Constructing Four-Photon States for Quantum Communication and Information Processing

Gregg Jaeger · Alexander Sergienko

Abstract We provide a method for constructing a set of four-photon states suitable for quantum communication applications. Among these states is a set of concatenated quantum code states that span a decoherence-free subspace that is robust under collective-local as well as global dephasing noise. This method requires only the use of spontaneous parametric down-conversion, quantum state post-selection, and linear optics. In particular, we show how this method can be used to produce all sixteen elements of the second-order Bell gem $\mathcal{G}_{16}$, which includes these codes states and is an orthonormal basis for the Hilbert space of four qubits composed entirely of states that are fully entangled under the four-tangle measure.

Keywords Quantum computing · Quantum coding · Entangled photons · Bell states

1 Introduction

It is advantageous for quantum information processing in practical situations to make use of decoherence-free subspaces (DFSs) for quantum decoherence mitigation or codes for quantum error-correction (QECCs) [9]. DFSs are properly called so only for the specific sort of noise under which they are, in fact, immune to decoherence, for example, in the form of the collective local dephasing of individual qubits. In such collective local dephasing, each qubit evolves as $|0\rangle \to |0\rangle$ and $|1\rangle \to e^{i\langle\chi\rangle}|1\rangle$, where $\langle\chi\rangle$ is an average of random phases shifts [7]. The existence of two conjugate bases, which each provide a pair of orthogonal logical-qubit states, for the same DFS enables single-qubit dephasing-noise-immune quantum key distribution (QKD) under the BB84 protocol [11]. However, the two-qubit DFS spanned by the qubit states $|01\rangle, |10\rangle$, as well as by the Bell states $|\Psi^+\rangle, |\Psi^-\rangle$, proposed for this purpose

G. Jaeger (✉)
Quantum Imaging Laboratory and College of General Studies, Boston University, Boston,
MA 02215, USA
e-mail: jaeger@bu.edu

A. Sergienko
Quantum Imaging Laboratory, Department of Electrical and Computer Engineering, and Department
of Physics, Boston University, Boston, MA 02215, USA

is immune to collective dephasing at the single-qubit scale but not global dephasing at the *two-qubit* scale. Nonetheless, by using logical-qubit states of a concatenated quantum code, specifically, elements of the Bell gem $\mathcal{G}_{16}$ described here, a dephasing-free subspace that is at the same time robust against one-qubit collective local *and* two-qubit global dephasing can be used that enables quantum information processing and quantum communication in environments where dephasing noise occurs both at the one-qubit level and at the two-qubit level [3].

Recently, a hierarchy of recursively defined sets of qubit states, the Bell gems, was introduced, elements of which can be used for error-correctable quantum computing as well as such two-scale-noise-immune quantum cryptography [2]. The elements of these sets of states share formal symmetry properties with the states of the Bell basis in terms of which the Bell gems are recursively defined. Here, we provide a *practical method* for constructing the Bell-gem states one level of scale above that of the Bell basis, namely, those of the Bell gem $\mathcal{G}_{16}$, which is defined on the Hilbert space of four qubits. Moreover, we show that these states can be produced in the laboratory using only the readily available spontaneous parametric down-conversion, quantum state post-selection, and linear optics. Specifically, we first show how the subset of these states that are concatenated quantum code states useful for two-scale-dephasing-free quantum key distribution can be so constructed in the polarization subspace of four-photons. We then go on to show how the *complete set* of states of the second-order Bell gem $\mathcal{G}_{16}$, which forms a basis of entangled states for the entire four-photon polarization subspace, according to the four-tangle measure, can be so constructed.

2 Bell Gem States for Quantum Communication

Self-similar quantum states have recently been identified in the context of quantum information processing, where quantum parallelism involves the exploitation of quantum states with large numbers of computational-basis components. In particular, the existence of a specific class of sets of self-similar entangled quantum states forming bases, known as Bell gems, for the Hilbert spaces of the systems they describe was found to include states useful for quantum error correction and quantum computation using four qubits [2]. These bases can be viewed formally as arising from the concatenation of quantum codes [5]. The states constituting them are a subset of the broader class of self-similar quantum fractal states [3].

States of the two-qubit decoherence-free subspaces proposed for use in QKD, discussed in [11] and elsewhere, are susceptible to decoherence in global-noise-filled environments. Specifically, environmental noise that dephases two-qubit logical states via the process

$$|0\rangle_{\mathrm{L}} \to |0\rangle_{\mathrm{L}}, \tag{1}$$

$$|1\rangle_{\mathrm{L}} \to e^{i\langle\bar{\chi}\rangle}|1\rangle_{\mathrm{L}}, \tag{2}$$

$\langle\bar{\chi}\rangle$ being an average random phase in superpositions of two-qubit states, in addition to single-qubit dephasing described in the introduction, dephases the logical states $|i\rangle_{\mathrm{L}}$ of the two-qubit decoherence-free subspace described in the previous section, rendering them susceptible to dephasing-induced errors. That two-qubit decoherence-free subspace is therefore no longer decoherence free in such a noise environment. However, it is known that when a single quantum code is repeatedly concatenated, the resulting code can be used to mitigate decoherence and bound quantum errors at a number of scales [6]. Such concatenated quantum codes produce quantum states at a number of scales resulting in a self-similar set of

quantum states [4]. In particular, the two elements of the Bell gem $\mathcal{G}_{16}$ produced by concatenating with itself the code using states $|0\rangle_L \equiv |\Psi^+\rangle$, $|1\rangle_L \equiv |\Psi^-\rangle$ remain robust under such collective dephasing noise; a subspace immune to two-scale dephasing thus results from repeating the encoding procedure for the production of the above two-qubit decoherence-free subspaces by encoding the logical qubit states $\{|0\rangle_L, |1\rangle_L\}$ themselves into more logical qubits at the four physical-qubit level.

In principle, by repeated concatenation of this code, an extremely large subspace that is decoherence-free at many scales of collective dephasing results. Formally, the concatenation process can be continued as long as necessary, producing increasingly robust logical qubits that, however, require an exponentially larger number of qubits with linear changes in scale. Continuing this process indefinitely produces a fractal quantum state [3]. Producing Fock states at the next level of concatenation beyond that of $\mathcal{G}_{16}$, namely, the eight-qubit level, is beyond the scope of current optical technology. We therefore restrict ourselves here to what can *now* be achieved in practice, which are the four-qubit states of the Bell gem $\mathcal{G}_{16}$. Specifically, the sixteen elements of this four-qubit Bell gem forming a basis for $\mathcal{H}_{16} = \mathcal{C}_2^{\otimes 2^2}$ can be written

$$\mathcal{G}_{16} = \left\{ \frac{1}{\sqrt{2}}(|\Phi^+\rangle|\Phi^+\rangle \pm |\Phi^-\rangle|\Phi^-\rangle), \right. \tag{3}$$

$$\frac{1}{\sqrt{2}}(|\Psi^+\rangle|\Psi^+\rangle \pm |\Psi^-\rangle|\Psi^-\rangle), \tag{4}$$

$$\frac{1}{\sqrt{2}}(|\Phi^+\rangle|\Phi^-\rangle \pm |\Phi^-\rangle|\Phi^+\rangle), \tag{5}$$

$$\frac{1}{\sqrt{2}}(|\Phi^+\rangle|\Psi^+\rangle \pm |\Psi^+\rangle|\Phi^+\rangle), \tag{6}$$

$$\frac{1}{\sqrt{2}}(|\Phi^+\rangle|\Psi^-\rangle \pm |\Psi^-\rangle|\Phi^+\rangle), \tag{7}$$

$$\frac{1}{\sqrt{2}}(|\Phi^-\rangle|\Psi^+\rangle \pm |\Psi^+\rangle|\Phi^-\rangle), \tag{8}$$

$$\frac{1}{\sqrt{2}}(|\Phi^-\rangle|\Psi^-\rangle \pm |\Psi^-\rangle|\Phi^-\rangle), \tag{9}$$

$$\left. \frac{1}{\sqrt{2}}(|\Psi^+\rangle|\Psi^-\rangle \pm |\Psi^-\rangle|\Psi^+\rangle) \right\}, \tag{10}$$

and can be constructed within the four-photon polarization subspace.

For implementing quantum key distribution in such a two-scale collective-dephasing-noise environment, one can begin with the Bell states

$$|0(1)\rangle_L = |\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \tag{11}$$

at the two-qubit scale $n = 0$, and concatenate this logical-qubit code once, resulting in the four-qubit states

$$|0\rangle_{\mathcal{L}} = \frac{1}{\sqrt{2}}(|\Psi^+\rangle|\Psi^-\rangle + |\Psi^-\rangle|\Psi^+\rangle) = \frac{1}{\sqrt{2}}(|0101\rangle - |1010\rangle), \tag{12}$$

$$|1\rangle_{\mathcal{L}} = \frac{1}{\sqrt{2}}(|\Psi^+\rangle|\Psi^-\rangle - |\Psi^-\rangle|\Psi^+\rangle) = \frac{1}{\sqrt{2}}(|1001\rangle - |0110\rangle), \tag{13}$$

at the scale $n = 1$ as the states of the standard computational basis and the states

$$|\nearrow\rangle_{\mathcal{L}} = \frac{1}{\sqrt{2}}(|0\rangle_{\mathcal{L}} + |1\rangle_{\mathcal{L}}) = |\Psi^+\rangle|\Psi^-\rangle, \tag{14}$$

$$|\searrow\rangle_{\mathcal{L}} = \frac{1}{\sqrt{2}}(|0\rangle_{\mathcal{L}} - |1\rangle_{\mathcal{L}}) = |\Psi^-\rangle|\Psi^+\rangle, \tag{15}$$

previously identified as spanning this DFS [10], as the diagonal logical basis, the two clearly being conjugate. Together, these two bases enable the use of the BB84 protocol in this subspace. In the following section, a practical method for producing the states of Eqs. 12–13 is described.

3 Method for Producing Bell Gem States

The production of high-fidelity Bell states by spontaneous parametric down-conversion is now commonplace throughout the world. The production of high-fidelity four-photon product states such as those of Eqs. 14–15 is much less common, although they have been known for some time to enable entanglement "swapping" and quantum state teleportation, the latter providing a quantum-computational primitive. Also related to quantum information processing is a recent scheme for producing a single (entangled) four-photon polarization "cluster state" using the simultaneous production of two Bell states [13]. Here, we describe a procedure for constructing all the four-photon polarization states of the Bell gem $\mathcal{G}_{16}$, which is an *entire* orthonormal basis of *entangled states*, according to the four-tangle measure, using only two simultaneously produced Bell states, quantum state post-selection, and linear optics. We first provide, as an illustration of the method, an explicit calculation showing how the logical-qubit states of Eqs. 12–13 useful for QKD can obtained; a similar procedure is then more briefly described that provides the remaining fifteen (entangled) Bell gem states, some known to be useful for quantum computation, to be constructed.

In the first step toward obtaining the four-qubit state of Eq. 13, two nonlinear crystals are synchronously pumped, each producing one (two polarization qubit) Bell state, resulting in a four-photon state that is a product of the two, namely, the standard four-qubit (logical) basis state of Eq. 15; by a rearrangement of terms in this four-qubit state, this joint state can be rewritten in a convenient form that exhibits correlations that can be exploited in the post-selection step to produce the desired entangled state. If one crystal is arranged to produce the $|\Psi^+\rangle$ polarization Bell state and the other to produce $|\Psi^-\rangle$, the resulting (two e-bit) product state is

$$\begin{aligned}
|\Psi^+\rangle_{12}|\Psi^-\rangle_{34} = \frac{1}{2}(&|\Psi^+\rangle_{13}|\Psi^-\rangle_{24} - |\Psi^-\rangle_{13}|\Psi^+\rangle_{24} \\
&+ |\Phi^+\rangle_{13}|\Phi^-\rangle_{24} - |\Phi^-\rangle_{13}|\Phi^+\rangle_{24}),
\end{aligned} \tag{16}$$

which is the diagonal-basis logical state $|\nearrow\rangle_{\mathcal{L}}$ and which is similar in structure to what one obtains in standard entanglement swapping [1, 8]; the other diagonal-basis logic state, $|\nearrow\rangle_{\mathcal{L}}$, is similarly obtained by interchanging particles pairs 1–2 and 3–4.

With the state of Eq. 16 thus made available directly by spontaneous parametric down-conversion, one can then post-select only the *first two terms* of the right-hand side to obtain the state of Eq. 13, namely,

$$|1\rangle_{\mathcal{L}} = \frac{1}{\sqrt{2}}(|\Psi^+\rangle_{13}|\Psi^-\rangle_{24} - |\Psi^-\rangle_{13}|\Psi^+\rangle_{24}). \quad (17)$$

Linear optics is known to be sufficient for the discrimination of three distinct subsets of Bell states, namely, $\{|\Psi^-\rangle\}$, $\{|\Psi^+\rangle\}$, and $\{|\Phi^+\rangle, |\Phi^-\rangle\}$. Linear optical methods are therefore sufficient in this case for enabling this post-selection: one simply rejects any states of the third of these subsets from the output. In particular, due to the correlation of Bell states exhibited in Eq. 16, it is sufficient to perform this selection process on either one of the two pairs for photons, photons 1 and 3, or photons 2 and 4. This is a standard partial Bell-state discrimination technique that exploits the fact that photons, being bosons, have a symmetric overall quantum state, that is, product of spatial and polarization parts. This discrimination can be done using beamsplitters and polarizers and checking the parity of outputs from them in succession [12]. In order to obtain the remaining four-qubit logical qubit state,

$$|0\rangle_{\mathcal{L}} = \frac{1}{\sqrt{2}}(|\Psi^+\rangle_{13}|\Psi^-\rangle_{24} + |\Psi^-\rangle_{13}|\Psi^+\rangle_{24}), \quad (18)$$

required for BB84-protocol QKD, it then suffices to invert the polarization-states of particles 1 and 3, which induces the required phase sign-change.

The remaining Bell gem states can be similarly produced. To see this conveniently, we label the states of second-order Bell gem $\mathcal{G}_{16}$ by $|e_i\rangle$, with index i corresponding to the order of the states as they appear in Eqs. 3–10 above. For example, as expressed in this e_i notation, we have just shown how to produce the states $|e_8\rangle_{1324}$ and $|e_7\rangle_{1324}$. In the above arrangement, if rather than post-selecting $|e_8\rangle_{1324}$, one post-selects, by the same means, the *second* pair of terms of the right-hand side of Eq. 16 instead of the first pair, one obtains $|e_6\rangle_{1324}$. If one desires to instead have $|e_5\rangle_{1324}$, it can then be obtained from $|e_6\rangle_{1324}$ again by performing polarization-state-flips on both photons 1 and 3.

Similarly, consider two SPDC events as above, but now arranged so as to produce the product state $|\Psi^-\rangle_{12}|\Psi^-\rangle_{34}$, which can be written as $\frac{1}{\sqrt{2}}(|e_2\rangle_{1324} - |e_4\rangle_{1324})$. The Bell gem state $|e_2\rangle_{1324}$ is a linear combination of products of two $|\Phi\rangle$-type states, whereas $|e_4\rangle_{1324}$ is a linear combination of products of two $|\Psi\rangle$-type states. Again, either of these two Bell gem states can be post-selected as desired by partial Bell-state analysis using only linear optics, which is capable of distinguishing these two types of Bell state and therefore the two Bell-gem states as needed. One can then also obtain $|e_3\rangle_{1324}$ from $|e_4\rangle_{1324}$ by performing polarization-flips on photons 1 and 3; one can also obtain $|e_1\rangle_{1324}$ from $|e_2\rangle_{1324}$ by similarly performing polarization-flips on photons 1 and 3.

One can also use SPDC in two nonlinear crystals to produce $|\Psi^-\rangle_{12}|\Phi^-\rangle_{34}$, which can be rewritten as $|e_{16}\rangle_{1324} - |e_{14}\rangle_{1324}$, either of which can the be post-selected for, as above. In the case of these states, however, performing a polarization-flip will not suffice for producing the sign-flip between two Bell-state-product components as above, because both will be of the same "Bell sign," $\pm$. However, again since linear optics suffices to distinguish the $|\Psi\rangle$-type states from the $|\Phi\rangle$-type states, after post-selecting either $|e_{14}\rangle_{1324}$ or $|e_{16}\rangle_{1224}$, one can give a phase-flip to the joint state of photons 1 and 3 *conditional on its being a $|\Psi\rangle$-type state*, providing Bell-gem states $|e_{13}\rangle_{1324}$ or $|e_{15}\rangle_{1324}$, respectively. To obtain the remaining four Bell-gems states, one can use SPDC in two nonlinear crystals to produce $|\Psi^-\rangle_{12}|\Phi^+\rangle_{34}$, which can be rewritten as $|e_{10}\rangle_{1324} + |e_{12}\rangle_{1324}$, either of which can then be post-selected for,

as above. Then, again by performing polarization flips on photons 1 and 3, one can obtain states $|e_9\rangle_{1324}$ or $|e_{11}\rangle_{1324}$, respectively, from $|e_{10}\rangle_{1324}$ or $|e_{12}\rangle_{1324}$.

Thus, two simultaneous spontaneous parametric down-conversion events, followed by appropriate four-photon quantum state post-selection and unconditional polarization flips or linear-optical partial-Bell-state-analysis-based conditional phase-flips on two-photon states using linear optics suffices for the production of the entire set of states of the four-photon entangled polarization-subspace basis $\mathcal{G}_{16}$. This then enables the use of these states in subsequent application to quantum communication or quantum information processing tasks.

4　Conclusion

We have provided a method for constructing four-photon states that are concatenated quantum code states and that span a two-scale dephasing-free subspace that can be used to perform quantum key distribution under the BB84 protocol on logical states composed of four photons. In particular, we showed that spontaneous parametric down-conversion, linear optical quantum state post-selection and two-photon polarization or phase-flips are sufficient for this. Moreover, we showed how to produce all the elements of an orthonormal basis of entangled states for the Hilbert space of four qubits, some of which are known to be useful for quantum information processing.

References

1. Boschi, D., Branca, S., De Martini, F., Hardy, L., Popescu, S.: Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. **80**, 1121 (1998)
2. Jaeger, G.S.: Bell gems: the Bell basis generalized. Phys. Lett. A **329**, 495 (2004)
3. Jaeger, G.S.: Fractal states in quantum information processing. Phys. Lett. A **358**, 373 (2006)
4. Jaeger, G.S.: Fractal states for quantum information processing. In: Foundations of Probability and Physics—4. AIP Conference Proceedings, vol. 889, p. 120 (2007)
5. Jaeger, G.S., Sergienko, A.V.: Symmetry and concatenated code states. In: Donkor, E.J., Piritch, A.R., Brandt, H.E. (eds.) Quantum Information and Computation III. Proceedings of the SPIE, vol. 5815, p. 27. SPIE, Bellingham (2005)
6. Knill, E., Laflamme, R., Zurek, W.H.: Resilient quantum computation. Science **279**, 46 (1998)
7. Kwiat, P.G., Berglund, A.J., Altepeter, J.B., White, A.G.: Experimental verification of decoherence-free subspaces. Science **290**, 498 (2000)
8. Pan, J.W., Bouwmeester, D., Weinfurter, H., Zeilinger, A.: Experimental entanglement swapping: entangling photons that never interacted. Phys. Rev. Lett. **80**, 3891 (1998)
9. Preskill, J.: In: Lo, H.K., Popescu, S., Spiller, J. (eds.) Quantum Communication and Quantum Computing. World Scientific, Hong Kong (1998)
10. Vaidman, L., Goldenberg, L., Wiesner, S.: Error prevention scheme with four particles. Phys. Rev. A **54**, R1745 (1996)
11. Walton, Z., Abouraddy, A.F., Sergienko, A.V., Saleh, B.E.A., Teich, M.C.: Decoherence-free subspaces in quantum key distribution. Phys. Rev. Lett. **91**, 087901 (2003)
12. Zeilinger, A.: Quantum entanglement: a fundamental concept finding its applications. Phys. Scr. **T-76**, 203 (1998)
13. Zou, X.-B., Mathis, W.: Generating a four-photon polarization-entangled state. Phys. Rev. A **71**, 032308 (2005)