qitd451

Graph States and Graph Codes

Robert B. Griffiths
Version of 6 April 2010

Contents

References:

M. Hein et al. "Entanglement in graph states and its applications," arXiv:quant-ph/0602096.

S. Y. Looi et al. "Quantum error correcting codes using qudit graph states," Phys. Rev. A 78 (2008) 042303. arXiv:0712.1979 [quant-ph]

1 Introduction

★ The introduction of *graph states* (originally called "cluster states") by Raussendorf and Briegel in 2001 had a major impact on quantum information and quantum computing in various ways. In particular, these states are the basis of *measurement-based* (or "one-way") quantum computing, and they provide a relatively simple way of constructing many of the *quantum codes* useful for quantum error correction.

2 Graph States and Graph Basis

★ Consider a system of n qubits labeled 1, 2, ... Define the trivial graph state to be

$$|G^0\rangle = |+\rangle \otimes |+\rangle \otimes \cdots |+\rangle = |+\rangle^{\otimes n}, \tag{1}$$

where

$$|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, \quad |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2} \tag{2}$$

are the orthonormal basis states for a single qubit that are eigenstates of the Pauli X operator.

★ We use X_j, Z_j and $Z_jX_j = -Z_jX_y = -iY_j$ to denote the Pauli operators on qubit j; along with I_j they form a basis of the operator space on a single qubit. Products of operators of this sort, called "Pauli products," span the space of operators on n qubits.

• If Q is an operator on n qubits, its *base*, also called its *support*, is the set of qubits on which it acts in a nontrivial fashion. The *size* $\sigma(Q)$ of Q is the number of qubits in its base. For example,

$$X_1Z_2X_2Z_4 = X_1 \otimes Z_2X_2 \otimes I_3 \otimes Z_4 \otimes I_5 \otimes \cdots I_n \tag{3}$$

has a base $\{1, 2, 4\}$, so its size is 3.

★ Let G be a graph with a collection V of n vertices and a collection E of edges. We are only interested in graphs in which at most one edge, denoted by (j, k), connects vertices j and k, and there are no loops, i.e., no edges of the form (j, j). The corresponding *graph state* $|G\rangle$ is defined as

$$|G\rangle = \mathcal{U}|G^0\rangle, \text{ where } \mathcal{U} := \prod_{(j,k)\in E} C_{jk} \tag{4}$$

is the unitary *entangling* operator, a product of controlled-phase (CP) gates, one for each edge of the graph.

• The controlled-phase (CP) operator $C_{jk} = C_{kj}$ for the pair of qubits $j \neq k$ is defined by

$$C_{jk}\Big(|m\rangle_j \otimes |n\rangle_k\Big) = (-1)^{mn}|m\rangle_j \otimes |n\rangle_k, \tag{5}$$

where m and n are the 0 and 1 labels in the standard basis. One can also write

$$C_{jk} = \tfrac{1}{2}[I + Z_j + Z_k - Z_jZ_k]. \tag{6}$$

□ Exercise. Prove the equivalence of these two definitions.

◦ In particular if $n = 2$ and G is the graph with one edge joining vertices 1 and 2,

$$|G\rangle = C_{12}|{+}{+}\rangle = \tfrac{1}{2}C_{12}\Big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\Big) = \tfrac{1}{2}\Big(|00\rangle + |01\rangle + |10\rangle - |11\rangle\Big) \tag{7}$$

★ The *graph basis* associated with the graph state $|G\rangle$ is the collection of orthonormal states of the form

$$|a\rangle = Z^a|G\rangle = \Big(\prod_j Z_j^{a_j}\Big)|G\rangle \tag{8}$$

where a stands for an n-tuple $(a_0, a_1, \ldots a_n)$, with each a_j equal to 0 or 1. Thus a can take on 2^n values, and the 2^n states $|a\rangle$ form an orthonormal basis of the Hilbert space. The graph state $|G\rangle$ itself corresponds to $a_0 = a_1 = \cdots a_n = 0$.

• To prove that the $|a\rangle$ form an orthonormal basis, observe that in light of (6) the Z_l commute with all the C_{jk}, which also commute with each other. Consequently we can rewrite (8) as

$$|a\rangle = \mathcal{U}\Big(\prod_j Z_j^{a_j}\Big)|G^0\rangle. \tag{9}$$

Now since $Z|{+}\rangle = |{-}\rangle$, it follows that the collection of states of the form $Z^a|G^0\rangle$ for different a is simply the orthonormal basis consisting of the 2^n states in which each qubit is either $|{+}\rangle$ or $|{-}\rangle$. As $\mathcal{U}$ is a unitary operator, it maps one orthonormal basis to another orthonormal basis.

★ Figure 1 shows a simple example of a graph state constructed by a circuit in which each CP gates is indicated by a vertical line joining two × marks. This notation exhibits the symmetry of the gate, though it would be equally correct to make it a controlled-Z or CZ gate with one of the qubits (it does not matter which one) serving as the control and the other as the target. The time ordering of the different CP gates does not matter, since they commute with each other.

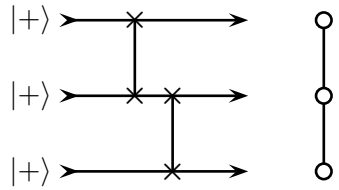

Figure 1: Circuit that produces the graph state corresponding to the graph on the right side.

3 Some Properties of Graph States

★ If $b = b_1 b_2 \dots b_n$ is the binary representation of an integer lying between 0 and $2^n - 1$ one can write

$$2^{n/2}|G^0\rangle = |00\cdots0\rangle + |00\cdots1\rangle + \cdots + |11\cdots1\rangle = \sum_{b=0}^{2^n-1} |b\rangle. \tag{10}$$

The action of each C_{jk} gate is to change some of the + signs in this sum to − signs. The same is true of any Z_l and thus of Z^a. Consequently, any graph basis state has the form

$$2^{n/2} Z^a |G\rangle = \sum_{b=0}^{2^n-1} (-1)^{\nu(b)} |b\rangle, \tag{11}$$

where $\nu(b) = 0$ or 1, and depends both on the graph G and on the n-tuple a.

□ Exercise. Let $\Gamma_{jk} = \Gamma_{kj}$ be the adjacency matrix of the graph: 1 if an edge connects vertices j and k and 0 otherwise. Show that

$$\nu(b) = \tfrac{1}{2} \sum_{jk} b_j \Gamma_{jk} b_k + \sum_j a_j b_j. \tag{12}$$

★ The following XZ *rule* for graph states is extremely useful. Let X_j be the Pauli X operator on qubit j. Then

$$X_j |G\rangle = \Big(\prod_{k \in N_j} Z_k \Big) |G\rangle, \tag{13}$$

where N_j is the set of *neighbors* of j in the graph G: i.e., vertices which are directly connected to j by a single edge. The XZ rule says that the action of any X_j on a graph state or a graph basis state is another graph basis state. See Fig. 2 for a simple example.

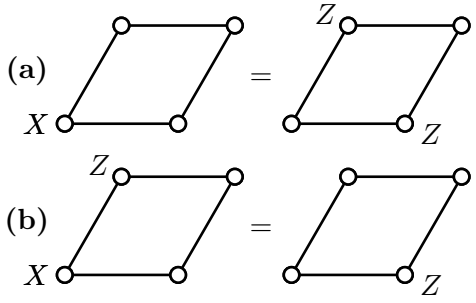

Figure 2: Examples of the XZ rule. In (a) applying X to the lower left vertex produces a Z on the two neighbors. In (b) one of these Z operators cancels one already present.

• There is one point that is slightly tricky. If one applies an X at a vertex where a Z is already present, one needs to first reverse the order, so X_jZ_j becomes $-Z_jX_j$, and then use the XZ rule as it would apply to a "bare" vertex. The anticommutation of X and Z produces a $-$ sign which one may need to keep track of.

□ Exercise. Prove the XZ rule. [Hint: Show that for $j \neq k$, $X_jC_{jk} = C_{jk}Z_kX_j$. What does X_j do to $|G^0\rangle$?]

4 Quantum Codes

4.1 Classical codes

★ A classical n-bit code used for correcting errors is constructed as follows. From the set of all 2^n n-bit strings choose a subset c_0, c_1, $\ldots c_{K-1}$ of *code words*. For example, if $n = 3$ and $K = 2$ the code words might be $c_0 = 000$ and $c_1 = 111$. The *Hamming distance* (or simply *distance*) $\delta(c_j, c_k)$ between two code words c_j and c_k is the minimum number of bit flips required to get from one to the other. Thus $\delta(c_0, c_1) = 3$ for our example. The distance δ for the code itself is the minimum of $\delta(c_j, c_k)$ over all distinct pairs of code words.

□ Exercise. Show that if the $n = 4$ code consists of all 4-bit strings with an even number of 1's (including 0000), the distance is $\delta = 2$.

◦ In the literature the distance is commonly denoted by d; our reason for using δ is that in quantum information theory d often refers to the dimension of some Hilbert space.

• We use the notation (n, K, δ) for an n-bit code with K codewords and distance δ, or $[n, k, \delta]$ when $K = 2^k$ is a power of 2.

★ It is not difficult to establish the following: for an n-bit classical code:

(i) A code with distance $\delta \geq 2m + 1$ can correct errors on any m bits; i.e, if at most m bits have been corrupted there is a decoding operation which will unambiguously restore the original code word.

(ii) Given that an error has occurred on some *known* subset of m bits, then unambiguous error correction is possible if the code has distance $\delta \geq m + 1$.

□ Exercise. Convince yourself that these assertions are correct, or at least reasonable, starting with simple examples when $n = 2$ or $n = 3$.

4.2 Quantum codes

★ A *quantum code* on n qubits is defined to be a K-dimensional subspace of the 2^n-dimensional Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \mathcal{H}_n$ that is the tensor product of the Hilbert spaces of the n *carrier qubits*.

• Such a subspace is the span of a collection $\{|c_j\rangle\}$, $0 \leq j \leq K - 1$ of K orthonormal vectors. We shall refer to these as "code words," while noting that there is no unique choice for such an orthonormal set. In practice one generally has in mind a particular collection of quantum code words with certain convenient properties, but it is well to keep in mind that it is the space itself, rather than these basis states, which constitutes the code.

• Such a quantum code (or coding space) is denoted by $((n, K, \delta))$, or by $[[n, k, \delta]]$ when $K = 2^k$, in analogy with the notation for classical codes.

★ The distance δ of a quantum code on n qubits is defined in the following way. Recall that the Knill-Laflamme (KL) error correction condition is the requirement that

$$\langle c_q|Q|c_r\rangle = f(Q)\delta_{qr} \tag{14}$$

for certain combinations $Q = E_j^\dagger E_k$ of error operators, where $f(Q)$ is a (complex) number, possibly 0, that depends on the operator Q.

• It is sometimes convenient to view (14) as consisting of two distinct conditions, a "diagonal" condition when $q = r$, which states that $\langle c_q|Q|c_q\rangle$ is independent of q, and an "off diagonal" condition that $\langle c_q|Q|c_r\rangle = 0$ when $r \neq q$.

• By rewriting (14) as

$$PQP = f(Q)P, \tag{15}$$

where $P = \sum_q |c_q\rangle\langle c_q|$ is the projector on the coding space, one sees that the KL condition depends only on the coding space itself, and not on the choice of orthonormal basis for this space. Nevertheless, for the applications considered below (14) is more convenient than the equivalent (15).

★ We shall be interested in the case where the Q are Pauli products, see the discussion above in connection with (3). The distance δ of the quantum code is then *defined* to be the smallest integer such that the KL condition (14) is satisfied for all Q of size in the range $1 \leq \sigma(Q) < \delta$. In other words, (14) holds for any Q with $\sigma(Q) < \delta$, but there is at least one Q with $\sigma(Q) = \delta$ for which it fails. The correctness, or at least the reasonableness, of this definition will emerge from considering various examples.

★ Suppose we want a code to be able to correct any error on a *single* qubit, so the space $\mathcal{E}_c$ of correctable errors is spanned by

$$I, X_1, Z_1, X_1Z_1, X_2, Z_2, X_2Z_2, \ldots X_nZ_n. \tag{16}$$

The operators entering the error correction condition will be things like $E^\dagger \bar{E} = X_2(X_3Z_3)$, i.e., of size 2 or less. Consequently we need a code with $\delta \geq 3$ to be able to correct all errors of this type; conversely, the KL condition guarantees that for $\delta \geq 3$ any such error can be corrected.

• This argument extends in an obvious way to the case in which we wish to correct all errors involving m or fewer carrier qubits, and one sees that the necessary and sufficient condition is that $\delta \geq 2m + 1$, the same as in the case of a classical code.

★ Suppose, on the other hand, that we are sure that if an error has occurred, it has only affected qubit 2. Then the space of correctable errors will be spanned by I, X_2, Z_2, X_2Z_2, so the operators appearing in the KL condition will have size at most 1. In this case a code with $\delta = 2$ will suffice for correcting the error.

• More generally, given a code with $\delta \geq 2$ we can correct any *single* qubit error provided we know on *which* qubit it occurred. Of course to recover from this error we will (in general) have to make use of our knowledge of where the error occurred in carrying out the recovery operation. That sort of information is *not* needed to recover from a single qubit error for a code with $\delta \geq 3$.

• If we allow for arbitrary errors on a set of m qubits, but we know which set of carriers is involved, then recovery can be made provided our code has distance $\delta \geq m + 1$, and the recovery operation is designed for this specific set. The reason is that the error operators which must be inserted in the KL condition are all based on this set of m qubits, and products of the type $E^\dagger \bar{E}$ are also based on this set, so have a size that cannot exceed m. Once again the condition is the same as in the classical case.

5 Graph codes

5.1 Introduction

★ A *graph code* is defined to be one in which a graph G is given, and the coding space is spanned by a subset of graph basis states, see Sec. 2. These states are regarded as code words,

though as emphasized earlier what is significant from the point of view of quantum information is the subspace they span, not the code words themselves.

★ The analysis in Sec. 4 applies to all quantum codes. What is significant about graph codes is that, in contrast to the general case, it is relatively easy to calculate the distance δ directly from the properties of the graph G once the choice of code words has been specified. In addition, it turns out, for reasons that are not yet understood, that most of the "best" quantum codes discovered up to now are either graph codes or locally equivalent to graph codes. (Local equivalence means there is a unitary map that is a product of one-qubit unitaries, one for each carrier, which maps one coding space onto the other. Two locally equivalent codes can for many purposes be regarded as essentially the same code.)

• The basic ideas for finding the distance of a graph code will emerge as we study examples.

5.2 Trivial graph

★ The trivial graph with no edges yields the graph-code analog of a classical code, because the basis states $Z^a|G^0\rangle$ are product states in which some of the $|+\rangle$ states (analogs of the classical 0) have been replaced by $|-\rangle$ states (analogs of the classical 1).

• Any such code regarded as a quantum code will have a very short distance, in fact $\delta = 1$, even if the classical (Hamming) distance between the code words is large. To see this, suppose that c_j and c_k are classical words that differ in a particular bit, say the first bit, where c_j has the value 0, corresponding to a quantum $|+\rangle$, and c_k has a 1, corresponding to a quantum $|-\rangle$. Then the corresponding $|c_j\rangle$ and $|c_k\rangle$ are eigenfunctions of X_1 with eigenvalues $+1$ and -1. Consequently,

$$\langle c_j|X_1|c_j\rangle = +1 = -\langle c_k|X_1|c_k\rangle \tag{17}$$

in violation of the KL condition (14) which requires that diagonal elements be identical. Since (14) is already violated for $Q = X_1$ of size 1, this means the quantum δ is 1, its minimum possible value.

5.3 Case of $n = 2$ or $n = 3$ carriers

★ In the case $n = 2$ there is only one nontrivial graph, with a single edge joining two vertices. But this graph cannot be used to construct a quantum graph code with distance $\delta > 1$. Consider a code with code words

$$|c_0\rangle = |G\rangle, \quad |c_1\rangle = Z_1Z_2|G\rangle. \tag{18}$$

Initially this looks hopeful in that for $j = 1$ or 2,

$$\langle c_0|Z_j|c_0\rangle = \langle c_1|X_j|c_1\rangle = 0 = \langle c_0|Z_j|c_1\rangle = \langle c_0|X_j|c_1\rangle, \tag{19}$$

and thus we might hope to have achieved $\delta = 2$. But, alas, there is also a one-qubit operator Z_1X_1, and

$$\langle c_0|Z_1X_1|c_1\rangle = 1, \tag{20}$$

for this operator of size 1. So $\delta = 1$.

□ Exercise. Work out the results in (19) and (20), using the XZ rule, (13), to evaluate $X_j|G\rangle$.

★ For $n = 3$ the graph can be either connected or disconnected. The disconnected graphs are not very interesting for a reason indicated in the following exercise. There are two connected graphs that are topologically distinct: the line and the triangle. One can show by methods that go beyond the scope of these notes that the two graph states and their corresponding codes are locally equivalent. Thus one need only consider the linear graph, Fig. 1. The analysis of different

possibilities is left as an exercise, and the conclusion is that any code with at least two code words will have $\delta = 1$.

□ Exercise. Show that if the $n = 3$ graph is disconnected with two vertices joined by an edge and one isolated vertex, the distance cannot exceed $\delta = 1$. [Hint. If two codewords assign different powers of Z on the qubit corresponding to the isolated vertex the comments in Sec. 5.2 apply. If the codewords assign the same power of Z to the isolated vertex things reduce to the $n = 2$ case.]

□ Exercise. Show that for the linear graph any code with at least two code words has $\delta = 1$ by showing that all graph basis states can be obtained by applying 1 qubit operators (Z_1, X_1, Z_1X_1, Z_2,...) to $|G\rangle$. Why does this settle the matter?

5.4 Square graph

★ For $n = 4$ construct a graph in the form of a square with vertices numbered 1, 2, 3, 4 going clockwise around the square, Fig. 3, and let 4 code words be defined as in the figure. The resulting code has $\delta = 2$.

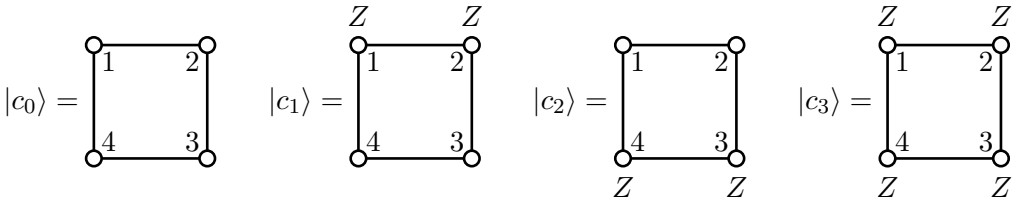

Figure 3: Square graph and code words

• The demonstration that (14), the KL condition, holds for all Q that act on only a single qubit can be made less tedious by the following observation. As noted just after (14), one can think of it as involving a diagonal condition for $q = r$ and an off-diagonal condition for $q \neq r$. In the present case it is easy to see by applying the operators X_1, Z_1, and Z_1X_1 to the first qubit, and then using symmetry, that $\langle c_0|Q|c_0\rangle = 0$ when Q is a Pauli of size 1. But then this is also the case if $|c_0\rangle$ is replaced by $|c_j\rangle$ for $j = 1$, 2, and 3, because

$$\langle c_j|Q|c_j\rangle = \langle c_0|\zeta Q\zeta|c_0\rangle, \tag{21}$$

where $\zeta = \zeta^\dagger$ is the product of a collection of Z_j operators. Since the Pauli operators on different qubits commute, and on the same qubit either commute or anticommute, $\zeta Q\zeta = \pm Q$. Thus since $\langle c_0|Q|c_0\rangle = 0$ the same must be true of $\langle c_j|Q|c_j\rangle$ when $\sigma(Q) = 1$.

• The remaining task is to check the off-diagonal condition in (14), but this is not difficult if one applies the XZ rule to cases in which Q involves (say) X_1, and uses the symmetry evident in Fig. 3.

5.5 Pentagon, hexagon, and heptagon

★ The smallest $\delta = 3$ quantum code employs $n = 5$ carriers and is realized for the pentagon graph G in Fig. 4, with code words $|c_0\rangle = |G\rangle$ and $|c_1\rangle = (\prod_{j=1}^5 Z_j)|G\rangle$.

• To check that $\delta = 3$ one needs to consider in (14) all Q which act on one or two qubits, i.e., $\sigma(Q) \leq 2$. Because of the high symmetry of the graph this is not very difficult with the help of the XZ rule. In particular, the diagonal condition can be checked by noting that $\langle c_0|Q|c_0\rangle = 0$ for the Q that are of interest, whence it will also be true for $\langle c_1|Q|c_1\rangle$; see remarks in Sec. 5.4. The off-diagonal condition is checked by showing that a one-qubit operator applied to any of the five

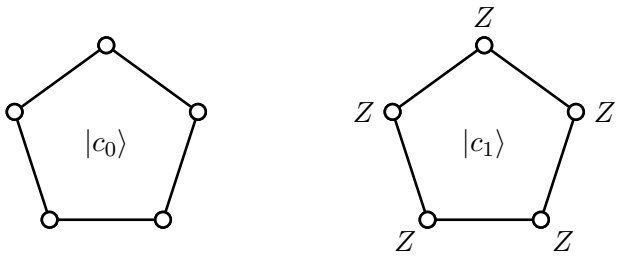

Figure 4: Pentagon graph code.

carriers, or a two-qubit operator applied to carriers adjacent on the pentagon, or to carriers which are next-nearest neighbors, always maps $|c_0\rangle$ into a graph basis state that is orthogonal to $|c_1\rangle$.

★ One can construct analogous codes for cyclic graphs with $n = 6$ and $n = 7$ vertices in which the pentagon is replaced with a hexagon or heptagon, and along with $|c_0\rangle = |G\rangle$ the second code word $|c_1\rangle$ is obtained by applying a Z to each of the carrier qubits. It turns out that this $n = 6$ code has distance $\delta = 2$, while the $n = 7$ code, like the pentagon code, has $\delta = 3$.

□ Exercise. Verify these distances.

• Of course the graphs just discussed are not the only possibilities for $n = 6$ or 7 vertices. The number of possible graphs increases very rapidly with n, and searching for codes becomes nontrivial if one wants to explore all possibilities for a given n.

5.6 Shor 9 qubit code

★ One can realize Shor's 9 qubit code, or at least one that is locally equivalent to it, by employing the graph shown in Fig. 5, with code words $|c_0\rangle = |G\rangle$ and $|c_1\rangle = Z_1Z_2Z_3|G\rangle$.

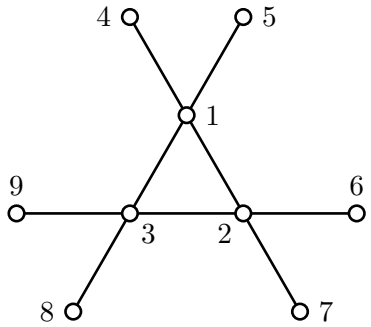

Figure 5: Nine qubit graph that yields a code locally equivalent to the Shor code.

□ Exercise. Show that this code has distance $\delta = 3$, but if one of the "exterior" vertices is removed, say 4, the resulting $n = 8$ code with the same two code words has distance $\delta = 2$.