Aberystwyth University

Subspace controllability of spin-½ chains with symmetries
Wang, Xiaoting; Burgarth, Daniel; Schirmer, S.

Subspace controllability of spin-$\frac{1}{2}$ chains with symmetries

Xiaoting Wang,[1] Daniel Burgarth,[2,*] and S. Schirmer[3,†]

[1]*Department of Physics and Astronomy, Hearne Institute for Theoretical Physics, Louisiana State University, Baton Rouge, Louisiana 70803, USA*

[2]*Institute of Mathematics, Physics and Computer Science, Aberystwyth University, Aberystwyth SY23 3BZ, United Kingdom*

[3]*Department of Physics, College of Science, Swansea University, Swansea SA2 8PP, United Kingdom*

We develop a technique to prove simultaneous subspace controllability on multiple invariant subspaces, which specifically enables us study the controllability properties of spin systems that are not amenable to standard controllability arguments based on energy level connectivity graphs or simple induction arguments on the length of the chain. The technique is applied to establish simultaneous subspace controllability for Heisenberg spin chains subject to limited local controls. This model is theoretically important and the controllability result shows that a single control can be sufficient for complete controllability of an exponentially large subspace and universal quantum computation in the exponentially large subspace. The controllability results are extended to prove subspace controllability in the presence of control field leakage and discuss minimal control resources required to achieve controllability over the entire spin chain space.

I. INTRODUCTION

Quantum spin models, that is, quantum systems composed of a collection of interacting spin-$\frac{1}{2}$ particles, are of considerable interest and importance in many areas of science with applications ranging from the study the quantum phase transitions [1] and the formation of quantum spin liquids [2] and spin glasses [3] in condensed matter physics to the huge and popular field of quantum information processing (QIP) [4], where spin-$\frac{1}{2}$ particles are proxies for qubits and spin networks effective models for finite-dimensional QIP devices. Considering the importance of quantum phenomena in physics, finding ways to control them has naturally been a long-standing dream of physicists and chemists. Progress was made with radio-frequency control of large spin ensembles in nuclear magnetic resonance decades ago, paving the way for many applications from spectroscopy to magnetic resonance imaging. Control of individual quantum systems such as single spins, atoms, or ions, however, was practically impossible until quite recently. While it still remains challenging, tremendous experimental progress has been made, making it possible, for instance, to simulate the spin-spin interaction using ions and ultracold atoms with superior control and the ability to tune parameters, as recently demonstrated in [5], for example.

Improving control of quantum systems in general, and spin systems in particular, and understanding fundamental issues that affect and limit control of these systems is of paramount importance from a theoretical point of view, as well as for the development of new applications such as QIP or quantum metrology devices. Not every controlled spin system is fully controllable. Controllability depends on the Hamiltonian of the physical system and the available control resources. Physical and technological limitations impose constraints on the system and control Hamiltonians that can be realized. k-body interactions for $k \geqslant 3$, for example, are difficult to generate

and much weaker than single and two-body interactions. Therefore, the system Hamiltonians for spin systems are usually restricted to two-body interactions, and as even those are not easily controllable, control is often limited to local control of individual spins. Furthermore, designs that require many independent controls acting on individual spins are generally far more difficult to realize than designs that require fewer controls. For example, while controlling individual ions in ion traps is possible today, it requires multiple lasers or precise dynamic positioning of a single laser to enable individual addressing of all the ions. For many other systems such dynamic individual addressing remains impossible. If we can control the system with a small number of simple actuators acting on fixed spins, the complexity of the system design can be considerably reduced. This prompts the question of minimal resources for controllability of spin systems, such as the minimum number of local controls required to control a certain spin network or, alternatively, what is the most we can achieve with fixed control resources for a given system.

The minimal requirements for different spin systems depend on the type and configuration of the interactions between spins, e.g., whether it is a one-dimensional (1D) spin chain, a spin ring, or a 2D or 3D arrangement. The simplest case is 1D spin chains, but even in this case the required control resources depend on the type of interaction and type and position of the actuator. As will be explained in detail in the following, a (closed) quantum spin system $\mathcal{S}$ with a system Hamiltonian H_0 subject to a set of control Hamiltonians $\{H_k\}$, $k = 1, \ldots, m$, is controllable if the controls can generate arbitrary unitary evolutions. In the language of QIP, complete controllability is equivalent to the concept of universal quantum computation (UQC) [4]. An important necessary and sufficient condition for complete controllability is that the dynamical Lie algebra (DLA) generated by $\{-i H_k\}$ is u(N) or su(N), the Lie algebra of Hermitian or trace-zero Hermitian matrices [6]. Using this condition, it has been shown that for chains with Ising coupling, local controls on every spin are required for controllability, while chains with Heisenberg coupling are known to be controllable given at least two noncommuting

controls acting on the first or last spin in the chain [7]. The DLA has also been calculated for different couplings with two and three local controls [8] and it is known that a Heisenberg chain with a single local control is not controllable as the Hilbert space can be decomposed into multiple subspaces that are invariant under the dynamics and the DLA is thus reducible [9]. However, the system is controllable on the smallest of the invariant subspaces, the single excitation subspace [10], and results based on numerical calculations in [11] further suggest that the system is indeed controllable on all invariant subspaces, including the largest one. Our first aim is to prove this conjecture, showing that a Heisenberg chain of any length is controllable on all invariant subspaces with a single local control acting on the first (or last) spin. As the dimension of the largest invariant subspace $\mathcal{H}_L$ is exponentially large with respect to the length of the chain, $\mathcal{H}_L$ is potentially a useful resource for UQC and it is the first example of a system where a single local control results in controllability on a subspace whose dimension is exponential in the number of qubits. It also illustrates the importance of the interaction type: If the Heisenberg (XXZ) coupling is replaced by XX coupling then the only subspace that remains controllable with a single local control is the single excitation subspace.

Subspace controllability problems of this kind have not been discussed in the literature very much and proving subspace controllability beyond the single excitation subspace is nontrivial and requires alternative computational approaches. The decomposition method suggested in [12] can be applied to discuss the reachable set [6], but further tools are required to establish controllability. The regularity-connectivity condition used by various authors [13–18] was applied to the problem considered here in [11] to infer subspace controllability, but the conditions, in particular strong regularity, could only be verified numerically for each subspace for short chains. Although specific eigenvectors and the corresponding eigenvalues for low excitation sectors can be found by a Bethe ansatz, the exponential complexity of the diagonalization is well beyond direct calculation when N is large. Another common approach to show controllability of a chain is by induction on the length of the chain, the method of choice to prove global controllability in [7] and many other works. However, as there is no simple relation between the subspace representations of $\{H_k\}$ for chains of lengths N and $N + 1$ beyond the single excitation subspace, the induction step cannot be completed. In general, the availability of a straightforward induction on the length of the chain relies on the fact that the DLA for a chain of length $N + 1$ can be expressed in terms of the DLA for a chain of length N, so we can complete the induction step by evaluating the DLA for the shorter chain and then use the connection between N and $N + 1$ to derive the DLA for the longer chain. Unfortunately, for our system there is no simple way of deriving any useful connections between the DLA generators for chains with size N and $N + 1$. Hence, a different argument is needed to construct a proof. In fact, when discussing the controllability for an N-spin system, rather than an n-level system, it is not a good idea to write the Hamiltonians in the energy eigenbasis of the system as they have a much simpler representation in terms of products of Pauli operators (as will become clear in the next section). As a result, the common method in the literature based on

connectivity graphs of the energy eigenvectors does not really help to assess controllability of an N-spin system. If we hope to use a connectivity graph to simplify the calculation of the DLA then it has to be a graph describing the connectivity of the N spins, rather than the $n = 2^N$ energy levels. Unfortunately, connectivity of the former graph is not sufficient to infer controllability as a spin system may be uncontrollable even if this graph is fully connected.

To prove subspace controllability we develop an approach based on decomposition of the Lie algebra into subspaces generated by n-body interaction terms. We then use induction arguments to derive general formulas for the dimension of these subspaces and sum over all subspaces to obtain the dimensionality of the Lie algebra of the entire system. We show that the resulting dimension can only be obtained if all subspaces are controllable. Using decomposition in terms of n-body interactions does not allow us to separately check controllability of a particular subspace, but there is no need to do so. Instead, we can prove the controllability for all subspaces at the same time, by finding the largest number of independent operators in the DLA generated by the system and control Hamiltonians. One difficulty in the proof is that the n-body operators generated by calculating the commutators are not all linearly independent, which makes it nontrivial to determine the rank of the operators generated, but fortunately, this problem can be overcome using a common trick in complex analysis.

This paper is organized as follows. In Sec. II we introduce different types of spin chains and define relevant symmetries for the system. In Sec. III we give a complete proof of subspace controllability for an arbitrary XXZ chain subject to a single end control and apply the technique to generalize the results to chains with anisotropic XYZ interactions. We further prove that the subspace controllability result is robust with regard to leakage of the single control field onto the neighboring spins. This result is interesting as it provides arguably the simplest model of a UQC one could imagine: a physical Hamiltonian with a single control switch to do the computation. For comparison, we show that the same result does not hold for XX chains, where a single end control can only give controllability on a subspace whose dimension does not scale exponentially with system size. In Sec. IV we investigate the XXZ or XYZ chains for various types of two controls and the according results present a complete picture of the minimal control resources for full controllability on the entire Hilbert space.

II. MODEL AND BASICS

The state of a quantum system is generally described in terms of a trace-one positive operator ρ, usually referred to as the density operator, acting on a Hilbert space $\mathcal{H}$. Any Hermitian operator on a spin-$\frac{1}{2}$ particle or qubit is a linear combination of the Pauli operators

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad (1)$$

and the identity $I = \mathrm{diag}(1,1)$. If a quantum system is composed of N spins then a local operator acting on the kth

spin is represented by $R_k = I \otimes \cdots \otimes I \otimes R \otimes I \otimes \cdots \otimes I$, where R is the 2×2 operator on the kth factor.

System Hamiltonian. We consider spin chains composed of N spins with spin-spin interactions characterized by the Hamiltonian

$$H_0 = \sum_n^{N-1} a_n X_m X_{n+1} + b_n Y_n Y_{n+1} + c_n Z_n Z_{n+1}, \quad (2)$$

which covers a large variety of systems: $a_n \neq b_n \neq c_n \neq 0$ corresponds to Heisenberg XYZ coupling, $a_n, b_n, c_n \neq 0$ with $a_n = b_n \neq c_n$ to Heisenberg XXZ coupling, $a_n = b_n = c_n \neq 0$ to isotropic Heisenberg coupling, $a_n = b_n \neq 0$ and $c_n = 0$ to XX coupling, and $a_n = b_n = 0$ and $c_n \neq 0$ to Ising coupling.

Controllability. The dynamics of the spin chain is characterized by the quantum Liouville equation

$$\dot{\rho} = -\frac{i}{\hbar}\left[H_0 + \sum_{j=1}^m f_j(t) H_j, \rho \right], \quad (3)$$

where H_0 is the system Hamiltonian in (2) and H_j, $j = 1, 2, \ldots, m$, is a series of control Hamiltonians with time-varying amplitudes $f_j(t)$. We say the system is density-operator controllable or simply controllable if the dynamical Lie algebra $\mathcal{L}$ generated by iH_j, $j = 0, 1, \ldots, m$, is equal to the largest Lie algebra that can be generated by anti-Hermitian operators iH_j acting on the 2^N-dimensional Hilbert space $\mathcal{H}$: either $u(2^N)$ or $su(2^N)$. This definition of controllability is very intuitive: It can be shown that if the system is controllable then any unitary process $U \in SU(2^N)$ can be generated up to a phase factor $e^{i\phi}$ by the dynamics (3) in finite time, for a suitable choice of the control fields $f_j(t)$. If $\mathcal{L} \subsetneq su(2^N)$ then there exists some unitary gate $U \in SU(2^N)$ that can never be generated under (3) [6]. The dynamical Lie algebra and the concept of controllability are very important for both theory and control applications as they characterize the reachable set of the control dynamics and allow us to decide whether a given control task can be achieved or not.

Symmetries. Symmetries of the Hamiltonian limit the type of processes a system is capable of generating and therefore controllability.

Definition 1. Let H_j, $j = 0, 1, \ldots, m$, be a set of Hamiltonians for a given quantum system. If there exists a Hermitian operator S that is not a multiple of the identity such that $[H_j, S] = 0$ for all j then S is called symmetry for the Hamiltonians.

The definition implies that for a symmetry S, H_j and S can be simultaneously diagonalized for all j.

Example 1. A simple class of symmetry operators for the system Hamiltonian (2) is of the form $S = A_1 A_2 \cdots A_N$, where $A_k = \alpha_1 X + \alpha_2 Y + \alpha_3 Z$ is a local operator on the kth spin. For symmetry operators of this form $[H_0, S] = 0$ requires $[a_{mn} X_m X_n + b_{mn} Y_m Y_n + c_{mn} Z_m Z_n, A_m A_n] = 0$ for any connected link (m, n) in (2). Observing the Pauli product relations $XX = YY = ZZ = I$, $XY = iZ$, $YZ = iX$, and $ZX = iY$ gives $[X_m X_n, S] = [Y_m Y_n, S] = [Z_m Z_n, S] = 0$ and thus $[H_0, S] = 0$ when A is one of the Pauli operators $\{X, Y, Z\}$. The operators $X_1 X_2 \cdots X_N$, $Y_1 Y_2 \cdots Y_N$, and $Z_1 Z_2 \cdots Z_N$ are often known as parity symmetries; H_0 commutes with all of them. Whether the controlled system has parity

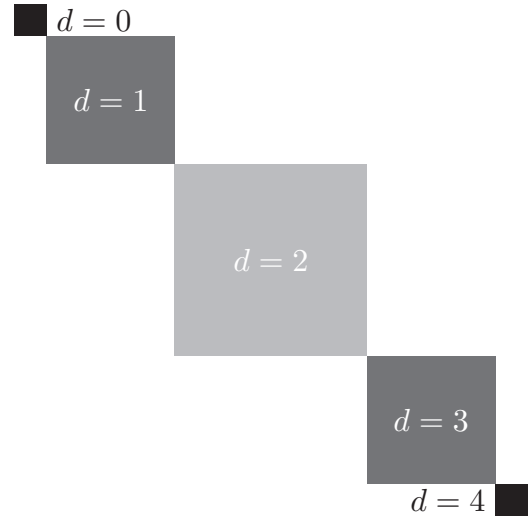FIG. 1. For $N = 4$, the XXZ network Hamiltonian H_0 and local control $H_1 = Z_k$ are simultaneously block diagonalized in five excitation subspaces $\mathcal{H}_d$, $d = 0, \ldots, 4$.

symmetries depends on the control Hamiltonians. Only the Z-parity operator $S_p = Z_1 Z_2 \cdots Z_N$ commutes with controls of the form $H_j = Z_j$, for example. Here S_p has two eigenspaces of dimension 2^{N-1} with eigenvalues (parity) $+1$ and -1, which are invariant under the dynamics if $[H_0, S_p] = [H_j, S_p] = 0$.

Example 2. If the system Hamiltonian (2) is of XXZ type then $[H_0, S_e] = 0$ for $S_e = \sum_j^N (Z_j + I)/2$. Here S_e has $N + 1$ distinct eigenvalues ranging from $n = 0$ to $n = N$. Hence, the Hilbert space decomposes $\mathcal{H} = \bigoplus_{k=0}^N \mathcal{H}_k$. If we denote the single-spin basis vectors by $|0\rangle$ (spin up) and $|1\rangle$ (spin down) and take the basis states of the N-spin systems to be the product states $|0 \cdots 0\rangle$ to $|1 \cdots 1\rangle$, then $\mathcal{H}_k$ is generated by the computational basis vectors with the number k of 1's, k being referred to as the number of excitations in the chain. For example, for $N = 4$, $\mathcal{H}_2$ is spanned by $|0011\rangle$, $|0101\rangle$, $|0110\rangle$, $|1001\rangle$, $|1010\rangle$, and $|1100\rangle$ and has dimension $\dim(\mathcal{H}_2) = d_{4,2} = 6$. If the control Hamiltonians only contain Z operators then S_e defines a symmetry, called excitation symmetry, and the system and control Hamiltonians are block diagonalized on the $N + 1$ invariant subspaces.

Having found all symmetries of the system, the entire Hilbert space can be written as a tensor product of minimal invariant subspaces $\mathcal{H} = \oplus_{d=1}^D \mathcal{H}_d$. The quantum dynamics is invariant on each $\mathcal{H}_d$ and the $\mathcal{H}_d$ cannot be further decomposed. The block-diagonal structure of the system Hamiltonian and control Hamiltonian illustrated in Fig. 1 implies that the associated dynamical Lie algebra $\mathcal{L}$ must be a subalgebra of $\bigoplus_{d=1}^D u(\dim \mathcal{H}_d)$.

Although the system is not controllable on the entire Hilbert space $\mathcal{H} = \mathcal{C}^{2^N}$ it may still be controllable on some or all of the subspaces $\mathcal{H}_d$. In the following we show that this subspace controllability holds for all subspaces even if the control is restricted to a single control acting locally on a single spin for most XYZ and XXZ chains.

III. SPIN CHAINS WITH SINGLE LOCAL END CONTROL

Many quantum systems, such as ultracold atoms, can be modeled as spin chains with Heisenberg interactions. Due to the symmetric roles played by the three Pauli operators, without loss of generality, we can assume that the local control is along the z direction, which physically corresponds to control fields being generated by an external magnetic field along the z direction. We find that subspace controllability depends on whether the spin-spin interactions in the two directions orthogonal to the control direction are equal or not, i.e., whether the spin chain is of (1) XXZ type (including XXX type) or (2) anisotropic XYZ type.

A. The XXZ chain

The system and control Hamiltonians for an XXZ chain of length N with a control in the z direction acting on spin 1 are

$$H_0 = \sum_j^N a_j(X_jX_{j+1} + Y_jY_{j+1} + c_jZ_jZ_{j+1}), \quad (4a)$$

$$H_1 = Z_1. \quad (4b)$$

As discussed above, the total excitation operator $S_e = \sum_j^N (Z_j + I)/2$ is a symmetry and due to this symmetry the Hilbert space of the N-spin system decomposes: $\mathcal{H} = \bigoplus_{k=0}^N \mathcal{H}_k$, where $\mathcal{H}_k$ is the invariant subspace with k excitations and $\dim(\mathcal{H}_k) = \binom{N}{k} \equiv d_{N,k}$, and the dynamical Lie algebra $\mathcal{L}$ of the controlled system (4) must be a subalgebra of $\mathcal{L}_T = \bigoplus_{k=0}^N \mathfrak{u}(d_{N,k})$. Notice that the structure of S_e ensures that traces of the Lie algebra generators on the kth and $(N-k)$th excitation subspace always add to 0 and thus $\mathcal{L}$ is also a subalgebra of $\mathfrak{su}(2^N)$.

To prove that the system is controllable on each $\mathcal{H}_k$, in particular $\mathcal{H}_{\lfloor N/2 \rfloor}$, we would like to show that $\mathcal{L} = \mathcal{L}_T$. However, we will see that this equality does not hold as there is a set of $N - 1$ elements in the Cartan subalgebra of $\mathcal{L}_T$ that cannot be generated by our Hamiltonians. However, these missing generators are not required for individual subspace controllability. The only effect they have is to impose nontrivial phase correlations between different subspaces, i.e., they impose some restrictions on the simultaneous control of different subspaces.

Since a Lie algebra is also a real vector space, we can drop some factors in the calculation and use linear combinations. We denote such (trivial) steps in the derivation by $\rightarrow$, which should be read as "generates" in the following. First, we observe that

$$[Z_1, H_0] \rightarrow X_1Y_2 - Y_1X_2,$$

$$[Z_1, X_1Y_2 - Y_1X_2] \rightarrow X_1X_2 + Y_1Y_2,$$

$$[X_1X_2 + Y_1Y_2, X_1Y_2 - Y_1X_2] \rightarrow Z_2 - Z_1 \rightarrow Z_2,$$

$$\vdots$$

Continuing this process, we can generate Z_j, $A_{jk} = X_jY_k - Y_jX_k$, and $B_{jk} = X_jX_k + Y_jY_k$ for all k,j as detailed in Appendix A. An operator is called an n-body operator if it contains n nontrivial factors, i.e., those comprised of X, Y, or Z Pauli operators. For example, Z_1Z_3 is a two-body operator, while $(Z_1 - Z_2)Z_3Z_4$ is a three-body operator. Denoting the

set of n-body operators in $\mathcal{L}$ by M_n, we list its elements and evaluate the rank:

$$M_1 = \{Z_k\},$$

$$M_2 = \{A_{jk}, B_{jk}, Z_jZ_k\},$$

$$M_3 = \{A_{jk}Z_m, B_{jk}Z_m, (Z_j - Z_k)Z_mZ_n\},$$

$$M_4 = \{A_{jk}Z_mZ_n, B_{jk}Z_mZ_n, A_{jk}A_{mn}, B_{jk}B_{mn}A_{jk}B_{mn},$$
$$\times (Z_j - Z_k)Z_lZ_mZ_n\},$$

$$\vdots$$

When ℓ is even, we can generate

$$C_{m_1,m_2}Z_{m_3}\cdots Z_{m_\ell},$$

$$C_{m_1,m_2}C_{m_3,m_4}Z_{m_5}\cdots Z_{m_\ell},$$

$$\vdots$$

$$C_{m_1,m_2}\cdots C_{m_{\ell-1},m_\ell},$$

$$(Z_{m_1} - Z_{m_2})Z_{m_3}\cdots Z_{m_\ell}.$$

When ℓ is odd, we can generate

$$C_{m_1,m_2}Z_{m_3}\cdots Z_{m_\ell},$$

$$C_{m_1,m_2}C_{m_3,m_4}Z_{m_5}\cdots Z_{m_\ell},$$

$$\vdots$$

$$C_{m_1,m_2}\cdots C_{m_{\ell-2},m_{\ell-1}}Z_{m_\ell},$$

$$(Z_{m_1} - Z_{m_2})Z_{m_3}\cdots Z_{m_\ell},$$

where $C_{k\ell}$ is either $A_{k\ell}$ or $B_{k\ell}$.

To compute $\text{rank}(M_\ell)$ we first evaluate the number of operators in the form $C_{m_1,m_2}\cdots C_{m_{2p-1},m_{2p}}$, which contains p pairs of operators of type $A = XY - YX$ or $B = XX + YY$. For a given N and p with $N \geqslant 2p > 0$, we denote the set of p-pair operators by $E_{N,p}$, e.g., for $N = 2p = 6$, $B_{12}B_{34}B_{56}$ is a 3-pair operator in $E_{6,3}$. The size of the set $E_{N,p}$ is obtained by simple combinatorics as

$$\frac{2^p}{p!}\binom{N}{2}\binom{N-2}{2}\cdots\binom{N-2(p-1)}{2} = p!\binom{N}{p}\binom{N-p}{p}.$$

However, not all of the elements in $E_{N,p}$ are linearly independent. For example, for $N = 4$ and $p = 2$, we find

$$B_{12}B_{34} - B_{13}B_{24} = A_{14}A_{23},$$

$$A_{12}A_{34} - A_{13}A_{24} = A_{14}A_{23},$$

$$B_{12}A_{34} - B_{13}A_{24} = B_{14}A_{23}.$$

Similarly, we can write down other dependence relations. Altogether only $1/2!$ of all 2-pair operators are linearly independent. In general, only $1/p!$ of all p-pair operators are linearly independent (Theorem 8, Appendix B):

$$\text{rank}(E_{N,p}) = \binom{N}{p}\binom{N-p}{p}. \quad (5)$$

Directly proving (5) is difficult as the linear dependence relations can become very complicated for large N and p.

For $\ell > 2$,

$$\text{rank}(M_\ell) = \sum_{p=1}^{\lfloor \ell/2 \rfloor} \text{rank}(E_{N,p}) \binom{N-2p}{\ell-2p} + \binom{N}{\ell} - 1.$$

After some simplification we obtain

$$\dim \mathcal{L} = \sum_{\ell=1}^{m} \text{rank}(M_\ell)$$
$$= \sum_{p=0}^{\lfloor N/2 \rfloor} \frac{N! 2^{N-2p}}{p!^2 (N-2p)!} - N + 1 = \binom{2N}{N} - N + 1$$

for both $N = 2m$ and $N = 2m+1$, where the preceding equation follows from the following.

Lemma 1.

$$\binom{2N}{N} = \sum_{p=0}^{\lfloor N/2 \rfloor} \frac{N!}{p!^2 (N-2p)!} 2^{N-2p}.$$

Proof. Let $f(x) = (x+1)^{2N}$. The term x^N has the coefficient $\binom{2N}{N}$ and

$$f(x) = (x^2 + 2x + 1)^N$$
$$= \sum_{p+q+r=N} \frac{N!}{p!q!r!} (x^2)^p (2x)^q$$
$$= \sum_{0 \leqslant p+q \leqslant N} \frac{N!}{p!q!(N-p-q)!} x^{2p+q} 2^q.$$

Hence,

$$\binom{2N}{N} = \sum_{0 \leqslant p+q \leqslant N, 2p+q=N} \frac{N!}{p!q!(N-p-q)!} 2^q$$
$$= \sum_{0 \leqslant p+q \leqslant N, 2p+q=N} \frac{N!}{p!(N-2p)!p!} 2^{N-2p}$$
$$= \sum_{p=0}^{\lfloor N/2 \rfloor} \frac{N!}{p!^2 (N-2p)!} 2^{N-2p}.$$

As discussed earlier, $\mathcal{L} \subset \mathcal{L}_T \equiv \oplus_{k=0}^{N} \mathfrak{u}(d_{N,k})$, with

$$\dim(\mathcal{L}_T) = \sum_{i=0}^{N} \dim[\mathfrak{u}(d_{N,k})] = \sum_{i=0}^{N} \binom{N}{k}^2 = \binom{2N}{N}.$$

All k-body Z-type operators, $k = 1, \ldots, N$, generate a Cartan subalgebra $\mathcal{C}$ in $\mathcal{L}_T$, with $\dim(\mathcal{C}) = 2^N$. Since we can only generate coupled k-body Z-type operators such as $(Z_{m_1} - Z_{m_2})Z_{m_3} \cdots Z_{m_k}$ for $k > 2$, the rank of all Z-type operators in $\mathcal{L}$ is $2^N - N + 1$, i.e., there are $N - 1$ independent Z-type operators that are in $\mathcal{L}_T$ but not in $\mathcal{L}$. Hence,

$$\dim(\mathcal{L}) \leqslant \dim(\mathcal{L}_T) - N + 1 = \binom{2N}{N} - N + 1 = \dim(\mathcal{L})$$

and $\dim(\mathcal{L})$ achieves the maximal allowed value. This is only possible if $\mathcal{L}$ is isomorphic to $\mathfrak{u}(d_{N,k})$ on each $\mathcal{H}_k$. The Lie algebra is indeed of type $\mathfrak{u}$ not $\mathfrak{su}$ on each subspace because the trace of the Hamiltonian H_0 restricted to any subspace is not zero, although the sum of the traces over all subspaces is zero. Hence, we have proved the following.

Theorem 1. For an XXZ chain of length N with a single local control on the end spin in the Z direction, the system is controllable on each of the $N + 1$ invariant excitation subspaces.

We note here that the result also applies to the special case of a fully isotropic Heisenberg XXX chain, in which case there is no preferred direction and the result applies for any local control applied in the x, y, or z direction. In particular, this theorem applies to antiferromagnetic Heisenberg chains ($a_j < 0$) and therefore justifies the observations in [11]. The latter paper also gives a nice motivation for this work. By cooling we can prepare the system in the ground state ψ_0, which is in the highest-dimensional excitation subspace $\mathcal{H}_{\lfloor N/2 \rfloor}$ at $t = t_0$. Then, by applying a single control Z_1 with amplitude $f(t)$ derived from optimization, we can generate the total Hamiltonian $H = H_0 + f(t)Z_1$ to drive the system into an arbitrary target state in $\mathcal{H}_{\lfloor N/2 \rfloor}$ at a later time $t = t_F$. In particular, we can generate perfect entangled pairs between the two end spins of the chain, which is an important quantum resource for many applications such as quantum communication or measurement-based quantum computing [11]. Moreover, as the dimension of $\mathcal{H}_{\lfloor N/2 \rfloor}$ increases exponentially with the number of qubits N, it can be used as a resource for universal quantum computation. For instance, we can encode qubits as $\alpha|01\rangle + \beta|10\rangle$, thereby performing universal quantum computation in $\mathcal{H}_{\lfloor N/2 \rfloor}$. This is a remarkable observation: We have found a system where quantum computation can be achieved with a single switch and where both the system and control Hamiltonian are physical, e.g., consist of nearest-neighbor two-body interactions, which are very common in physics. It provides possibly the simplest and most elegant way of achieving quantum computation so far (leaving efficiency issues beside [19]). Having only a single switch, we avoid the experimental difficulty of quickly changing field directions, which can be challenging due to hysteresis.

B. The XYZ chain

The previous results beg the question of controllability of inhomogeneous XYZ Heisenberg chains subject to local Z_1 control. In this case we have

$$H_0 = \sum_{j}^{N} a_j X_j X_{j+1} + b_j Y_j Y_{j+1} + c_j Z_j Z_{j+1}, \quad (6a)$$

$$H_1 = Z_1, \quad (6b)$$

with $a_j \neq b_j$. As discussed in Example 1, there exists a parity symmetry $S_p = Z_1 \cdots Z_N$ satisfying $[H_0, S_p] = [H_1, S_p] = 0$, with two invariant subspaces $\mathcal{H}_1$ and $\mathcal{H}_{-1}$, corresponding to eigenvalues ± 1 of S_p. Unlike in the homogeneous case the Hamiltonians cannot be further block diagonalized on each of the two subspaces. Thus, compared to the XXZ chain, the number of invariant subspaces for XYZ chain is reduced from $N + 1$ to 2 as a result of symmetry breaking between the x and y directions. Using the same technique as in the previous section, we compute all operators in the dynamical

Lie algebra $\mathcal{L}$ generated by H_0 and H_1 and show that the system is controllable on both subspaces:

$$
\begin{aligned}
[Z_1, H_0] &\rightarrow a_1 Y_1 X_2 - b_1 X_1 Y_2 \\
&\rightarrow a_1 X_1 X_2 + b_1 Y_1 Y_2, \\
&\times [a_1 Y_1 X_2 - b_1 X_1 Y_2, a_1 X_1 X_2 + b_1 Y_1 Y_2] \\
&\rightarrow (a_1^2 + b_1^2) Z_1 - 2a_1 b_1 Z_2 \rightarrow Z_2.
\end{aligned}
$$

Continuing this process, we obtain all Z_j, $a_j X_j X_{j+1} + b_j Y_j Y_{j+1}$, $a_j Y_j X_{j+1} - b_j X_j Y_{j+1}$, and $H_2 = \sum_j c_j Z_j Z_{j+1}$. Next we have

$$
[a_j Y_j X_{j+1} - b_j X_j Y_{j+1}, Z_{j+1}] \rightarrow a_j Y_j Y_{j+1} - b_j X_j X_{j+1}
$$

and together with $a_j X_j X_{j+1} + b_j Y_j Y_{j+1}$ we can decouple and get $X_j X_{j+1}$ and $Y_j Y_{j+1}$. Similarly, we can decouple and independently generate $X_j Y_{j+1}$ and $Y_j X_{j+1}$. This is a major difference from the XXZ case, where the XX and YY operators at neighboring locations cannot be decoupled. Due to such decoupling, we expect that the dynamical Lie algebra $\mathcal{L}$ generated by H_0 and H_1 will be larger than the XXZ case. Repeating the same generation process by calculating the commutators and letting P denote either the Pauli operator X or Y here, we obtain the k-body operators

$$
\begin{aligned}
M_1 &= \{Z_k\}, \\
M_2 &= \{P_j P_k, Z_j Z_k\}, \\
M_3 &= \{P_j P_k Z_m\} \cup \{Z_k Z_m Z_n\}, \\
&\quad \vdots
\end{aligned}
$$

For M_ℓ, when ℓ is even, we can generate

$$
\begin{aligned}
&P_{m_1} P_{m_2} Z_{m_3} \cdots Z_{m_\ell}, \\
&P_{m_1} P_{m_2} P_{m_3} P_{m_4} Z_{m_5} \cdots Z_{m_\ell}, \\
&\quad\quad\quad \vdots \\
&P_{m_1} P_{m_2} \cdots P_{m_{\ell-1}} P_{m_\ell}, \\
&Z_{m_1} Z_{m_2} \cdots Z_{m_\ell}.
\end{aligned}
$$

When ℓ is odd, we can generate

$$
\begin{aligned}
&P_{m_1} P_{m_2} Z_{m_3} \cdots Z_{m_\ell}, \\
&P_{m_1} P_{m_2} P_{m_3} P_{m_4} Z_{m_5} \cdots Z_{m_\ell}, \\
&\quad\quad\quad \vdots \\
&P_{m_1} P_{m_2} \cdots P_{m_{\ell-2}} P_{m_{\ell-1}} Z_{m_\ell}, \\
&Z_{m_1} Z_{m_2} \cdots Z_{m_\ell}.
\end{aligned}
$$

Compared with the XXZ chain, where we can only generate coupled Z-type operators such as $(Z_1 - Z_2) Z_3 Z_4$, for the XYZ chain, we can separately generate $Z_1 Z_3 Z_4$ and $Z_2 Z_3 Z_4$. Here M_ℓ can be divided into two subsets: the set of $(P - Z)$-type operators and the set of Z-type operators, where each $P - Z$ operator can contain $2p$ operators of type P and $N - 2p$ operators of type Z, $p = 1, \ldots, \lfloor \ell/2 \rfloor$. Hence, a basic

combinatorics argument gives

$$
\text{rank}(M_\ell) = \sum_{p=1}^{k} 2^{2p} \binom{N}{2p} \lfloor \ell/2 \rfloor r_p \binom{N-2p}{\ell-2p} + \binom{N}{\ell}
$$

and the dimension of $\mathcal{L}$ ($N > 2$),

$$
\dim(\mathcal{L}) = \sum N_\ell = 2^N \sum_{k=0}^{\lfloor N/2 \rfloor} \binom{N}{2k} - 2 = 2^{2N-1} - 2,
$$

where we have used the identity

$$
\sum_{k=0}^{\lfloor N/2 \rfloor} \binom{N}{2k} = \sum_{k=0}^{\lfloor N/2 \rfloor} \binom{N}{2k+1} = 2^{N-1}.
$$

Since H_0 and H_1 are simultaneously block diagonalized on $\mathcal{H}_1 \oplus \mathcal{H}_{-1}$, $\mathcal{L}$ must be a subalgebra of $\mathcal{L}_T = \text{u}(2^{N-1}) \oplus \text{u}(2^{N-1})$. Moreover, since the k-body Z operators in $\mathcal{L}$ are generated from the $(k+1)$-body $P - Z$ operators, $\mathcal{L}$ does not include two Z-type operators, the identity I and S_p, which are contained in $\mathcal{L}_T$. Hence, we have

$$
\dim(\mathcal{L}) \leqslant \dim(\mathcal{L}_T) - 2 = 2^{2N-1} - 2 = \dim(\mathcal{L})
$$

and $\dim(\mathcal{L})$ achieves the allowed maximal value, which is only possible when $\mathcal{L} = \text{u}(2^{N-1})$ or $\text{su}(2^{N-1})$ on both subspaces $\mathcal{H}_1$ and $\mathcal{H}_{-1}$. Noticing that H_0 and H_1 are trace zero on $\mathcal{H}_1$ and $\mathcal{H}_{-1}$ for $N > 2$, we must have $\mathcal{L} = \text{su}(2^{N-1})$ on both $\mathcal{H}_1$ and $\mathcal{H}_{-1}$ for $N > 2$. For $N = 2$ it is easy to check that $\mathcal{L} = \text{u}(2)$ on $\mathcal{H}_1$ and $\mathcal{H}_{-1}$. Thus, we have proved the following.

Theorem 2. For an XYZ chain of length N with a single local control on the end spin in the Z direction, the system is controllable on each of the two invariant subspaces $\mathcal{H}_1$ and $\mathcal{H}_{-1}$.

As there is nothing special about the z direction here, this result applies for a local control in the x, y, or z direction.

C. Control leakage on neighboring spins

The previous assumption of the control affecting only a single spin is an idealization. In practice, it is difficult to apply a control field that only acts on a single spin without affecting its neighbors to some extent. Hence, a more realistic assumption is that a control applied to one spin will also perturb neighboring spins due to field leakage. This leads to a modification of the control Hamiltonian from $H_1 = Z_1$ in the ideal case to $H_1 = \sum_{j=1}^{k} \gamma_j Z_j$, where γ_j characterizes the effect of the field leakage. We consider two typical cases: linear $\gamma_j = -\alpha j + \beta$ and exponential $\gamma_j = e^{-\mu(j-1)^2}$ decay. In the following, we show that the subspace controllability results discussed in the previous sections are robust with regard to such control leakage, in that the invariant subspace structure and controllability of the system remain unchanged.

Starting with our system and control Hamiltonians

$$
H_0 = \sum_{j=1}^{N} a_j X_j X_{j+1} + b_j Y_j Y_{j+1} + c_j Z_j Z_{j+1}, \quad \text{(7a)}
$$

$$
H_1 = \sum_{j=1}^{k} \gamma_j Z_j \quad\quad\quad\quad\quad \text{(7b)}
$$

and defining the adjoint action of H_1 on $\mathcal{H}_1$ as $\mathrm{Ad}_{H_1}(H_0) = [H_1, H_0]$ and $A_j = a_j X_j X_{j+1} + b_j Y_j Y_{j+1}$, we have

$$\mathrm{Ad}_{H_1}^{(2)}(H_0) = \gamma_{12}^2 A_1 + \cdots + \gamma_{k-1,k}^2 A_{k-1} + \gamma_k^2 A_k,$$

$$\mathrm{Ad}_{H_1}^{(4)}(H_0) = \gamma_{12}^4 A_1 + \cdots + \gamma_{k-1,k}^4 A_{k-1} + \gamma_k^4 A_k,$$

$$\vdots$$

$$\mathrm{Ad}_{H_1}^{(2k)}(H_0) = \gamma_{12}^{2k} A_1 + \cdots + \gamma_{k-1,k}^{2k} A_{k-1} + \gamma_k^{2k} A_k,$$

where we used the shorthand notation $\gamma_{k\ell} = \gamma_k - \gamma_\ell$. The coefficients in this expression can be gathered in a matrix

$$V = \begin{pmatrix} (\gamma_1 - \gamma_2)^2 & \cdots & (\gamma_{k-1} - \gamma_k)^2 & \gamma_k^2 \\ (\gamma_1 - \gamma_2)^4 & \cdots & (\gamma_{k-1} - \gamma_k)^4 & \gamma_k^4 \\ \vdots & \cdots & \vdots & \vdots \\ (\gamma_1 - \gamma_2)^{2k} & \cdots & (\gamma_{k-1} - \gamma_k)^{2k} & \gamma_k^{2k} \end{pmatrix}.$$

Case (1) When the leakage of the local control is linear, i.e., $\gamma_j - \gamma_{j+1} = \gamma_\ell - \gamma_{\ell+1}$ for different j and ℓ, we can generate the operator $A_k = a_k X_k X_{k+1} + b_k Y_k Y_{k+1}$ from any two rows of V. Analogously, we can generate $a_k X_k Y_{k+1} - b_k Y_k X_{k+1}$ and hence generate $Z_k - Z_{k+1}$. From A_k, we can also generate $B_0 = \mathrm{Ad}_{H_1}^{(2)}(H_0) - \gamma_k^2 A_k$. From $Z_k - Z_{k+1}$ and B_0, we can sequentially generate A_j and Z_j, $j = k-1, k-2, \ldots, 1$.

Case (2) When the leakage of the local control decays nonlinearly, e.g., $\gamma_j = e^{-\mu(j-1)^2}$, we have $\gamma_j - \gamma_{j+1} \neq \gamma_\ell - \gamma_{\ell+1} \neq \gamma_k$, and from the property of Vandermonde matrix, $\det(V) \neq 0$. Hence we can generate each A_j, $j = 1, \ldots, k$. Together with H_1, we can decouple and generate Z_j, $j = 1, \ldots, k$.

Hence, in both cases, $\mathcal{L}$ generated by H_0 and H_1 in (7) is the same as that generated by H_0 and $H_1 = Z_1$. In general, for other types of nonlinear leakage, the above reasoning is valid for almost all choices of γ_j. Thus we have the following.

Theorem 3. For an XXZ or XYZ chain of length N, under a single local control on the end spin in the Z direction with leakage to the neighboring spins, the system is controllable on each of the invariant subspaces.

D. The XX chain under a single end control

Based on the previous results, one might be tempted to conclude that the controllability results in spin chains with other types of couplings as well. We will now show that this is not the case and the presence of spin-spin interactions in all three directions is essential to guarantee subspace controllability. When the Heisenberg coupling is replaced by XX coupling, subspace controllability no longer holds, except on the first excitation subspace. Specifically, the Hamiltonian describing an XX chain and a single end control in the Z direction are written as

$$H_0 = \sum_n^N \gamma_n (X_n X_{n+1} + Y_n Y_{n+1}), \quad H_1 = Z_1. \quad (8)$$

Theorem 4. For an XX chain of length N with a single local control on the end spin in the Z direction, the associated dynamical Lie algebra $\mathcal{L}$ is a faithful representation of $u(N)$ in each excitation subspace $\mathcal{H}_k$, $k = 1, \ldots, N-1$.

Proof. To prove that $\mathcal{L}$ is indeed isomorphic to $u(N)$, we determine all independent operators generated from the Hamiltonians, as we did in previous sections, and show that these operators satisfy the same commutation relations as the standard basis of $u(N)$ [10]. However, to make the analysis of faithful representations simpler and more convenient, we transform the original representation using the Jordan-Wigner transformation, a powerful tool initially developed in theoretical physics: Defining

$$a_m := \prod_{n < m} Z_n (X - iY)_m,$$

where a_m are fermionic annihilation operators, with the canonical anticommutation relations

$$\{a_m, a_n\} = \{a_m^\dagger, a_n^\dagger\} = 0, \quad \{a_m, a_n^\dagger\} = \delta_{mn},$$

the Hamiltonians are transformed into

$$H_0 = \sum_{n=1}^N \gamma_n (a_n^\dagger a_{n+1} + a_{n+1}^\dagger a_n),$$

$$H_1 = a_1^\dagger a_1.$$

By calculating the commutation relations between the Hamiltonians, we can verify the following identities:

$$[iH_1, iH_0] \to y_{12} := a_1^\dagger a_2 - a_2^\dagger a_1,$$

$$[iH_1, y_{12}] \to x_{12} := i(a_1^\dagger a_2 + a_2^\dagger a_1),$$

$$[x_{12}, y_{12}] \to z_2 := i a_2^\dagger a_2.$$

Then we can generate $\bar{H}_0 = H_0 - \gamma_1 x_{12}$, which represents the system Hamiltonian for a chain of length $N-1$, and z_2 amounts to the end control on $\bar{H}_0$. Thus, by induction we can sequentially generate

$$y_{n,n+1} := a_n^\dagger a_{n+1} - a_{n+1}^\dagger a_n, \quad n = 1, \ldots, N-1$$

$$x_{n,n+1} := i(a_n^\dagger a_{n+1} + a_{n+1}^\dagger a_n), \quad n = 1, \ldots, N-1$$

$$z_n := i(a_n^\dagger a_n), \quad n = 1, \ldots N.$$

Hence, we have generated three kinds of anti-Hermitian operators $x_{n,n+1}$, $y_{n,n+1}$, and z_n, satisfying

$$[x_{mn}, z_n] = y_{mn}, \quad (9a)$$

$$[y_{mn}, z_n] = -x_{mn}, \quad (9b)$$

$$[x_{mk}, x_{kn}] = y_{mn}, \quad (9c)$$

$$[x_{mk}, y_{kn}] = -x_{mn}, \quad (9d)$$

$$[x_{mn}, y_{mn}] = 2(z_m - z_n), \quad (9e)$$

which are the same as the commutation relations satisfied by the standard basis of $u(N)$ [10]. Hence, we have $\mathcal{L} = u(N)$.

Finally, to show that $\mathcal{L}$ is a faithful representation in each excitation subspace $\mathcal{H}_k$, $k = 1, \ldots, N-1$, it is sufficient to show that the images of the generators $x_{n,n+1}$, $y_{n,n+1}$, and z_n in H_k are nonzero. Choose a vector $|\alpha\rangle \in \mathcal{H}_k$ in the computational basis with n and $n+1$ positions as $|0\rangle$ and $|1\rangle$ and define another basis vector $|\beta\rangle \in \mathcal{H}_k$ such that β only differs from α

at n and $n+1$ positions, with values $|1\rangle$ and $|0\rangle$. Restricted on $\mathcal{H}_k$, we have

$$\langle\beta|y_{n,n+1}|\alpha\rangle = \langle\beta|a_n^\dagger a_{n+1}|\alpha\rangle = 1,$$

$$\langle\beta|x_{n,n+1}|\alpha\rangle = \langle\beta|a_n^\dagger a_{n+1}|\alpha\rangle = i,$$

$$\langle\beta|z_n|\beta\rangle = \langle\beta|a_n^\dagger a_n|\beta\rangle = 1.$$

Hence, on each $\mathcal{H}_k$, $k = 1,\ldots,N-1$, $\mathcal{L}$ is a faithful representation of $u(N)$.

IV. MINIMAL CONTROLS FOR FULL CONTROLLABILITY

In the previous section we discussed the control problem of spin chains with a single local control acting at the end of the spin chain. In general, as the number of controls increases, symmetries will disappear and the system will become fully controllable on the entire Hilbert space under a sufficient number of independent controls. An interesting question in this context is what minimal control resources are required to make our chain fully controllable and whether the type and location of the control actuator matter. For example, does it matter if we control the end spin or will any spin in the chain do, or are controls acting in different directions preferable to controls acting in the same direction on different spins?

A. Controlling Z_1 and X_1

In [7] it was proved by the propagation property that an XXZ chain with two independent local controls such as $H_1 = Z_1$ and $H_2 = X_1$ is fully controllable on the entire space. We can rederive this result from our analysis in the previous section: Observing the operators generated by H_0 and H_1 and writing down the operators generated by H_0 and H_2, it is easy to see that we can generate all k-body Pauli operators $k = 1,\ldots,N$ in $u(2^N)$. Hence the system is fully controllable.

Theorem 5. For an XXZ or XYZ chain of length N, with two local controls on the end spin, $H_1 = Z_1$ and $H_2 = X_1$, the system is controllable on the whole space.

B. Controlling Z_k and X_k

Theorem 5 shows that two controls acting in orthogonal directions on the end spin suffice to make the system controllable on the entire Hilbert space. What if we can fully control one spin at other locations? It is not easy to prove controllability in this case using the propagation property, but it is easy to prove using our computational technique that two independent controls acting in orthogonal directions such as Z and X on the kth spin in the chain, giving rise to the Hamiltonians

$$H_0 = \sum_j^N a_j X_j X_{j+1} + b_j Y_j Y_{j+1} + c_j Z_j Z_{j+1},$$

$$H_1 = Z_k, \quad H_2 = X_k,$$

are sufficient for controllability on the entire Hilbert space, except when $N = 2k + 1$, in which case the Hamiltonians exhibit mirror permutation symmetry with respect to the center spin.

To extend our controllability results to controls acting on the kth spin, we show that given H_0, Z_k, and X_k we can generate Z_1 and X_1 and apply the previous theorem. Without loss of generality assume $k \leqslant \lfloor N/2 \rfloor$. For simplicity let $B_k = a_k X_k X_{k+1} + b_k Y_k Y_{k+1}$ and note $[Z_k,[Z_k,H_0]] = B_{k-1} + B_k$,

$$P := \tfrac{1}{4}[B_{k-1} + B_k, [B_{k-1} + B_k, Z_k]]$$

$$= \left(a_{k-1}^2 + b_{k-1}^2 + a_k^2 + b_k^2\right)Z_k + W - Q_1,$$

$$W := 2(a_{k-1}a_k X_{k-1}X_{k+1} + b_{k-1}b_k Y_{k-1}Y_{k+1})Z_k,$$

$$Q_1 := 2a_{k-1}b_{k-1} Z_{k-1} + 2a_k b_k Z_{k+1}.$$

The term proportional to Z_k can be subtracted from P and further subtracting $\tfrac{1}{4}[X_k,[X_k,Q_1 + W]] = W$, we generate Q_1. Next setting $c_k = 2a_k b_k$ and $d_k = c_k c_{k+1}^5$ we obtain

$$\tfrac{1}{4}[Q_1,[Q_1,H_0]] \to c_{k-1}^2 B_{k-2} + c_k^2 B_{k+1} = D_1,$$

$$\tfrac{1}{4}[D_1,[D_1,Q_1]] \to c_{k-2}c_{k-1}^5 Z_{k-2} + c_{k+1}c_k^5 Z_{k+2} = Q_2.$$

Iterating the procedure, replacing Q_1 above by Q_2, etc., we can sequentially generate coupled B and Z terms of the form

$$B_{k-1} + B_k, \quad d_{k-1}Z_{k-1} + d_{k+1}Z_{k+1},$$

$$d'_{k-2}B_{k-2} + d'_{k+1}B_{k+1}, \quad d_{k-2}Z_{k-2} + d_{k+2}Z_{k+2},$$

$$d'_{k-3}B_{k-3} + d'_{k+2}B_{k+2}, \quad d_{k-3}Z_{k-3} + d_{k+3}Z_{k+3},$$

$$\vdots$$

$$d'_1 B_1 + d'_{2k-1}B_{2k-1}, \quad d_1 Z_1 + d_{2k-1}Z_{2k-1}.$$

When we hit the end of the chain we continue generating

$$B_{2k-1}Z_{2k} - Z_{2k-1},$$

$$B_{2k}Z_{2k+1} - Z_{2k},$$

$$\vdots$$

$$B_{N-1}Z_{N-1} - Z_N.$$

Finally, starting from $[Z_{N-1} - Z_N, H_0]$, we can sequentially generate $Z_{N-1} - Z_N, Z_{N-2} - Z_{N-1}, \ldots, Z_k - Z_{k+1}$. Together with Z_k, we can therefore generate Z_{k+1} and hence $Z_{k+1},\ldots,Z_{2k-1},\ldots,Z_N$. Together with $d_1 Z_1 + d_{2k-1}Z_{2k-1}$, we can decouple and generate Z_1. Similarly, starting with $[X_k,[X_k,H_0]]$ instead of $[Z_k,[Z_k,H_0]]$, we can generate X_1.

Theorem 6. For an XXZ or XYZ chain of length N, with two local controls on the kth spin, $H_1 = Z_k$ and $H_2 = X_k$, and $N \neq 2k + 1$ the system is controllable on the whole space.

C. Controlling Z_1 and X_k

Finally, it is interesting to consider whether two independent controls acting on different spins such as Z_1 and X_k on the first and the kth spins are still sufficient for full controllability for an XYZ or XXZ chain. In this case the Hamiltonians are

$$H_0 = \sum_j^N a_j X_j X_{j+1} + b_j Y_j Y_{j+1} + c_j Z_j Z_{j+1},$$

$$H_1 = Z_1, \quad H_2 = X_k.$$

We show in Appendix A that H_0 and H_1 can generate the Ising coupling term $H_{ZZ} = \sum_j^{N-1} c_j Z_j Z_{j+1}$. Taking commutators

with the second control X_k further gives

$$[X_k, H_{ZZ}] \to c_{k-1} Z_{k-1} Y_k + c_k Y_k Z_{k+1},$$

$$[X_k, a_{k-1} X_{k-1} X_k + b_{k-1} Y_{k-1} Y_k] \to Y_{k-1} Z_k,$$

$$[X_k, Y_{k-1} Z_k] \to Y_{k-1} Y_k,$$

$$[Y_{k-1} Y_k, c_{k-1} Z_{k-1} Y_k + c_k Y_k Z_{k+1}] \to X_{k-1}.$$

Continuing this process, we can sequentially generate $X_{k-2}, X_{k-3}, \ldots, X_2$ and finally X_1 and by Theorem 5 we have the following.

Theorem 7. For an XXZ or XYZ chain of length N, with two local controls Z_1 and X_k, $1 \leqslant k \leqslant N$, on the first and the kth spins, the system is controllable on the whole space.

V. CONCLUSION

We have proved that spin chains with Heisenberg coupling, although not fully controllable with a single control field acting locally due to symmetries, are fully controllable on all invariant subspaces of the symmetry operator. The symmetries differ depending on whether the coupling is isotropic or anisotropic. If the coupling is isotropic in the directions perpendicular to the control field then there are $N + 1$ invariant subspaces of dimensions $d_k = \binom{N}{k}$ ranging from 1 for $k = 0, N$ to $\binom{N}{N/2}$ for the largest subspace with $k = N/2$; otherwise there are only two subspaces of dimension 2^{N-1} corresponding to parity symmetry with regard to the control direction. In both cases the dimension of the largest invariant subspace increases exponentially with the number of spins, showing that a Heisenberg spin chain with a single local control is theoretically sufficient for scalable quantum computation. Notably, the controllability result is robust with regard to system inhomogeneity (nonuniform interaction strengths) and control leakage, i.e., unwanted effects of the control field on nearby spins.

To prove these results we developed a technique to systematically evaluate the dynamical Lie algebra of the system based on the decomposition of the operators into subspaces spanned by n-body interaction terms, which can be iteratively constructed starting from the given local control and the two-body interactions present in the system Hamiltonian. This approach enables us to construct the DLA and evaluate its dimension for chains of any length, different symmetries, and different types of controls. It is also applicable when the propagation property is not fulfilled and thus simple induction on the length of the chain is not possible, for example, when we have only a single local control (as opposed to two linearly independent controls) acting on one end of the chain, local controls in orthogonal directions acting on an interior spin, or local controls acting on different spins. The techniques used to iteratively construct the n-body interaction subspaces and evaluate their dimension can also be applied to construct the DLA for spin networks with different topologies and different types of interactions.

A comparison of chains with different types of iterations such as XXZ, XYZ, and XX shows that the interaction type is important. If there is no spin-spin coupling in the direction of the applied control field, as in the XX case with local controls in the Z direction, then the DLA on all excitation subspaces is simply a high-dimensional representation of the dynamical Lie

algebra on the single excitation subspace. Such a spin system may be of interest for information transfer applications (e.g., quantum wires) but not applications such as scalable quantum computing, which require a DLA that grows exponentially in the number of qubits (or spins). If there is spin-spin coupling in the direction of the control field then our results show that a single local control is sufficient for controllability of an exponentially large subspace, and in general the addition of a second local control acting in a different direction, either on the same spin or a different spin, is sufficient to achieve controllability on the entire space. This does increase the overall Hilbert space dimension but does not change the scaling of the Hilbert space dimension with the number of qubits, showing that the benefit of the addition of a second local control in a direction orthogonal to the first is not significant for large N and the costs of including physical effects such as hysteresis may well outweigh any gains.

APPENDIX A: THE XXZ AND XYZ CHAINS WITH Z_1 CONTROL

We calculate the Lie algebra $\mathcal{L}$ generated by H_0 and H_1 in (4).

Step 1. Show that we can implement the local operators Z_k for $k = 1, \ldots, N$ and the nearest-neighbor two-body interaction terms $A_k = X_k Y_{k+1} - Y_k X_{k+1}$ and $B_k = X_k X_{k+1} + Y_k Y_{k+1}$ for $k = 1, \ldots, N-1$ and reduce the Heisenberg Hamiltonian H_0 to an Ising chain Hamiltonian $H_{zz} = \sum_{j=1}^{N-1} a_j c_j Z_j Z_{j+1}$. The proof is straightforward. The elementary product rules for Pauli matrices give

$$[Z_1, H_0] \to A_1, \quad [Z_1, A_1] \to B_1,$$

$$[A_1, B_1] \to Z_2 - Z_1 \to Z_2.$$

Subtracting $a_1 B_1$ from H_0 and repeating the above steps with H_0 replaced by $H_0' = H_0 - a_1 B_1$ and Z_1 replaced by Z_2, we generate A_2, B_2, and Z_3, and iterating the process, we generate all Z_k, A_k, and B_k and reduce H_0 to the Ising chain coupling term $H_{ZZ} = H_0 - \sum_j a_j B_j$.[1]

Step 2. Show that we can generate the nearest-neighbor three-body terms $Z_k B_{k+1}$, $B_k Z_{k+2}$, $Z_k A_{k+1}$, and $A_k Z_{k+2}$ and the individual nearest-neighbor Z-coupling terms $Z_k Z_{k+1}$ for $1 \leqslant k < N$:

$$[A_1, H_{ZZ}] \to B_1 Z_3,$$

$$[A_1, B_1 Z_3] \to (Z_1 - Z_2) Z_3,$$

$$[A_2, (Z_1 - Z_2) Z_3] \to Z_1 B_2,$$

$$[A_2, H_{ZZ}] \to Z_1 B_2 + B_2 Z_4,$$

$$[A_2, B_2 Z_4] \to (Z_2 - Z_3) Z_4,$$

$$[A_3, (Z_2 - Z_3) Z_4] \to Z_2 B_3,$$

---

[1]Notice the difference here from the case where there are two independent local controls such as X_1 and Y_1. In this case we can immediately generate $Z_1 = [X_1, Y_2]$ and taking commutators of these local operators with H_0, we immediately generate su(2) and we can then proceed to show controllability by induction on the length of the chain.

$$[A_3, H_{ZZ}] \to Z_2 B_3 + B_3 Z_5,$$
$$[A_3, B_3 Z_5] \to (Z_3 - Z_4) Z_5,$$
$$\vdots$$

which shows that we can generate the three-body terms $Z_k B_{k+1}$ and $B_k Z_{k+2}$, from which we obtain $[Z_{k+1}, Z_k B_{k+1}] \to Z_k A_{k+1}$ and $[Z_k, B_k Z_{k+2}] \to A_k Z_{k+2}$. Finally, let $A_{j,k} = X_j Y_k - Y_j Y_k$ and $B_{j,k} = X_j X_k + Y_j Y_k$ and observe

$$[A_k, B_{k-1}] \to B_{k-1,k+1} Z_k,$$
$$[A_{k-1}, Z_{k-1} B_k] \to B_{k-1,k+1},$$
$$[Z_{k-1}, B_{k-1,k+1}] \to A_{k-1,k+1},$$
$$[B_{k-1,k+1} Z_k, A_{k-1,k+1}] \to Z_{k-1} Z_k - Z_k Z_{k+1}.$$

Together with H_{ZZ} we can decouple and generate $Z_k Z_{k+1}$ for $1 \leqslant k < N$.

Step 3. We use the nearest-neighbor two-body and three-body interaction terms A_k, B_k, $Z_k Z_{k+1}$, and $B_k Z_{k+2}$ to show that we can generate the non-nearest-neighbor two-body interactions A_{kj}, B_{kj}, and $Z_k Z_j$ for any $1 \leqslant k < j \leqslant N$ and the three-body terms $A_{kj} Z_m$ and $B_{kj} Z_m$:

$$[A_k, Z_{k+1} Z_{k+2}] \to B_k Z_{k+2},$$
$$[B_k Z_{k+2}, A_{k+1}] \to B_{k,k+2},$$
$$[Z_k, B_{k,k+2}] \to A_{k,k+2},$$
$$[A_{k,k+2}, Z_{k+2} Z_{k+3}] \to B_{k,k+2} Z_{k+3},$$
$$[B_{k,k+2} Z_{k+3}, A_{k,k+2}] \to B_{k,k+3},$$
$$\vdots$$

Continuing this process, we generate all A_{kj} and B_{kj} for $1 \leqslant k < j \leqslant N$. We also generate the three-body terms $B_{kj} Z_{j+1}$, from which we can generate $(Z_k - Z_j) Z_{j+1}$ together with the already generated $Z_j Z_{j+1}$ and $Z_k Z_j$ for $k < j$, and finally the three-body terms $A_{kj} Z_m$ and $B_{kj} Z_m$.

Step 4. So far we have generated the local operators Z_k, the two-body operators A_{jk}, B_{jk}, and $Z_j Z_k$ and the three-body operators $B_{jk} Z_m$ and $A_{jk} Z_m$. From these operators we generate the four-body operators and three-body Z operators

$$[B_{jk} Z_m, A_{mn}] \to B_{ij} B_{mn},$$
$$[B_{jk} Z_m, Z_k Z_n] \to A_{jk} Z_m Z_n,$$
$$[B_{jk}, A_{jk} Z_m Z_n] \to (Z_j - Z_k) Z_m Z_n.$$

Continuing this process, we sequentially generate ℓ-body XYZ-mixed operators and $(\ell - 1)$-body Z operators. When ℓ is even, we can generate

$$B_{m_1,m_2} Z_{m_3} \cdots Z_{m_\ell},$$
$$B_{m_1,m_2} B_{m_3,m_4} Z_{m_5} \cdots Z_{m_\ell},$$
$$\vdots$$
$$B_{m_1,m_2} \cdots B_{m_{\ell-1},m_\ell},$$
$$(Z_{m_1} - Z_{m_2}) Z_{m_3} \cdots Z_{m_\ell}.$$

When ℓ is odd, we can generate

$$B_{m_1,m_2} Z_{m_3} \cdots Z_{m_\ell},$$
$$B_{m_1,m_2} B_{m_3,m_4} Z_{m_5} \cdots Z_{m_\ell},$$
$$\vdots$$
$$B_{m_1,m_2} \cdots B_{m_{\ell-2},m_{\ell-1}} Z_{m_\ell},$$
$$(Z_{m_1} - Z_{m_2}) Z_{m_3} \cdots Z_{m_\ell}.$$

APPENDIX B: RANK OF $E_{N,p}$

Theorem 8. For given N and p with $N \geqslant 2p$, the rank of the p-pair operator set $E_{N,p}$ is equal to $\binom{N}{p}\binom{N-p}{p}$.

Since, when evaluating $\text{rank}(E_{N,p})$, only linear relations between the operators of $E_{N,p}$ are involved, we can consider every element of $E_{N,p}$ as a polynomial in terms of $2N$ variables and transform the original problem into evaluating the rank of a set of polynomials. Specifically, for positive integers N and p with $N \geqslant 2p$, let E be the set of any polynomials in terms of $2N$ variables $x_1, x_2, \ldots, x_N$ and $y_1, y_2, \ldots, y_N$, satisfying the following form:

$$P[x_1, x_2, \ldots, x_N; y_1, y_2, \ldots, y_N]$$
$$= q(m_1, m_2) q(m_3, m_4) \cdots q(m_{2p-1}, m_{2p}) q(m_{2p-1}, m_{2p}),$$

where $q(j,k)$ can take two forms, either $q(j,k) = x_j x_k + y_j y_k$ or $q(j,k) = x_j y_k - y_j y_k$, and the m_k's are distinct from each other, with $m_k \in [1, \ldots, N]$, $k = 1, \ldots, 2p$. In other words, any element in E is a product of p terms, each taking the form $xx + yy$ or $xy - yx$. For example, the following polynomials are in E:

$$(x_1 x_2 + y_1 y_2)(x_3 x_4 + y_3 y_4) \cdots (x_{2p-1} x_{2p} + y_{2p-1} y_{2p}),$$
$$(x_1 y_2 - y_1 x_2)(x_3 y_4 - y_3 x_4) \cdots (x_{2p-1} y_{2p} - y_{2p-1} x_{2p}).$$

As discussed earlier, the total number of polynomials in E is $p! \binom{N}{p}\binom{N-p}{p}$. However, not all of them are linearly independent and we aim to evaluate $\text{rank}(E)$ over $\mathbb{R}$.

Since the numbers $2N$ of variables x_j and y_j are linearly independent, the rank of E over $\mathbb{R}$ is the same as its rank over $\mathbb{C}$, i.e., $\text{rank}_{\mathbb{R}}(E) = \text{rank}_{\mathbb{C}}(E)$. Next, over the field $\mathbb{C}$, we can apply the reversible transformations $z_j = x_j + i y_j$ and $z_j^* = x_j - i y_j$ and then all elements in E can be expressed as polynomials over $\mathbb{C}$ in terms of z_j and z_k^*. This is equivalent to considering raising and lowering operators in the algebra. Specifically,

$$x_j x_k + y_j y_k = \text{Re}(z_j^* z_k),$$
$$x_j y_k - y_j x_k = \text{Im}(z_j^* z_k).$$

Then any element $q(m_1, m_2) \cdots q(m_{2p-1}, m_{2p})$ in E can be rewritten as $Q(z_{m_1}^* z_{m_2}) \cdots Q(z_{m_{2p-1}}^* z_{m_{2p}})$, where $Q(z)$ is an operation that takes either the real or the imaginary part of z. Hence, all elements in E can be rewritten in terms of the number $2N$ of independent complex variables: $z_1, \ldots, z_N$ and $z_1^*, \ldots, z_N^*$. Next we can show that the space generated by the set E is the same as the one generated by the set F whose elements are in the following form: $z_{m_1}^* z_{m_2} \cdots z_{m_{2p-1}}^* z_{m_{2p}}$, where $m_k \in [1, \ldots, N]$, $k = 1, \ldots, 2p$. In order to see this, we will show that $Q(z_{m_1}^* z_{m_2}) \cdots Q(z_{m_{2p-1}}^* z_{m_{2p}})$ in E can be

generated by the elements in F: From the sum of or the difference between $z_{m_1}^* z_{m_2} \cdots z_{m_{2p-1}}^* z_{m_{2p}}$ and $z_{m_2}^* z_{m_1} \cdots z_{m_{2p-1}}^* z_{m_{2p}}$, we can generate $Q(z_{m_1}^* z_{m_2}) z_{m_3}^* z_{m_4} \cdots z_{m_{2p-1}}^* z_{m_{2p}}$. Continuing such a process, we can use polynomials in the form of $Q(z_{m_1}^* z_{m_2}) z_{m_3}^* z_{m_4} \cdots z_{m_{2p-1}}^* z_{m_{2p}}$ to generate elements in the form of $Q(z_{m_1}^* z_{m_2}) Q(z_{m_3}^* z_{m_4}) \cdots z_{m_{2p-1}}^* z_{m_{2p}}$. Continuing such a process, we can finally generate $Q(z_{m_1}^* z_{m_2}) \cdots Q(z_{m_{2p-1}}^* z_{m_{2p}})$. On the other hand, reversing such a process, we can generate $z_{m_1}^* z_{m_2} \cdots z_{m_{2p-1}}^* z_{m_{2p}}$ from $Q(z_{m_1}^* z_{m_2}) \cdots Q(z_{m_{2p-1}}^* z_{m_{2p}})$. Therefore, we have shown that $\mathrm{span}(E) = \mathrm{span}(F)$ over $\mathbb{C}$, inducing $\mathrm{rank}_{\mathbb{C}}(E) = \mathrm{rank}_{\mathbb{C}}(F)$.

Next we evaluate the rank of F over $\mathbb{C}$. Since the $2N$ variables z_j and z_j^* are linearly independent, all elements in F, as in the product form of $z_{m_1}^* z_{m_2} \cdots z_{m_{2p-1}}^* z_{m_{2p}}$, are hence independent as well. In order to obtain an element in F, we choose number p of z_j's from the indices $j \in \{1, \ldots, N\}$ and choose a number p of z_j^*'s from the remaining $N - p$ number of indices. Then the number of elements in F is $\binom{N}{p}\binom{N-p}{p}$, which equals $\mathrm{rank}_{\mathbb{C}}(F) = \mathrm{rank}_{\mathbb{C}}(E) = \mathrm{rank}_{\mathbb{R}}(E)$. Thus, we have proved $\mathrm{rank}_{\mathbb{R}}(E) = \binom{N}{p}\binom{N-p}{p}$. Therefore, $\mathcal{L}$ is the Lie algebra described in the text before Theorem 1.

[1] S. Sachdev, *Quantum Phase Transitions* (Cambridge University Press, Cambridge, 2011).

[2] L. Balents, Nature (London) **464**, 199 (2010).

[3] K. Binder and A. P. Young, Rev. Mod. Phys. **58**, 801 (1986).

[4] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[5] J. Simon, W. S. Bakr, R. Ma, M. E. Tai, P. M. Preiss, and M. Greiner, Nature (London) **472**, 307 (2011).

[6] D. D'Alessandro, *Introduction to Quantum Control and Dynamics* (Chapman & Hall/CRC, Boca Raton, 2008).

[7] D. Burgarth, S. Bose, C. Bruder, and V. Giovannetti, Phys. Rev. A **79**, 060305 (2009).

[8] R. Zeier and T. Schulte-Herbrüggen, J. Math. Phys. **52**, 113510 (2011).

[9] T. Polack, H. Suchowski, and D. J. Tannor, Phys. Rev. A **79**, 053403 (2009).

[10] X. Wang, P. Pemberton-Ross, and S. G. Schirmer, IEEE Trans. Automat. Control **57**, 1945 (2012).

[11] X. Wang, A. Bayat, S. G. Schirmer, and S. Bose, Phys. Rev. A **81**, 032312 (2010).

[12] D. D'Alessandro, IEEE Trans. Automat. Control **55**, 1416 (2010).

[13] F. Silva-Leite and P. E. Crouch, Math. Control Signal. Syst. **1**, 31 (1988).

[14] C. Altafini, J. Math. Phys. **43**, 2051 (2002).

[15] V. Jurdjević and I. Kupka, Ann. Inst. Fourier **31**, 151 (1981).

[16] V. Jurdjević, *Geometric Control Theory* (Cambridge University Press, Cambridge, 1997).

[17] F. Albertini and D. D'Alessandro, Linear Algebra Appl. **350**, 213 (2002).

[18] G. Turinici and H. Rabitz, J. Phys. A: Math. Gen. **36**, 2565 (2003).

[19] D. Burgarth, K. Maruyama, M. Murphy, S. Montangero, T. Calarco, F. Nori, and M. B. Plenio, Phys. Rev. A **81**, 040303 (2010).