput.* **15**, 721-736 (2015).

[30] D. Castelvecchi, *Nature* **541**, 9-10 (2017).

[31] J. I. Cirac and P. Zoller, *Phys. Rev. Lett.* **74**, 4091-4094 (1995).

[32] A. Steane, *Appl. Phys. B* **64**, 623?643 (1997).

[33] We thank the Monroe quantum computing group at the University of Maryland for valuable discussions.

[34] K. R. Brown, J. Kim, and C. Monroe, *Nature Quantum Information* **2**, 16034 (2016).

[35] J. J. Bollinger, D. J. Heinzen, W. M. Itano, S. L. Gilbert, and D. J. Wineland, *IEEE Trans. Instrum. Meas.* **40**, 126 (1991).

[36] P. T. H. Fisk, M. J. Sellars, M. A. Lawn, and C. Coles, *IEEE Trans. Ultrason. Ferroelectr. Freq. Control* **44**, 344 (1997).

[37] https://en.wikipedia.org/wiki/RSA_numbers#RSA-1024.

[38] C. Miquel, J. P. Paz, and W. H. Zurek, *Phys. Rev. Lett.* **78**, 3971-3974 (1997).

[39] Reference to whoever also uses the fidelity formula ("extensively used in the literature").

[40] S. Beauregard, *Quantum Inf. and Comput.* **3**, 175-185 (2003).

[41] I. L. Markov and M. Saeedi, *Quantum Inf. Comput.* **12**, 361-394 (2012).

[42] C. Miquel, J. P. Paz, and R. Perazzo, *Phys. Rev. A* **54**, 2605-2613 (1996).

[43] L. F. Wei, X. Li, X. Hu, and F. Nori, *Phys. Rev. A* **71**, 022317 (2005).

[44] I. García-Mata, K. M. Frahm, and D. L. Shepelyansky, *Phys. Rev. A* **78**, 062323 (2008).

[45] D. Wecker and K. M. Svore, *LIQUi|>: A software design architecture and domain-specific language for quantum computing*, Preprint at http://arxiv.org/abs/1402.4467 (2014).

[46] H. J. García and I. L. Markov, *IEEE Trans. on Comput.* **64**, 2323-2336 (2014).

[47] T. Häner and D. S. Steiger, arXiv:1704.01127 [quant-ph].

[48] Y. S. Nam and R. Blümel, *Phys. Rev. A* **92**, 042301 (2015).

[49] Y. S. Nam and R. Blümel, *Phys. Rev. A* **87**, 032333 (2013).

[50] N. Huntemann, C. Sanner, B. Lipphardt, Chr. Tamm, and E. Peik, *Phys. Rev. Lett.* **116**,

063001 (2016).

[51] W. Pfeifer, *The Lie Algebras SU(N): An Introduction* (Birkhäuser Verlag, Basel, 2003).

[52] E. L. Hahn, *Phys. Rev.* **80**, 580-594 (1950).

[53] M. V. Berry, N. L. Balazs, M. Tabor, and A. Voros, Ann. Phys. (N.Y.) **122**, 26 (1979).

[54] R. Blümel, *Foundations of Quantum Mechanics – From Photons to Quantum Computers* (Jones and Bartlett, Sudbury, 2010).

[55] J. J. Wallman and J. Emerson, Phys. Rev. A **94**, 052325 (2016).