Physics Letters A ••• (••••) ••••••

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

# Deterministic twirling with low resources

David Jakob Stonner [a], Jaroslav Kysela [b,1], Graeme Weir [b,*], Jaroslav Novotný [b], Gernot Alber [a], Igor Jex [b]

[a] Institut für Angewandte Physik, Technische Universität Darmstadt, Hochschulstraße 4a, D-64289 Darmstadt, Germany
[b] Department of Physics, Faculty of Nuclear Sciences and Physical Engineering, Czech Technical University in Prague, Břehová 7, 115 19 Praha 1-Staré Město, Czech Republic

a r t i c l e i n f o

*Article history:*
Available online xxxx
Communicated by M.G.A. Paris

*Keywords:*
Werner states
Twirling
Entanglement distillation
Quantum operations

a b s t r a c t

Twirling operations, which average a quantum state with respect to a unitary subgroup, have become a frequently-employed tool in quantum information processing. We investigate the efficient implementation of twirling operations with minimal resources, without necessitating the ability to perform all possible unitary operations on the quantum system of interest. We present a general algebraic method allowing us to choose a set of - typically very few - unitary operators which, when applied randomly and repeatedly, produce the given twirling operation exponentially quickly. The method is applied to twirling operations for bipartite quantum systems with respect to the unitary group $\mathcal{U}(d)\otimes\mathcal{U}(d)$, an essential ingredient in entanglement distillation protocols. In particular, we provide a complete classification of sets of unitary operators capable of performing twirling on two qubits. Moreover, we construct a generic set containing at most three unitary operators achieving the twirling operation for a general two-qudit system.



## 1. Introduction

Entanglement, due to its delicate quantum correlations, lies at the heart of numerous quantum information protocols [1–5]. Therefore, our ability to prepare, distribute, and manipulate entanglement efficiently is one of the key factors enabling a significant further advancement of quantum technology. Unfortunately, entanglement is rather fragile and is affected easily even by small interactions of quantum systems with their surroundings [6]. In order to counteract such destructive influences, powerful entanglement distillation protocols have been designed allowing remote participants to prepare, by local means, high-fidelity entangled states even from poorly-entangled shared sources [1]. These protocols rely on the existence of efficient twirling operations which are capable of converting multipartite quantum states into so-called Werner states [7]. In general, a twirling operation $\mathcal{T}$ performs a group averaging over a subgroup $\mathcal{G}$ of the unitary group $\mathcal{U}(d)$, i.e.

$$\mathcal{T}(\rho)=\int_{\mathcal{G}} U\rho U^{\dagger}\mathrm{d}U, \tag{1}$$

with $\rho$ and $\mathrm{d}U$ denoting an arbitrary quantum state and the Haar measure on $\mathcal{G}$, respectively. Furthermore, $d$ is the dimension of the underlying Hilbert space. For finite groups the integral simplifies to a sum over all group elements, normalised by the group order. Twirling operations have interesting applications in numerous areas of quantum information processing, such as quantum distillation processes [1,2], theory of entanglement measures [3–5], resource theory of asymmetry [8,9], quantum reference frames [10,11], quantum secret-sharing [12], data hiding [13], depolarization of quantum channels [14], and the addressability of quantum gates [15].

In the standard approach, a general twirling operation is obtained by applying a sequence of $M$ randomly chosen unitary operators $(U_i)_{i=1}^{M}$ from the group $\mathcal{G}$ randomly to $M$ systems prepared in the same initial state $\rho$: i.e., the output state is given by the averaging operation $\mathcal{T}_M$

$$\rho'=\mathcal{T}_M(\rho)=\frac{1}{M}\sum_{i=1}^{M}U_i\rho U_i^{\dagger}. \tag{2}$$

Practical implementations of this straightforward procedure face two serious issues. Firstly, experimentally it must be possible to realise all required unitary operators from such a group reliably. In general this is a highly demanding task. Secondly, even if this can be accomplished, typically the convergence of such a straightforward procedure scales polynomially with the number of steps (uni-

* Corresponding author.
*E-mail address:* weirgrea@fjfi.cvut.cz (G. Weir).
[1] Present address: Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria.

https://doi.org/10.1016/j.physleta.2019.126179
0375-9601/

taries) involved [16]. However, it was numerically demonstrated [16] that with a clever choice of a few unitary operators, not even necessarily from the group $\mathcal{G}$, which are applied randomly and repeatedly, one can achieve an exponential speedup. Thus, instead of increasing the number of unitary operators, it is significantly more efficient to repeat an averaging operation $\mathcal{T}_m$ with $m$ fixed but well-chosen unitary operators so that after $N$ iterations the quantum system is in the state

$$\rho' = (\mathcal{T}_m)^N(\rho). \tag{3}$$

Such an iterative procedure can result in an exponential convergence towards the desired group averaging operation. Simultaneously it requires significantly less resources. Motivated by this advantage of the latter procedure, in this paper we present a general algebraic method addressing the crucial practical question of how to choose the set of unitary operators $(U_i)_{i=1}^m$ whose repeated random application approximates a given group-averaging operation exponentially quickly. In the following, this method will be applied not only to the twirling of two qubits by providing a characterisation of an arbitrary number of unitary operators achieving this goal, but we will also present generic sets containing at most three unitary operators which achieve twirling exponentially quickly in arbitrary finite-dimensional bipartite quantum systems.

## 2. A general algebraic method

We present a general method for determining the set of unitary operators $(U_i)_{i=1}^m$ of a random unitary operation (RUO)

$$\mathcal{R}(\rho) = \sum_{i=1}^{m} p_i U_i \rho\, U_i^\dagger \tag{4}$$

which efficiently approximates a given twirling operation (1) by the iterative evolution (3). Thereby, the quantities $p_i > 0$ with $i = 1, ..., m$ and $\sum_{i=1}^m p_i = 1$ describe the probabilities with which the corresponding unitary operator $U_i$ is applied. The asymptotic regime of the generated iterative evolution is well-understood in terms of attractors of an attractor space $\mathsf{Attr}(\mathcal{R})$ associated with the given RUO [17,18]. This attractor space is defined as the span of all eigenvectors of the map $\mathcal{R}$ associated with eigenvalues of the asymptotic spectrum: i.e.,

$$\mathsf{Attr}(\mathcal{R}) := \bigoplus_{\lambda\in\sigma_{\mathrm{as}}} \mathsf{Ker}(\mathcal{R} - \lambda\mathbb{1}), \tag{5}$$

with the asymptotic spectrum $\sigma_{\mathrm{as}}$ being defined as the set of eigenvalues of $\mathcal{R}$ with unit modulus. Once an orthonormal basis $X_{\lambda,i}$ of the individual attractor eigenspaces $\mathsf{Ker}(\mathcal{R} - \lambda\mathbb{1})$ with respect to the Hilbert-Schmidt scalar product $(X, Y)_{\mathrm{HS}} = \mathrm{Tr}\{X^\dagger Y\}$ is known, the asymptotic dynamics of any initial state $\rho$ after sufficiently many steps $n$ is given by

$$\rho_\infty(n) = \sum_{\lambda\in\sigma_{as},i} \lambda^n (X_{\lambda,i}, \rho)_{\mathrm{HS}} X_{\lambda,i} \tag{6}$$

so that $\|\mathcal{R}^n\rho - \rho_\infty(n)\| \to 0$ for $n \to \infty$.

Due to properties of the Haar measure of a group $\mathcal{G}$, a general twirling operation (1) is an orthogonal projection. Therefore, the evolution generated by the RUO (4) converges to the desired twirling operation (1) if and only if the asymptotic spectrum $\sigma_{\mathrm{as}}$ of $\mathcal{R}$ contains solely the eigenvalue $\lambda = 1$ and, simultaneously, the range of the twirling operation $\mathcal{T}$ coincides with the set of fixed points of $\mathcal{R}$, i.e.,

$$\mathsf{Ran}(\mathcal{T}) = \mathsf{Attr}(\mathcal{R}) = \mathsf{Ker}(\mathcal{R} - \mathbb{1}). \tag{7}$$

Moreover, the attractor eigenspaces $\mathsf{Ker}(\mathcal{R} - \lambda\mathbb{1})$ are determined by the set of attractor equations

$$U_i X_{\lambda,i} = \lambda X_{\lambda,i} U_i, \tag{8}$$

which must be satisfied by the attractors $X_{\lambda,i}$ simultaneously for all unitary operators $(U_i)_{i=1}^m$. The attractor equations (8) provide a convenient algebraic tool for deciding whether the convergence conditions (7) are fulfilled by a given set of unitary operators $(U_i)_{i=1}^m$ generating the RUO (4). Note also that the assigned probabilities $(p_i)_{i=1}^m$ do not affect the resulting asymptotic dynamics of a RUO. This can be exploited to further speed up the convergence of the iterated dynamics towards the desired twirling operation. As a further consequence of the attractor equations (8) we obtain the result that the range of the twirling operation over the group $\mathcal{G} = \langle U_1, ..., U_m\rangle$ (i.e., the group generated by the unitary operators $U_1, ..., U_m$) equals the set of fixed points of $\mathcal{R}$, i.e., $\mathsf{Ran}(\mathcal{T}) = \mathsf{Ker}(\mathcal{R} - \mathbb{1})$. Therefore, the group $\mathcal{G}$ determines the asymptotic limit of the evolution generated by the RUO (4), in the case that this limit exists.

Finally, we conclude that the iterative evolution (3) driven by the RUO (4) approaches the twirling operation (1) if and only if all elements of the range of the twirling operation (1) are solutions of the attractor equations (8) for $\lambda = 1$ and there is no other solution. In the following we apply this algebraic method to investigate which sets of unitaries are suitable to approximate the twirling of pairs of finite-dimensional qudits averaged over the group $\mathcal{U}(d)\otimes\mathcal{U}(d) := \{U\otimes U \mid U\in\mathcal{U}(d)\} \subseteq \mathcal{U}(d^2)$.

## 3. Twirling and Werner states

Entanglement distillation protocols [1] exploit twirling operations as one of the tools which brings a weakly entangled composite quantum system into a Werner state by local operations and classical communication [19], i.e. without mutual interaction between the individual subsystems. In general, Werner states, introduced in [7], are mixed $N$-qudit states $\rho$, supported on the Hilbert space $\mathcal{H} \simeq (\mathbb{C}^d)^{\otimes N}$, which are left unaltered if all qudits involved undergo the same local unitary evolution, i.e.,

$$U^{\otimes N}\rho\, U^{\otimes N\dagger} = \rho \tag{9}$$

for all unitary single-qudit operators $U \in \mathcal{U}(d)$. Correspondingly, these states can be obtained as twirled states resulting from the twirling operation

$$\mathcal{P}(\rho) := \int_{\mathcal{U}(d)} U^{\otimes N}\rho\, U^{\otimes N\dagger} \mathrm{d}U \tag{10}$$

with the Haar measure $\mathrm{d}U$ on the unitary group $\mathcal{U}(d)$. Note that $\mathcal{P}$ coincides with $\mathcal{T}$ from Eq. (1) for $\mathcal{G} = \mathcal{U}(d)^{\otimes N}$. Such a twirling operation maps any state $\rho$ to a Werner state and, conversely, every Werner state is contained in the range of $\mathcal{P}$. In the case of bipartite Hilbert spaces, the description of Werner states simplifies significantly [7]. They form a one-parameter family of states which are a mixture of symmetric and antisymmetric states, i.e.,

$$\rho = \eta\frac{2}{d(d+1)}P_{\mathrm{sym}} + (1-\eta)\frac{2}{d(d-1)}P_{\mathrm{asym}} \tag{11}$$

for $0 \le \eta \le 1$. Here $P_{\mathrm{sym}}$ and $P_{\mathrm{asym}}$ are the projections onto the symmetric and antisymmetric eigenspaces of the flip operator $F|\phi\rangle|\psi\rangle := |\psi\rangle|\phi\rangle$ corresponding to the eigenvalues 1 and $-1$, respectively.

Please cite this article in press as: D.J. Stonner et al., Deterministic twirling with low resources, Phys. Lett. A (2020), https://doi.org/10.1016/j.physleta.2019.126179

### 3.1. Twirling of two qubits

The simplest situation arises for a twirling operation (10) acting on two qubits. In such a case we have $P_{\text{asym}} = |\psi_-\rangle\langle\psi_-|$ with the singlet state $|\psi_-\rangle := 1/\sqrt{2}\,(|1\rangle|0\rangle - |0\rangle|1\rangle)$. Consequently, according to condition (7), asymptotically the two-qubit twirling operation (10) can be achieved by iteration of the RUO (4) if and only if

$$\text{Attr}(\mathcal{R}) = \text{span}\left\{\mathbb{1}, |\psi_-\rangle\langle\psi_-|\right\}. \tag{12}$$

Therefore, a natural question arises: what is the most general form of the set of unitary operators $(U_i)_{i=1}^m$ capable of asymptotically generating a Werner state? Employing the attractor equations (8), we can provide an exhaustive answer.

First of all let us focus on a scenario with only two unitary operators, say $U_1 = u_1 \otimes u_1$ and $U_2 = u_2 \otimes u_2$. Without loss of generality $u_1, u_2 \in SU(2)$ and the computational basis of both qubit systems can be chosen in such a way that the matrix representation of one of these unitary single qubit operations, say $u_1$, is diagonal, i.e.,

$$u_1 = \begin{bmatrix} e^{i\varphi} & 0 \\ 0 & e^{-i\varphi} \end{bmatrix} \tag{13}$$

with $\varphi \in [0, 2\pi)$, and that the matrix representation of the second unitary single qubit operation $u_2$ takes the general form

$$u_2 = \begin{bmatrix} e^{i\theta}\cos(\gamma) & -e^{-i\mu}\sin(\gamma) \\ e^{i\mu}\sin(\gamma) & e^{-i\theta}\cos(\gamma) \end{bmatrix} \tag{14}$$

with $\theta, \mu \in [0, 2\pi)$, $\gamma \in [0, \pi)$. By explicit solution of the attractor equations (8) it can be shown that RUOs involving the corresponding unitary two-qubit operators $U_1$ and $U_2$ converge asymptotically to a Werner state for arbitrary probabilities $p_1, p_2 = (1 - p_1) \in (0, 1)$, if and only if the parameters $\varphi, \gamma, \theta$ satisfy one of the following relations:

- $\varphi \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$ and $\gamma \notin \{0, \frac{\pi}{2}\}$ and $\theta \notin \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$;
- $\varphi \notin \{\frac{\pi}{2}, \frac{3\pi}{2}\}$ and $\gamma \notin \{0, \frac{\pi}{2}\}$;

independently of $\mu$. For more than two unitary operators involved in the iterative generation of Werner states, i.e., $m > 2$, we can generalise the necessary and sufficient condition for convergence in the following way. Again we can always choose a computational basis such that one of our matrices, say $u_{i_0}$, is diagonal for some $i_0 \in I := \{1, \ldots, m\}$ and is characterised by a single parameter, say $\varphi_{i_0}$, analogous to Eq. (13). Each of the remaining matrices $u_j$ with $i_0 \neq j \in I$ is parametrised by three parameters $\gamma_j^{(i_0)}, \theta_j^{(i_0)}, \mu_j^{(i_0)}$ in analogy to equation (14). The iterative dynamics (3) generated by RUO (4) with $(U_i = u_i \otimes u_i)_{i=1}^m$ converge towards the two-qubit twirling operation (10) if and only if one of the following twirling conditions holds:

- If $\text{Tr}(u_{i_0}) \neq 0$ for some $i_0 \in I$, then there is some $i_0 \neq j \in I$, for which $\gamma_j^{(i_0)} \notin \{0, \frac{\pi}{2}\}$.
- If $\text{Tr}(u_i) = 0$ for all $i \in I$, we choose an arbitrary $i_0 \in I$ and associated $u_{i_0}$. Then there exist $j, k_1, k_2 \in I \setminus \{i_0\}$ such that $\gamma_j^{(i_0)} \notin \{0, \frac{\pi}{2}\}$, and $\mu_{k_1}^{(i_0)} \neq \mu_{k_2}^{(i_0)} + r\frac{\pi}{2}$ for all $r \in \mathbb{Z}$.

The proof of both statements is straightforward but lengthy and is presented in Ref. [20]. An immediate consequence of these statements is that for any random choice of operators $(u_i)_{i=1}^m$ the associated iterated RUO prepares Werner states asymptotically. Numerical evidence suggests that this is also the case for qudits with $d > 2$ (see Fig. 2). Furthermore, the above mentioned characterisation of two-qubit twirling for RUOs involving an arbitrary number of unitary operators $(U_i)_{i=1}^m$ implies that any RUO (4) that prepares Werner states gives rise to another RUO that also prepares Werner states, using at most four of the original unitary operators $U_i$.

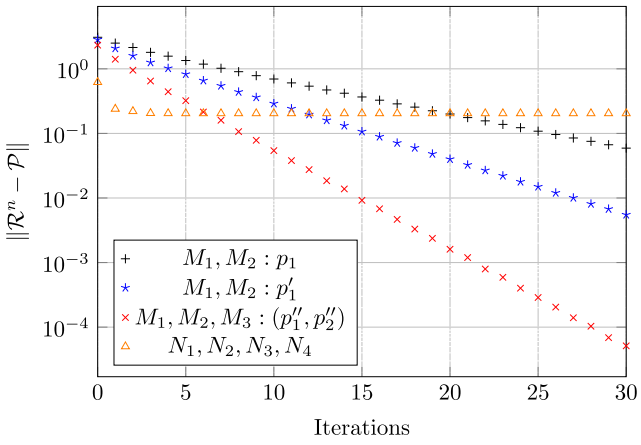


**Fig. 1.** Hilbert-Schmidt distance between the two-qubit twirling operation (10) and the iterated RUO associated with the given unitary operators as a function of the number of iterations: The involved RUOs are given by two unitary operators $M_1, M_2$ with probabilities $p_1 = 0.75$ (black, plus); two unitary operators $M_1, M_2$ with optimised probabilities $p_1' = 0.459$ (blue, star); three unitary operators $M_1, M_2, M_3$ with optimised probabilities $(p_1'', p_2'') = (0.41, 0.18)$ (red, cross); and four unitary operators $(N_i)$ avoiding the twirling conditions (yellow, triangle). The Hilbert-Schmidt norm is plotted on a logarithmic scale. (For interpretation of the colours in the figure(s), the reader is referred to the web version of this article.)

In [18] it was shown that the convergence of the iterated dynamics (3) generated by a RUO towards its asymptotic regime is exponential with the number of iterations. However, one can further improve the rate of convergence by properly chosen unitary operators $U_i$ and their associated probabilities $p_i$, provided they follow the twirling conditions. In Fig. 1 we compare exponential convergence rates of the iterated dynamics for different chosen settings with unitary operators $M_1, M_2$ and $M_3$ defined via parameters $\varphi_1 = \frac{\pi}{4}, \theta_2 = \frac{\pi}{4}, \mu_2 = 0, \gamma_2 = \frac{\pi}{4}, \theta_3 = 0, \mu_3 = \frac{\pi}{4}, \gamma_3 = \frac{\pi}{4}$. This figure demonstrates how optimised probabilities or an extension of the set of unitary operators may significantly speed up the resulting convergence. Fig. 1 also shows an example of a RUO whose four involved unitary operators $(N_i)$ do not follow the twirling conditions ($\text{Tr}(N_1) \neq 0$, and $\gamma_j^{(1)} \in \{0, \frac{\pi}{2}\}$ for all $j \in I \setminus \{1\}$).

### 3.2. Twirling of two qudits

It is a demanding task to derive the analogous necessary and sufficient conditions which generalise the results of Sec. 3.1 to two-qudit twirling operations (10). In this section we restrict ourselves to the less difficult but practically interesting problem of determining a generic set of three unitary operators capable of implementing the twirling operation (10) asymptotically for any finite dimension $d \geq 2$ of the underlying Hilbert space. For this purpose let us consider an arbitrary finite-dimensional bipartite qudit system with Hilbert space $\mathcal{H} \simeq \mathbb{C}^d \otimes \mathbb{C}^d$ and let us fix some orthonormal basis $|1\rangle, \ldots, |d\rangle$ on both qudit subsystems. Furthermore, let $\mathcal{R}$ be the RUO (4) with unitary operators $U_i = u_i \otimes u_i$ for $u_1 = h, u_2 = u$ and $u_3 = v$, and let the relevant single-qudit unitary operators be defined by

- $h\,|k\rangle := \exp\left(2^{k-d}\pi i\right)|k\rangle$,
- $u\,|k\rangle := |(k \bmod d) + 1\rangle$,
- $v := A \oplus \mathbb{1}_{d-2}$, where $A \in \mathcal{U}(2)$ has no vanishing entries.

We now prove that if $\mathcal{R}$ is asymptotically stationary then this RUO prepares Werner states asymptotically, i.e., $\mathcal{R}^n$ converges to $\mathcal{P}$ (10).

**Proof.** According to the equations (7) and (11), it suffices to show that $\mathsf{Ker}(\mathcal{R}-\mathbb{1}) = \mathsf{span}\{P_{\mathrm{sym}}, P_{\mathrm{asym}}\}$. From the definition of Werner states, it is clear that $\mathsf{Ker}(\mathcal{R}-\mathbb{1}) \subseteq \mathsf{span}\{P_{\mathrm{sym}}, P_{\mathrm{asym}}\}$. In order to show the other inclusion, we introduce the orthonormal basis $B$ consisting of the vectors

$$\begin{aligned} |\phi_i\rangle &:= |i\rangle\,|i\rangle\,, \\ |\phi_{i,j}\rangle &:= \frac{1}{\sqrt{2}}(|i\rangle\,|j\rangle + |j\rangle\,|i\rangle), \\ |\psi_{i,j}\rangle &:= \frac{1}{\sqrt{2}}(|i\rangle\,|j\rangle - |j\rangle\,|i\rangle) \end{aligned} \tag{15}$$

with $i<j \in \{1,\ldots,d\}$. These states are the eigenbasis of the flip operator $F$ so that $P_{\mathrm{sym}}$ and $P_{\mathrm{asym}}$ are diagonal with respect to $B$. Thus, by equation (11), it suffices to show that any eigenvector $X \in \mathsf{Ker}(\mathcal{R}-\mathbb{1})$ is diagonal with respect to $B$ and that the diagonal matrix elements corresponding to $P_{\mathrm{sym}}$ and $P_{\mathrm{asym}}$ coincide, respectively.

If $X \in \mathsf{Ker}(\mathcal{R}-\mathbb{1})$ the attractor equations (8) imply the relations

$$h^\dagger \otimes h^\dagger X\, h\otimes h = u^\dagger \otimes u^\dagger X\, u\otimes u = v^\dagger \otimes v^\dagger X\, v\otimes v = X.$$

As $h\otimes h$ is diagonal with respect to $B$, we can write $h\otimes h = \sum_{i=1}^d h_i\,|b_i\rangle\langle b_i|$ with basis vectors $|b_i\rangle \in B$ and $|h_i|=1$. We find

$$\langle b_i|\,X\,|b_j\rangle = \langle b_i|\,h^\dagger\otimes h^\dagger X\, h\otimes h\,|b_j\rangle = h_i h_j^*\,\langle b_i|\,X\,|b_j\rangle$$

for all $i$ and $j$, which implies that we have $\langle b_i|\,X\,|b_j\rangle = 0$ whenever $h_i \neq h_j$. Using the choice of the diagonal entries of $h$, it follows that the only non-vanishing non-diagonal matrix elements of $X$ with respect to $B$ are $\langle\phi_{i,j}|\,X\,|\psi_{i,j}\rangle$ and $\langle\psi_{i,j}|\,X\,|\phi_{i,j}\rangle$ for $i<j$.

Moreover, since we have $u^\dagger\otimes u^\dagger X\; u\otimes u = X$, it follows that matrix elements of $X$ corresponding to the same orbit of $u\otimes u$, acting on the basis $B$, have to coincide. Note that each of these orbits contains at least one of the vectors in Eq. (15) with $i=1$. Thus, it remains to show that $\langle\phi_{1,k}|\,X\,|\psi_{1,k}\rangle = 0 = \langle\psi_{1,k}|\,X\,|\phi_{1,k}\rangle$, $\langle\phi_{1,k}|\,X\,|\phi_{1,k}\rangle = \langle\phi_1|\,X\,|\phi_1\rangle$ and $\langle\psi_{1,k}|\,X\,|\psi_{1,k}\rangle = \langle\psi_{1,2}|\,X\,|\psi_{1,2}\rangle$ for all $1<k\leq d$. Using a parametrisation of $A$ of the form

$$A = \mathrm{e}^{i\varphi}\begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha}\end{bmatrix}, \tag{16}$$

for $\alpha\neq 0\neq\beta$ and $|\alpha|^2+|\beta|^2=1$, the validity of these equations can be shown by straightforward calculation and induction. □

In general the RUO $\mathcal{R}$ is not necessarily asymptotically stationary for all choices of $A\in\mathcal{U}(2)$. However, the attractor equations (8) imply that the condition $\bigcap_{i=1}^m\{\lambda\lambda^* \mid \lambda\in\sigma(U_i)\}\subseteq\{1\}$ is sufficient for asymptotic stationarity of a RUO (4), which can be used to show that $\mathcal{R}$ is asymptotically stationary for almost all choices of $A$, i.e., the set of parameters of $A$ for which $\mathcal{R}$ is not guaranteed to be asymptotically stationary has measure zero [21]. The presented construction depends on six continuous independent real-valued parameters, namely $p_1, p_2$ and the four parameters defining a particular unitary operator $A\in\mathcal{U}(2)$ (compare with Eq. (16)). Thus, this construction has the advantage that these parameters can be varied in order to optimise the convergence rate of the iterated RUO. Furthermore, since the eigenspace $\mathsf{Ker}(\mathcal{R}-\mathbb{1})$ is completely determined by the (possibly countably infinite) group $\mathcal{G}=\langle h,u,v\rangle$ generated by the operators $h,u$ and $v$, this construction gives rise to a whole family of RUOs satisfying $\mathsf{Ker}(\mathcal{R}-\mathbb{1}) = \mathsf{span}\{P_{\mathrm{sym}}, P_{\mathrm{asym}}\}$. It is also possible to generalise this construction without having to change the crucial arguments of the proof. For instance, the non-trivial part of $v$ could be defined on any other two-dimensional subspace of $\mathbb{C}^d$ or $u$ could be replaced by any other unitary operator that acts transitively on the fixed orthonormal basis, and one could introduce additional parameters into its definition.

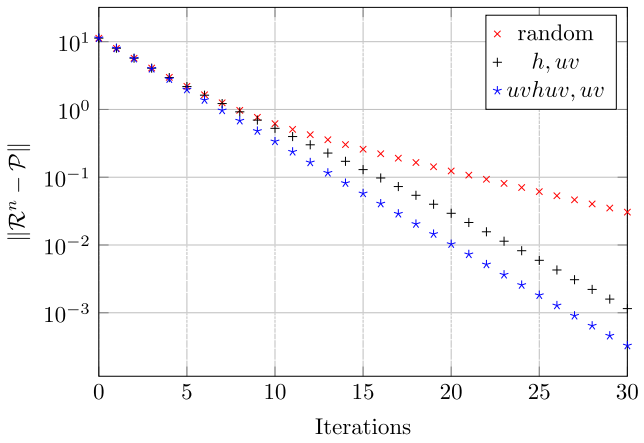


**Fig. 2.** Hilbert-Schmidt distance between the two-qudit twirling operation (10) and the iterated RUO associated with the given unitary operators as a function of the number of iterations, in dimension $d=4$: The involved RUOs are given by two randomly generated unitary operators (red, cross), the two unitary operators $h$ and $uv$ (black, plus) and the two unitary operators $uvhuv$ and $uv$ (blue, stars). The probability distribution $p_1, p_2 = 1-p_1$ has been optimised numerically in each case, in order to obtain the fastest possible convergence. The Hilbert-Schmidt norm is plotted on a logarithmic scale.

If the dimension $d$ characterising the qudits is an odd number, then it is possible to show that the RUO $\mathcal{R}_2$ involving only the two unitary operators $U_1 = h\otimes h$ and $U_2 = uv\otimes uv$ (according to Eq. (4)) also satisfies $\ker(\mathcal{R}_2-\mathbb{1}) = \mathsf{span}\{P_{\mathrm{sym}}, P_{\mathrm{asym}}\}$. Thus, if it is asymptotically stationary then $\mathcal{R}_2$ prepares Werner states asymptotically as well [21]. Even though all the crucial arguments of the above proof stay valid in such a case, the calculations get much more involved. Numerical evidence suggests the conjecture that this construction may also work in even dimensions. Indeed, Fig. 2 shows the convergence of the iterated dynamics (3) generated by the RUO $\mathcal{R}_2$ in dimension $d=4$. It is compared with the iterated dynamics generated by RUO (4) with two randomly chosen unitary operators $u_1, u_2 \in \mathcal{U}(4)$ and $U_i = u_i\otimes u_i$, as well as with a RUO with $u_1 = uvhuv$ and $u_2 = uv$. Note that the generated groups $\langle uvhuv, uv\rangle$ and $\langle h, uv\rangle$ coincide. In order to obtain fast convergence, the values of the probabilities $p_i$ and the parameters $\alpha,\beta,\varphi$ according to Eq. (16) have been optimised using a sequential least squares algorithm for a large number of randomly chosen initial values. The figure demonstrates the significant advantage, in terms of convergence rates, of optimising continuous parameters instead of choosing them at random.

## 4. Conclusions

Werner states are of considerable interest in the field of quantum information and have useful practical applications in the important area of entanglement purification [1,2]. It is therefore of great utility to be able to generate these states in a manner which is both experimentally easy to implement and quick to converge.

In this work we give a general recipe for how to choose unitary operators which, applied randomly and repeatedly, efficiently approximate a given twirling operation. This method is applied to investigate procedures allowing us to generate Werner states using random unitary operations. Firstly, we found a set of criteria which any set of unitary operators $(U_i)_{i=1}^m$ generating a RUO must satisfy in order to bring a two-qubit system into a Werner state asymptotically for arbitrary $m\geq 2$. Secondly, we formulated a procedure

for generating bipartite Werner states in arbitrary finite dimension $d \geq 2$ using RUOs. This can be achieved using only three unitary operators, and in fact there are infinitely many such triplets which yield this result. Furthermore, if $d$ is odd we only need two unitary operators. There is numerical evidence to conjecture that this is also true for even dimensions $d$.

It is shown that various RUOs may be chosen to generate the same desired twirling operation exponentially quickly with the number of iterations. By adjusting parameters specifying unitary operators and their associated probabilities one can significantly improve the convergence rate. A systematic exploration of the issue of convergence rates is beyond the scope of this paper, although some first results are presented here. Another avenue which might be explored in the future on the basis of our results is the question of whether RUOs might be generalised to generate other states, for instance isotropic states - i.e., bipartite qudit states which are invariant under the operation $U \otimes U^*(.)\ U^\dagger \otimes U^{*\dagger}$ for all $U \in \mathcal{U}(d)$ acting on one qudit [22–24].

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgements

JN, GW and IJ acknowledge the financial support from MŠMT No. 8J18DE011, RVO14000 and “Centre for Advanced Applied Sciences”, Registry No. CZ.02.1.01/0.0/0.0/16_019/0000778, supported by the Operational Programme Research, Development and Education, co-financed by the European Structural and Investment Funds and the state budget of the Czech Republic. JN and IJ are supported by the Czech Science Foundation (GACR) project number 16-09824S. IJ was partially supported from GACR 17-00844S. JS, JN and GA acknowledge support by the DAAD (PPP-Tschechien, 57390900) and by the Center of Excellence “Crossing” funded by the DFG.

## References

[1] Charles H. Bennett, et al., Purification of noisy entanglement and faithful teleportation via noisy channels, Phys. Rev. Lett. 76 (5) (1996) 722.
[2] H. Bombin, Miguel Angel Martin-Delgado, Entanglement distillation protocols and number theory, Phys. Rev. A 72 (3) (2005) 032313.
[3] Karl Gerd H. Vollbrecht, Reinhard F. Werner, Entanglement measures under symmetry, Phys. Rev. A 64 (6) (2001) 062307.
[4] Soojoon Lee, et al., Convex-roof extended negativity as an entanglement measure for bipartite quantum systems, Phys. Rev. A 68 (6) (2003) 062304.
[5] Masahito Hayashi, et al., Entanglement of multiparty-stabilizer, symmetric, and antisymmetric states, Phys. Rev. A 77 (1) (2008) 012104.
[6] Jaroslav Novotný, Gernot Alber, Igor Jex, Entanglement and decoherence: fragile and robust entanglement, Phys. Rev. Lett. 107 (2011) 090501.
[7] Reinhard F. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, Phys. Rev. A 40 (8) (1989) 4277.
[8] Iman Marvian, Robert W. Spekkens, The theory of manipulations of pure state asymmetry: I. Basic tools, equivalence classes and single copy transformations, New J. Phys. 15 (3) (2013) 033001.
[9] Iman Marvian, Robert W. Spekkens, Paolo Zanardi, Quantum speed limits, coherence, and asymmetry, Phys. Rev. A 93 (5) (2016) 052331.
[10] Joan Alfina Vaccaro, et al., Tradeoff between extractable mechanical work, accessible entanglement, and ability to act as a reference system, under arbitrary superselection rules, Phys. Rev. A 77 (3) (2008) 032114.
[11] Michael Skotiniotis, Gilad Gour, Alignment of reference frames and an operational interpretation for the G-asymmetry, New J. Phys. 14 (7) (2012) 073022.
[12] Vlad Gheorghiu, Generalized semiquantum secret-sharing schemes, Phys. Rev. A 85 (5) (2012) 052309.
[13] David P. DiVincenzo, et al., Quantum data hiding, IEEE Trans. Inf. Theory 48 (3) (2002) 580–598.
[14] Wolfgang Dür, et al., Standard forms of noisy quantum operations via depolarization, Phys. Rev. A 72 (5) (2005) 052326.
[15] Jay M. Gambetta, et al., Characterization of addressability by simultaneous randomized benchmarking, Phys. Rev. Lett. 109 (24) (2012) 240504.
[16] Géza Tóth, Juan José García-Ripoll, Efficient algorithm for multiqudit twirling for ensemble quantum computation, Phys. Rev. A 75 (4) (2007) 042311.
[17] Jaroslav Novotný, Gernot Alber, Igor Jex, Random unitary dynamics of quantum networks, J. Phys. A, Math. Theor. 42 (28) (2009) 282003.
[18] Jaroslav Novotný, Gernot Alber, Igor Jex, Asymptotic evolution of random unitary operations, Cent. Eur. J. Phys. 8 (6) (2010) 1001–1014.
[19] Michael A. Nielsen, Isaac Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000.
[20] Jaroslav Kysela, Twirling operations in quantum algorithms, Bachelor’s Thesis, 2013, https://physics.fjfi.cvut.cz/publications/mf/2013/bp_mf_13_Kysela.pdf.
[21] David Jakob Stonner, Construction of random unitary operations for asymptotic preparation of Werner states, Bachelor’s Thesis, 2019.
[22] Gernot Alber, et al., Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments, Springer, 2003.
[23] Barbara M. Terhal, Karl Gerd, H. Vollbrecht, Entanglement of formation for isotropic states, Phys. Rev. Lett. 85 (12) (2000) 2625.
[24] Pranaw Rungta, Carlton M. Caves, Concurrence-based entanglement measures for isotropic states, Phys. Rev. A 67 (1) (2003) 012307.