Number-theoretic nature of communication in quantum spin systems

Chris Godsil,[1] Stephen Kirkland,[2] Simone Severini,[3] and Jamie Smith[4]

[1]*Combinatorics & Optimization, University of Waterloo, N2L 3G1 Waterloo, Canada*
[2]*Hamilton Institute, National University of Ireland, Maynooth, Co. Kildare, Ireland*
[3]*Department of Computer Science, and Department of Physics & Astronomy,*
University College London, WC1E 6BT London, United Kingdom
[4]*Institute for Quantum Computing, and Combinatorics & Optimization,*
University of Waterloo, N2L 3G1 Waterloo, Canada

(Dated: 24 June 2012)

Abstract

The last decade has witnessed a substantial interest in protocols for transferring information on networks of quantum mechanical objects. A variety of control methods and network topologies have been proposed, on the basis that transfer with perfect fidelity – *i.e.*, deterministic and without information loss – is impossible through unmodulated spin chains with more than a few particles. Solving the original problem formulated by Bose [*Phys. Rev. Lett.* **91**, 207901 (2003)], we determine the exact number of qubits in unmodulated chains (with XY Hamiltonian) that permit the transfer with fidelity arbitrarily close to 1, a phenomenon called *pretty good state transfer*. We prove that this happens if and only if the number of nodes is $n = p - 1$, $2p - 1$, where p is a prime, or $n = 2^m - 1$. The result highlights the potential of quantum spin systems dynamics for reinterpreting questions about the arithmetic structure of integers, and in this case, primality.

Introduction – Since the pioneering work by Bose [3], quantum channels implemented by spin systems have been interpreted as wires for the transmission of possibly unknown qubit states. Motivated by the perspective of designing quantum buses and nanodevices, a vigorous effort has delineated the field of quantum spin systems engineering [4]. In this context, one of the desirable tasks is to transfer the state of a particle into another one with maximum fidelity; when the fidelity is 1, we have *perfect state transfer* (for short, *PST*), a notion originally introduced in [7]. Given an inherent difficulty in the manipulation of coherent quantum mechanical objects, the most appealing set up for state transfer employs a time-independent Hamiltonian and no interaction with the system except at initialisation and read-out. If we do not use *ad hoc* coupling schemes and control protocols (see [14]; also the recent [23] and the references therein), a spin chain (1D magnet), with Heisenberg XY Hamiltonian, exhibits PST only between two and three qubits [7]. This is a negative result, because such a chain is arguably the quantum wire obtainable with the smallest amount of physical and technological resources.

On the basis of sufficient conditions for PST, this fact fueled a mathematically challenging classification programme aimed to identify PST in general network topologies [11]. The k-dimensional hypercube (with $n = 2^k$ qubits) has the best known performance in terms of the distance travelled by a single excitation: PST occurs between antipodal nodes at (network) distance k. However, for practical purposes, it is natural to study whether a minimalist structure like the chain (with n qubits) can still be usefully employed. In particular, even if we already know that there is no PST for $n \geq 4$, we may still ask the following question: given n and an $\varepsilon > 0$, does there exist t such that the fidelity at time t between qubits 1 and n is larger than $1 - \varepsilon$? When the answer is

"yes", we say that there is *pretty good state transfer* (for short, *PGST*). While Bose [3] verified that the fidelity could be remarkably high even for rather long chains, the notion of PGST was formally isolated in [10] as a relaxation of PST. We give in the present work a complete characterization of the parameters for which there is PGST. Our findings can be combined into the following simple-sounding statement:

Theorem. A uniformly coupled chain of n particles with *XY* Hamiltonian has PGST if and only if $n = p - 1$ or $2p - 1$, where p is a prime, or if $n = 2^m - 1$.

The significance of the result is twofold. From the physical point of view, it is valuable that we rigorously describe a phenomenon with applications to the study of quantum nanodevices [9]. In fact, the related observations obtained up to now are either numerical or fragmented. The message conveyed by the notion of PGST is that an unknown qubit state can be transferred with arbitrarily large fidelity between the end nodes of "long" chains, whenever the waiting time is not an issue. From the mathematical point of view, we highlight properties of quantum interference as a consequence of number-theoretic constraints. The appearance of prime numbers in the theorem indicates a connection between the occurrence of PGST in chains of a given length and primality testing. This suggests a potential application of quantum dynamics on graphs for reinterpreting number-theoretic problems, when the problem description is encoded in the parameters of the system.

It is well established that the dynamics of a single excitation in networks of spins with unmodulated couplings is a continuous-time quantum walk on the unweighted graph modeling the network. Hence, our result can also be reinterpreted in the language of continuous-time quantum walks: it describes the maximum hitting probability between antipodal vertices induced by a one-

dimensional quantum walk. Walks of this type have been studied in great detail [16]. This analogy prompts to disregard the original spin system set-up and to work with a single n-level system. The realisation and simulation of this quantum device is the centre of several discussions [21]. It is remarkable that at a wider level, state transfer can be seen as the simplest model in a family of processes for quantum transport: for example, the population transfer of n-level systems [22]; after including the role of the environment, the transport of energy in organic molecules [20]; a closely related mathematical setting describes state transfer in chains of harmonic oscillators coupled with beam-splitter interactions [19]. Finally, the experimental implementation of the Heisenberg XY chain has been proposed in schemes including cold-atom optical lattices and superconducting circuits [2].

PGST – The Hamiltonian governing the evolution of the system acts on the Hilbert space $\mathcal{H} \cong \mathbb{C}_1^2 \otimes \cdots \otimes \mathbb{C}_n^2$. If we do not include external static potentials, the Hamiltonian is

$$\widehat{H} = \frac{1}{2} \sum_{u=1}^{n-1} J_u \left(\sigma_u^x \sigma_{u+1}^x + \sigma_u^y \sigma_{u+1}^y \right),$$

where σ_u^w ($w \in \{x, y, z\}$) is a Pauli matrix on $\mathbb{C}_u^2$ and J_u is the coupling strength between the particles u and $u+1$. By virtue of the Jordan-Wigner transform [17], the free evolution for a time t of a single excitation originally located at site $|u\rangle \in \{|1\rangle, ..., |n\rangle\}$ is given by $e^{iHt}|u\rangle = U(t)|u\rangle$, where $H_{u,v} = J_u$ if $v = u+1$ or $u = v+1$, and $H_{u,v} = 0$, otherwise. The $n \times n$ real symmetric matrix H is the Hamiltonian restricted to the single excitation sector. PST occurs between 1 and n if there is a $t \in \mathbb{R}^+$ such that $|\langle n|U(t)|1\rangle| = 1$, *i.e.*, the channel has maximum fidelity; PGST occurs between 1 and n if for every $\epsilon > 0$ there is $t \in \mathbb{R}^+$ such that $|\langle n|U(t)|1\rangle| > 1 - \epsilon$. Analytical solutions for coupling design able to achieve PST for any n have been presented in previous works (see [23]). Abstractly, a chain of length n is modeled by a network called an *n-path* and denoted by P_n. The links representing the particle-particle interactions are $\{1, 2\}, \{2, 3\}, ..., \{n-1, n\}$. When the chosen couplings are uniform (*w.l.o.g.*, $J_u = 1$), the Hamiltonian H is the adjacency matrix of the n-path. (Recall that the adjacency matrix of a graph has ij-th entry 1 if there is a link between the nodes i and j; 0, otherwise.) We know from [10] that there is PGST in P_4 and P_5.

We shall first prove the theorem. Next, we present some details about the cases when there is no PGST. In particular, we will give an explicit upper bound on the fidelity in a special case. We then propose a discussion concerning the links between state transfer and control theory, when we consider PGST between internal nodes.

Proof of the theorem – The proof of the theorem is based on a direct linear-algebraic analysis of the eigensystem of $U(t)$ and on the application of standard number-

theoretic tools, especially Kronecker's Theorem on Diophantine approximation. We begin by considering a general property of PGST and basic facts about bipartite graphs. We then use relations on the eigenvalues with a detailed case-by-case treatment.

For any two vertices u and v of a graph,

$$U(t)|u\rangle - \gamma|v\rangle = \gamma U(t)(\gamma^{-1}|u\rangle - U(-t)|v\rangle);$$

here $\gamma^{-1}I - U(-t)$ is the Hermitian adjoint of $\gamma^{-1}I - U(t)$. Since $U(t)$ is unitary and $\|\gamma\| = 1$, we see that

$$\|U(t)|u\rangle - \gamma|v\rangle\| = \|U(t)|v\rangle - \gamma|u\rangle\|.$$

So, if we have PGST from u to v, we also have it from v to u.

A graph X is *bipartite* if there is a bipartition of the set of nodes such that the links connect only nodes in different parts. Suppose X is bipartite and let D be a diagonal matrix such that $D_{u,u}$ is 1 or -1 according as u is in one of the other part of the bipartition. Then $DAD = -A$ and if $U(t)|u\rangle \approx \gamma|v\rangle$,

$$\gamma D|v\rangle \approx DU(t)D\,D|u\rangle = U(-t)D|u\rangle.$$

But $|u\rangle$ and $|v\rangle$ are eigenvectors for D with eigenvalues 1 or -1; the eigenvalues are equal if and only if u and v are in the same part. So there is a sign factor $\sigma_{u,v}$ and $\gamma|v\rangle \approx \sigma_{u,v}U(-t)|u\rangle$. Accordingly, $U(t)|v\rangle \approx \gamma^{-1}\sigma_{u,v}|u\rangle$.

By the above, $U(t)|v\rangle \approx \gamma|v\rangle$, and we conclude that $\gamma \approx \gamma^{-1}\sigma_{u,v}$. Hence $\gamma \approx \pm 1$ if u and v are in the same part, and $\gamma \approx \pm i$ if they are not. (For PST this observation is due to Kay [4].) Let F denote the permutation matrix of order $n \times n$ such that $F|r\rangle = |n+1-r\rangle$ for all r. Let $E_1, \ldots, E_n$ be the idempotents in the spectral decomposition of the path P_n (*i.e.* of its adjacency matrix). We can then write $F = \sum_{r=1}^{n} (-1)^{r-1} E_r$. If we have PGST at time t then $U(t) \approx \gamma F$ and therefore

$$1 = \det U(t) \approx \gamma^n \det(F) = \gamma^n (-1)^{\lfloor n/2 \rfloor}.$$

This yields three cases: *(1)* if $n \equiv 1 \mod 4$ then $(-1)^{\lfloor n/2 \rfloor} = 1$ and $\gamma \approx 1$; *(2)* if $n \equiv 3 \mod 4$ then $(-1)^{\lfloor n/2 \rfloor} = -1$ and $\gamma \approx -1$; *(3)* if n is even then $i^n = (-1)^{n/2}$ and $\gamma \approx \pm i$. It is well known that the eigenvalues θ_r of P_n are given by $\theta_r = 2\cos(\pi r/(n+1))$.

We start with the positive results. If PGST occurs then $U(t)$ gets arbitrarily close to γF. This means that $e^{i\theta_r t} \approx (-1)^{r-1}\gamma$ for $r = 1, \ldots, n$. Set $m = \lfloor n/2 \rfloor$. Assume $\gamma = \pm 1$ if n is odd and $\pm i$ if n is even.

First, we prove that for the path P_n, if $e^{i\theta_r t} \approx (-1)^{r-1}\gamma$, for $r = 1, \ldots, m$, then $e^{i\theta_r t} \approx (-1)^{r-1}\gamma$, for all $r = 1, ..., n$, and hence $U(t) \approx \gamma F$. To see this, assume $e^{i\theta_r t} \approx (-1)^{r-1}\gamma$. Since n-paths are bipartite, $\theta_{n+1-r} = \theta_r$, and therefore $e^{i\theta_{n+1-r}t} = e^{-i\theta_r t} \approx (-1)^{r-1}\gamma^{-1}$. For PGST, we need $(-1)^{n-r}\gamma = (-1)^{r-1}\gamma^{-1}$, or equivalently $\gamma^2 = (-1)^{n-1}$. As this holds for our choice of γ, we are done. Since $\theta_r = 2\cos(\pi r/(n+1))$ we have that θ_r is

a polynomial with rational coefficients of degree r in θ_1. We also set $\theta_0 = 2$. It follows that the numbers $\theta_0, \ldots, \theta_d$ are linearly independent over $\mathbb{Q}$ if and only if the degree of the algebraic integer θ_1 is greater than d.

This provides us with the necessary tools to prove the first part of the theorem: if $n = p - 1$ or $2p - 1$, where p is prime, or if $n = 2^m - 1$ then we have PGST on P_n. If $\alpha \in \mathbb{C}$ we use use $\mathbb{Q}(\alpha)$ to denote the field obtained by adjoining α to $\mathbb{Q}$. If $\mathbb{F}$ is a subfield of $\mathbb{Q}(\alpha)$, then $\mathbb{Q}(\alpha)$ is a vector space over $\mathbb{F}$; its dimension is the index of $\mathbb{F}$ in $\mathbb{Q}(\alpha)$. (For details see, $e.g.$, [13], Ch. 5.) Let $\theta = 2\cos(\pi/(n+1))$ and set $\zeta = e^{\pi/(n+1)}$. Then $\theta \in \mathbb{Q}(\zeta)$ and ζ is a root of the quadratic $x^2 - x\cos(\theta) + 1$. So the index of $\mathbb{Q}(\theta)$ in $\mathbb{Q}(\zeta)$ is at most two. If $n \geq 3$ though, θ is real and ζ is not. Thus, the index is exactly two. The degree of ζ is $\phi(2n+2)$, where ϕ is Euler's function, and therefore the degree of θ is $\phi(2n+2)/2$. If $n = p - 1$, $2p-1$, or $2^m - 1$, where p is a prime, we have respectively

$$\phi(2n+2) = \phi(2p) = \phi(p) = p - 1,$$
$$\phi(2n+2)/2 = \phi(4p)/2 = \phi(p) = p - 1,$$
$$\phi(2(n+1))/2 = 2^{m-1}.$$

Finally, in each of these three cases the positive eigenvalues of P_n are linearly independent over $\mathbb{Q}$. Next, let δ equal $0, \frac{1}{2}, \frac{1}{4}$ or $\frac{3}{4}$ according as γ equals $1, -1, i, -i$, respectively. For each $r = 1, \ldots, m$, let $\alpha_r = \frac{1}{2}$ if r is even and $\alpha_r = 0$ if r is odd. By Kronecker's Theorem (see [12]), for any $\epsilon, T > 0$ there is a $t_\epsilon > T$, and integers $p_r, r = 1, \ldots, m$, such that $\left| t_\epsilon \frac{\theta_r}{2} - p_r - \alpha_r - \delta \right| < \epsilon$. It follows that as $\epsilon \to 0$, $e^{i\pi t_\epsilon \theta_r} \to (-1)^{r-1}\gamma$, with $r = 1, \ldots, n$, so that we have PGST. Let us now focus on the negative cases: if $n = mp - 1$, where p is odd and $m \geq 3$, then PGST does not occur on P_n. Suppose $n + 1 = mp$, where p is odd. Then

$$1 + 2 \sum_{r=1}^{(p-1)/2} (-1)^r \cos(\pi r/p) = 0.$$

If we multiply this by $\cos(\pi/(n+1))$, we get

$$\cos\left(\frac{\pi}{n+1}\right) + \sum_{r=1}^{\frac{p-1}{2}} (-1)^r$$
$$\left[\cos\left(\frac{\pi(mr+1)}{n+1}\right) + \cos\left(\frac{\pi(mr-1)}{n+1}\right) \right] = 0,$$

which yields the following relations on eigenvalues:

$$\theta_x + \sum_{r=1}^{\frac{p-1}{2}} (-1)^r \theta_{mr+x} + \sum_{r=1}^{\frac{p-1}{2}} (-1)^r \theta_{mr-x} = 0,$$

with $x = 1, 2$. The equation with $x = 2$ is obtained if we multiply by $\cos(2\pi/(n+1))$ the equation with $x = 1$. If

we subtract these equations, we find that

$$(\theta_1 - \theta_2) + \sum_{r=1}^{\frac{p-1}{2}} (-1)^r (\theta_{mr+1} - \theta_{mr+2})$$
$$+ \sum_{r=1}^{\frac{p-1}{2}} (-1)^r (\theta_{mr-1} - \theta_{mr-2}) = 0.$$

Denote the three terms on the left by D, E and F respectively. If we have PGST then there is a sequence of times $(t_k)_{k\geq 0}$ such that $e^{i\theta_r t_k} \to (-1)^{r-1}\gamma$, and so $e^{i(\theta_s - \theta_{s+1})t_k} \to -1$. Therefore $e^{iDt_k} \to -1$, while e^{iEt_k} and e^{iEt_k} both tend to 1 or to -1. Thus, $e^{i(D+E+F)t_k} \to -1$, which is impossible, since $D + E + F = 0$. It is not difficult to verify that the cases considered above include all integers. This ends the proof of the theorem. A corollary is that if $2 \leq n \leq 10$, we have always PGST, except in the case $n = 8$.
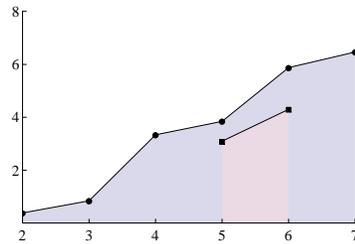
FIG. 1: Logarithm of the earliest points in which the fidelity is strictly greater than 0.99 for $2 \leq n \leq 7$. The numbers have been obtained by plotting $|U(t)_{1,n}|$ ($n = 2, ..., 7$) and then by analysing sections of the curves. Clearly 0.99 is an arbitrary choice. Notice the jumps between the pairs $(2, 3), (4, 5), (6, 7)$. Because PGST depends on the positive eigenvalues of P_n, this phenomenon may be explained by the fact that $\lfloor n/2 \rfloor = \lfloor (n + 1)/2 \rfloor$, for n even.

Fig. 1 gives the smallest times needed to achieve a relatively large fidelity (> 0.99 and thus $\epsilon = 0.01$) for chains of length $2 \leq n \leq 7$. The parameters to be considered for numerics are n and ϵ. Indeed, the waiting time depends also on the tolerance ε for being close to one. The log plot suggests that for a fixed ε there is a behaviour that is linear in n.

It is a corollary of the theorem that there is PGST on P_n if and only if its positive eigenvalues are linearly independent over the rationals. A proof of some cases when there is PGST can be constructed with the use of facts about linear independence of roots of unity discussed by Conway and Jones (in particular Theorems 1 and 7) and by Watkins and Zeitlin [8]. The crucial observation for PGST is indeed the linear independence (over the rationals) of the numbers $\cos(\pi j/(n+1))$ for certain choices of j.

Bounding fidelity – We have seen that there are many cases in which there is no PGST for P_n. We outline now a general technique for proving upper bounds on the

3

fidelity whenever this happens. Algebraic graph theory is again the natural toolbox to employ. The spectral decomposition of the adjacency matrix of a graph X is $A = \sum_r \theta_r E_r$. Two vertices u and v of X are *cospectral* if, for each r, the projections $E_r|u\rangle$ and $E_r|v\rangle$ have the same length. We say they are *strongly cospectral* if, for each r, we have $E_r|u\rangle = \pm E_r|v\rangle$. In [10], it is shown that if we have PGST (or PST) from u to v then u and v are strongly cospectral. If the eigenvalues of A are simple, two vertices are strongly cospectral if and only if they are cospectral. Assume $U(t)_{u,v} = \sum_r (E_r)_{u,v} e^{i\theta_r t}$. Define ϵ_r by the requirement that $(E_r)_{u,v} = \epsilon_r (E_r)_{u,u}$. (For paths, $\epsilon_r = (-1)^{r-1}$.) Then $U(t)_{u,v}$ is a convex combination of the norm one complex numbers $\epsilon_r e^{it\theta_r}$. For PGST to occur, these numbers must all be approximately equal. We can see this by applying the triangle inequality:

$$|U(t)_{u,v}| \leq \sum_r |(E_r)_{u,v}| = \sum_r |(E_r)_{u,u}| = 1.$$

In particular, PGST cannot happen if there is some set S of eigenvalue indices such that

$$\sum_{r \in S} (E_r)_{u,u} - \left| \sum_{r \in S} (E_r)_{u,v} e^{i\theta_r t} \right| \qquad (1)$$

is bounded away from zero (for all t). With a direct analysis of this expression, we can rule out PGST explicitly when $n = 3k + 2$ and k is even. (The details are in Appendix.) We leave open the challenge of finding explicit bounds on the fidelity in the remaining cases. The proof technique outlined here can be potentially extended to other network topologies.

Internal nodes – Through this work we have studied PGST between the extremities of a chain. For practical purposes it may be useful to have PGST between particles corresponding to internal nodes. We discuss an argument for showing that if there is PGST between internal nodes then there is PGST between the extremities. In doing so, we appeal to algebraic techniques from quantum control theory of spin systems [6]. Given a graph X with set of vertices V and adjacency matrix A, let z be the characteristic vector of some set $S \subseteq V$. We define and denote by $W_z = [z|Az|...|A^{n-1}z]$ an $n \times n$ matrix with entries in $\mathbb{Z}^{\geq 0}$. The matrix W_z is called the *walk matrix* of X with respect to S. The pair (X, z) is said to be *controllable* if the matrix W_z is invertible (*i.e.*, $\det(W_z) \neq 0$). The set-up is a graph-theoretic analogue of the famous Kalman rank condition in control theory: the matrices e^{iAs} and $e^{izz^T t}$ ($s, t \in \mathbb{R}^+$) from a controllable pair generate a dense subgroup of the unitary group $U(n)$ ($n \geq 2$).

A *closed walk* is a sequence of vertices, with consecutive vertices adjacent, that starts and ends at the same vertex. If we have PGST on P_n from k to ℓ then the vertices k and ℓ are cospectral, so then $k + \ell = n + 1$ and the generating functions for closed walks at k and

at ℓ are equal. Consequently, the distance from k to an end vertex equals the distance from ℓ to the antipodal end vertex. By the *A-module* generated by a vector, we mean the smallest A-invariant subspace that contains the vector. If $|\ell\rangle$ lies in the A-module generated by $|k\rangle$ and we have PGST from k to $n + 1 - k$, then we have PGST from ℓ to $n + 1 - \ell$. Suppose $U(t)|k\rangle \approx \gamma|n + 1 - k\rangle$. Because $|\ell\rangle$ lies in the A-module generated by $|k\rangle$, there is a polynomial f such that $|\ell\rangle = f(A)|k\rangle$. Then

$$U(t)|\ell\rangle = U(t)f(A)|k\rangle = f(A)U(t)|k\rangle \approx \gamma f(A)e_{n+1-k}.$$

If Φ is the 'flip' automorphism on the path, then Φ commutes with A and so

$$f(A)|n + 1 - k\rangle = f(A)\Phi|k\rangle =$$
$$\Phi f(A)|k\rangle = \Phi|\ell\rangle = |n + 1 - \ell\rangle.$$

If $n + 1$ is a prime, then all vertices i give a controllable pair (P_n, i), and so PGST between any pair of vertices implies PGST between end vertices. If $n + 1 = 2p$ where p is prime and $k \neq 2, p$, then PGST from k to $n + 1 - k$ implies PGST between the end vertices. If $k = p$ then k is the central vertex and PGST cannot occur at k. We leave open the case $n = 2^m + 1$.

Conclusions – By solving an open problem about quantum transport [3], we have highlighted number-theoretic properties of quantum communication in spin chains. We have studied general properties of PGST. We have given necessary and sufficient mathematical conditions for PGST to occur on XY spin chains with uniform couplings.

The physical intuition paralleling the mathematical result suggests that the *spin wave* can reach the end of the chain with an arbitrary high peak only when the number of particles does not permit significant constructive interference. In this case, the trajectory of the amplitude (in a fixed time interval) suggests an intriguing analogy with chaotic dynamics that remains to be explored. Deciding whether there is PGST is computationally equivalent to primality testing, a task that is performed efficiently with the AKS test [1]. Experimental detection of PGST would correspond to a *natural algorithm* for primality. Its complexity would be determined via bounds on the time required by physical evolution (or its simulation) and on resources for tomography and sequential measurements.

We have outlined a technique for quantifying maximum fidelity when there is no PGST. Some cases remain with no complete answer. We have shown how notions of network control theory can be applied to study communication in spin systems. Exploring PGST in general networks beyond the n-path requires similar methods, but it is a challenging task. It is valuable to observe that we have considered a system without spatial disorder; its behaviour does not exhibit effects due to Anderson localization. Numerics in [5] indicated that the fidelity of this system tends to be robust when a relatively small amount

of disorder is introduced in the couplings. On the other side, it was shown in [15] that the speed of propagation of coherent walks is suppressed exponentially in the amount of imperfection.

We have left open the development of a comprehensive theory of PGST. Such a theory is important to obtain a fuller understanding of transport in networks of quantum mechanical particles, either engineered or found in nature. Experimental tests based on photonic waveguides are currently investigated. (See [18] for background on such schemes.)

———————

[1] M. Agrawal, N. Kayal, and N. Saxena, *Ann. of Math.* (2) **160** (2004), no. 2, 781-793.
[2] I. Bloch, *Nature* **453**, 1016 (2008); J. Majer, *et al.*, *Nature* **449**, 443 (2007).
[3] S. Bose, *Phys. Rev. Lett.* **91**, 207901 (2003).
[4] S. Bose, *Contemp. Phys.*, **Vol. 48** (1), pp. 13–30, 2007; A. Kay, *Phys. Rev. A* **84**, 022337 (2011); V. M. Kendon and C. Tamon, *J. Comput. Theor. Nanosci.*, **8**(3):422-433, 2011.
[5] D. Burgarth, S. Bose, *New J. Phys.* **7** 135 (2005).
[6] D. Burgarth, D. D'Alessandro, L. Hogben, S. Severini, and M. Young, arXiv:1111.1475v1 [quant-ph]; C. Godsil and S. Severini, *Phys. Rev. A* **81**, 052316 (2010).
[7] M. Christandl, *et al.*, *Phys. Rev. Lett.* **92**, 187902 (2004).
[8] J. H. Conway and A. J. Jones, *Acta Arith.* **30** (1976), 229-240; W. Watkins and J. Zeitlin, *Amer. Math. Monthly*, **100**(5):471–474, May 1993.
[9] D. DiVincenzo, *et al.*, *Nature* **408**, 339 (2000).
[10] C. Godsil, *Discrete Math.* **312**(1): 129-147 (2012).
[11] C. Godsil, arXiv:1011.0231v2 [math.CO]; N. Saxena, S. Severini, and I. Shparlinski, *Int. J. Quantum Inf.* **5**, 417 (2007).
[12] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Oxford University Press, Oxford, 2008), 6th ed.
[13] I. N. Herstein, *Topics in Algebra*, Wiley (New York), 1975.
[14] A. Kay, *Int. J. Quantum Inf.* **8**, 641 (2010).
[15] J. P. Keating, *et al.*, *Phys. Rev. A* **76**, 012315 (2007).
[16] N. Konno, *Phys. Rev. E*, **72**, 026113 (2005); P. L. Knight, E. Roldán, and J. E. Sipe, *Phys. Rev. A* **68**, 020301(R) (2003).
[17] E. Lieb, F. Wu, *Phys. Rev. Lett.* **20** (1968), 1445-1448.
[18] H. B. Perets, *et al.*, *Phys. Rev. Lett.* **100**, 170506 (2008).
[19] M. B. Plenio, J. Hartley, and J. Eisert, *New J. Phys.* 6, **36** (2004).
[20] P. Rebentrost, *et al.*, *New J. Phys.* **11**, 033003 (2009).
[21] H. Schmitz, *et al.*, *Phys. Rev. Lett.* **103**, 090504 (2009).
[22] B. Shore, *Acta Phys. Slovaca* **58**, 243 (2008).
[23] Y. Wang, F. Shuang, and H. Rabitz, *Phys. Rev. A* **84**, 012307 (2011).

Appendix – We have outlined a general technique for bounding fidelity. We know that there is no PGST when $n = 3k + 2$ and k is even. This is the case considered here. There is no PGST if there exists some set S of eigenvalue indices such that the expression in Eq. (1) is bounded away from zero (for all t). In this case,

$$\theta_1 = \theta_k + \theta_{k+2}.$$

Define

$$h(t) = \sum_r (E_r)_{1,n} e^{i\theta_r t}.$$

Here,

$$(E_r)_{1,n} = (-1)^{r-1}(E_r)_{1,1},$$

where $(E_r)_{1,1} \geq 0$ and $\sum_r (E_r)_{1,1} = 1$. So, we can rewrite $h(t)$ in the form

$$h(t) = \sum_r a_r (-1)^{r-1} e^{i\theta_r t}.$$

Since $\sum_r a_r = 1$, if $|h(t)| \approx 1$ then the summands in this expression must be approximately equal. Consider the sum

$$a_1 e^{i\theta_1 t} + (-1)^{k-1} a_k e^{i\theta_k t}$$
$$+ (-1)^{k+1} a_{k+2} e^{i\theta_{k+2} t} + (-1)^n a_n e^{i\theta_n t}.$$

For PGST to occur, its absolute value must be close to $a_1 + a_k + a_{k+2} + a_n$. We can simplify a little by working with

$$a_1 + (-1)^{k-1} a_k e^{i(\theta_k - \theta_1)t}$$
$$+ (-1)^{k+1} a_{k+2} e^{i(\theta_{k+2} - \theta_1)t} + (-1)^n a_n e^{i(\theta_n - \theta_1)t};$$

which has the same absolute value. We aim to show that the real part of this sum is bounded away from $a_1 + a_k + a_{k+2} + a_n$. We note that $\theta_n = -\theta_1$, $a_n = a_1$, and each of a_1, a_k, a_{k+2}, a_n is positive.

When k is even, we can write the real part of this sum as

$$a_1 - a_k \cos((\theta_k - \theta_1)t)$$
$$- a_{k+2} \cos((\theta_{k+2} - \theta_1)t) - a_1 \cos(2\theta_1 t).$$

Since $\theta_1 = \theta_k + \theta_{k+2}$, this is equal to

$$a_1 - a_k \cos(\theta_{k+2} t)$$
$$- a_{k+2} \cos(\theta_k t) - a_1 \cos(2(\theta_k + \theta_{k+2})t).$$

When $\cos(\theta_{k+2} t), \cos(\theta_k t) \leq -\sqrt{3}/2$, we have $-1/2 \leq \sin(\theta_{k+2} t), \sin(\theta_k t) \leq 1/2$. Whence

$$\cos((\theta_k + \theta_{k+2})t) \geq (3/4 - 1/4) = 1/2$$

and so $\cos(2(\theta_k + \theta_{k+2})t) \geq -1/2$. Consequently,

$$a_1 - a_k \cos(\theta_{k+2}t) - a_{k+2}\cos(\theta_k t)$$
$$- a_1 \cos(2(\theta_k + \theta_{k+2})t)$$
$$\leq 3a_1/2 + (a_k + a_{k+2})\sqrt{3}/2$$
$$= 2a_1 + a_k + a_{k+2} - (a_1 + (2 - \sqrt{3})a_k$$
$$+ (2 - \sqrt{3})a_{k+2})/2.$$

On the other hand, if $\cos(\theta_{k+2}t) \geq \sqrt{3}/2$ then

$$a_1 - a_k \cos(\theta_{k+2}t) - a_{k+2}\cos(\theta_k t)$$
$$- a_1 \cos(2(\theta_k + \theta_{k+2})t)$$
$$\leq 2a_1 + \sqrt{3}a_k/2 + a_{k+2} + a_1$$
$$= 2a_1 + a_k + a_{k+2}$$
$$- (2 - \sqrt{3})a_k/2.$$

It follows that if $\cos(\theta_k t) \geq \sqrt{3}/2$ then we have an explicit upper bound: $2a_1 + a_k + a_{k+2} - (2 - \sqrt{3})a_{k+2}/2$. This rules out PGST when $n = 3k + 2$ and k is even.

6