A Characterization of Entanglement-Assisted Quantum Low-Density Parity-Check Codes

Yuichiro Fujiwara, *Member, IEEE*, and Vladimir D. Tonchev

Abstract—As in classical coding theory, quantum analogs of low-density parity-check (LDPC) codes have offered good error correction performance and low decoding complexity by employing the Calderbank–Shor–Steane construction. However, special requirements in the quantum setting severely limit the structures such quantum codes can have. While the entanglement-assisted stabilizer formalism overcomes this limitation by exploiting maximally entangled states (ebits), excessive reliance on ebits is a substantial obstacle to implementation. This paper gives necessary and sufficient conditions for the existence of quantum LDPC codes which are obtainable from pairs of identical LDPC codes and consume only one ebit, and studies the spectrum of attainable code parameters.

Index Terms—Entanglement-assisted quantum error correction, low-density parity-check (LDPC) code, pairwise balanced design, stabilizer code, Steiner 2-design.

I. INTRODUCTION

THIS paper addresses the question of how much one pair of qubits in a maximally entangled state can be exploited to import classical sparse graph codes by the entanglement-assisted stabilizer formalism proposed by Brun *et al.* [4]. We will show how quantum error-correcting codes with particular desirable properties under this framework are equivalent to some fundamental objects from combinatorial design theory, known as pairwise balanced designs [3]. While earlier relevant results in the literature give sufficient conditions for the existence of entanglement-assisted quantum codes based on classical sparse graph codes (see [10], [17], and references therein), results presented here give necessary and sufficient conditions under the conventional standard assumptions, and mathematically describe the structure of such quantum codes consuming only one ebit.

Low-density parity-check (LDPC) codes are among the best known classical codes in terms of error correction performance and decoding complexity [25]. Extensive efforts have been

Y. Fujiwara is with the Division of Physics, Mathematics and Astronomy, California Institute of Technology, Pasadena, CA 91125 USA (e-mail: yuichiro.fujiwara@caltech.edu).

V. D. Tonchev is with the Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931 USA (e-mail: tonchev@mtu.edu).

made to generalize this class of error-correcting schemes in classical coding theory to the quantum setting. Among others, codes obtained by applying the well-known Calderbank–Shor–Steane (CSS) construction [5], [27] to pairs of carefully chosen identical LDPC codes have shown remarkable error correcting performance in simulations (see, for example, [1], [8], [15], and [22] for recently proposed combinatorial quantum LDPC codes).

However, the progress on the quantum analogs of LDPC codes has lagged behind their classical counterparts because of special requirements imposed on the code structure in the quantum setting; only a limited class of classical codes can be exploited in a direct manner.

The development of the entanglement-assisted stabilizer formalism is a recent breakthrough in this regard [4], [16]. This framework allows us to import any binary or quaternary linear codes to the quantum setting by exploiting maximally entangled states. In other words, by taking advantage of ebits, the code designer can turn good classical linear codes into quantum error-correcting codes and expect similar good performance in the quantum setting. In fact, Hsieh *et al.* [15] demonstrated this advantage by constructing entanglement-assisted quantum LDPC codes which have notable error correction performance.

However, the entanglement-assisted stabilizer formalism is not a silver bullet; an adequate supply of ebits may not be available. The number of ebits required to import a given pair of classical LDPC codes varies greatly from pair to pair. In fact, as stated by Hsieh *et al.* [17], until recently it was conjectured that the entanglement-assisted stabilizer formalism required an impractically large number of ebits to make use of classical codes with good error correction performance.

Fortunately, Fujiwara *et al.* [10] and Hsieh *et al.* [17] independently disproved this conjecture by giving examples of codes which require only one ebit, while outperforming the previously known quantum LDPC codes in simulations. Given the positive results on quantum error-correcting codes requiring a tiny amount of entanglement and the fact that excessive reliance on ebits is a substantial obstacle to implementation, it is of interest to investigate the characteristics of quantum codes consuming only one ebit.

In this paper, we investigate what kind of quantum LDPC code is obtainable if only one ebit is allowed to import pairs of identical classical LDPC codes. We show the equivalence between such quantum LDPC codes and special classes of combinatorial objects, namely Steiner 2-designs and pairwise balanced designs of index one. (For a thorough introduction to combinatorial design theory, we refer the interested reader to [3] and [7].) This equivalence provides theoretical insight into the properties and attainable code parameters and explains why all

known high-performance quantum LDPC codes requiring only one ebit were derived from combinatorial designs of this kind.

It should be noted that it is also possible to utilize a pair of nonidentical classical error-correcting codes to construct a quantum LDPC code as long as they are of the same length. In fact, very recently quantum LDPC codes with good error correction performance have been found through a clever use of nonidentical ingredients [13], [20]. However, their methods require a large number of physical qubits to encode, which is at odds with the focus of this paper, that is, shedding light on more easily implementable quantum LDPC codes. For this reason, we leave the equally interesting case of nonidentical ingredients consuming only a small amount of entanglement to future work.

In the following sections, we will show how the requirement of consuming only one ebit dictates the structure of the exploitable pairs of identical classical LDPC codes. In Section II, we briefly review the entanglement-assisted quantum LDPC codes and related facts from combinatorial design theory and then prove the equivalence between pairwise balanced designs of index one and entanglement-assisted quantum LDPC codes consuming one ebit. Section III provides bounds for the code parameters. Section IV discusses some open questions and directions for future work.

II. ENTANGLEMENT-ASSISTED QUANTUM LDPC CODES

In this section, we study the existence of entanglement-assisted quantum LDPC codes consuming one ebit and its relation to combinatorial designs. For a concise introduction to the entanglement-assisted stabilizer formalism, we refer the reader to Hsieh *et al.* [17]. An $[[n, k; c]]$ *entanglement-assisted quantum error-correcting code* (EAQECC) encodes k logical qubits into n physical qubits with the help of c copies of maximally entangled states. The parameters n and k are the *length* and *dimension* of the EAQECC, respectively. An $[[n, k; c]]$ EAQECC requires c *ebits*.

A classical LDPC code is a binary linear code which admits a parity-check matrix with a small number of nonzero entries. The *quantum check matrix* of an EAQECC of length n constructed by the CSS construction with a pair of LDPC codes has the form

$$\begin{bmatrix} H_1 & 0 \\ 0 & H_2 \end{bmatrix}$$

where H_1 and H_2 are the parity-check matrices of classical LDPC codes of length n, and 0 represents a zero matrix. The EAQECC is called *homogeneous* if H_1 is obtained by permuting rows of H_2. In this case, because permuting rows does not affect the code parameters, without loss of generality, we assume $H_1 = H_2$ and omit the subscripts. As far as the authors are aware, at the time of writing, all entanglement-assisted quantum LDPC codes proposed in the literature for the depolarizing channel are homogeneous.

The required amount of entanglement can be calculated from the rank of $H_1 H_2^T$ over the field of order 2, that is, its 2-rank (see [29] for the proof and [28] for an alternative, equivalent formula). Since we do not use ranks over another field, we always assume that ranks are computed over $\mathbb{F}_2$. If the parity-check

matrix H defines an $[n, k, d]$ linear code C, then the resulting homogeneous code requires $c = \text{rank}(HH^T)$ ebits and is of length n and dimension $2k - n + c$ [16]. The case when $c = 0$ gives the well-known *stabilizer code* of *minimum distance* d', where $d' \geq d$ is the minimum Hamming weight of a codeword in $C \setminus C^\perp$ (see [24] for a more detailed treatment of this special case). Similarly, the minimum distance for the case $c > 0$ is the minimum Hamming weight of a codeword in $C \setminus \mathcal{R}(C^\perp)$, where $\mathcal{R}(C^\perp)$ is the normal subgroup $C \cap C^\perp$. A particularly useful fact to quantum LDPC codes is that regardless of the value c, the standard syndrome decoding can correct up to $\lfloor \frac{d-1}{2} \rfloor$ phase flips and up to $\lfloor \frac{d-1}{2} \rfloor$ bit flips through two separate steps, where each decoding step utilizes H to compute the error syndrome for one of the two kinds of error [15]. In other words, we can take advantage of the "classical minimum distance" of ingredients in a straightforward manner as we would in the classical setting during decoding. In what follows, when the distance of a quantum error-correcting code is discussed, we generally focus on this type of straightforwardly exploitable classical minimum distance of a quantum LDPC code.

The *Tanner graph* of an $m \times n$ parity-check matrix H is the bipartite graph consisting of n bit vertices and m parity-check vertices, where an edge joins a bit vertex to a parity-check vertex if that bit is included in the corresponding parity-check equation. A *cycle* in a graph is a sequence of connected vertices which starts and ends at the same vertex in the graph and contains no other vertices more than once. The *girth* of a parity-check matrix is the length of a shortest cycle in the corresponding Tanner graph. Since the Tanner graph is bipartite, its girth is even. Clearly, a 4-cycle in a parity-check matrix is a 2×2 all-one submatrix. A 6-cycle is a 3×3 submatrix in which each row and column has exactly two ones. Typically, 4-cycles severely reduce error correction performance while 6-cycles have a mild negative effect. Since we are interested in codes with excellent performance, we only consider codes with girth at least six. To avoid triviality, we also assume that the row and column weights of a parity-check matrix are at least two. An LDPC code is *regular* if its parity-check matrix has constant row and column weights, and *irregular* otherwise.

We begin with a simple observation about the structure of a classical LDPC code without short cycles which form a homogenous quantum LDPC code requiring only one ebit.

Theorem 2.1: There exists a homogeneous quantum LDPC code which requires only one ebit and has girth greater than four if and only if the following conditions on the parity-check matrix of the corresponding classical LDPC code hold.

1) For each pair of distinct parity-checks r_i, r_j, there exists exactly one bit involved in both r_i and r_j.
2) The size of each parity-check is odd and greater than one.
3) Each bit is involved in more than one parity-check.

Proof: First we prove sufficiency. Let H be a parity-check matrix of a classical LDPC code which satisfies the three conditions in the statement. Since the sizes of parity-checks are odd, the entries on the diagonal of HH^T representing the inner products of the same rows are ones. Because for each pair of parity-checks there exists exactly one bit involved in the pair, the other entries of HH^T are also ones. Hence, HH^T is the all-one square matrix. Thus, we have $\text{rank}(HH^T) = 1$. Since

no pair of rows of H produces a 4-cycle, the girth of the corresponding classical LDPC code is greater than four.

Next we prove necessity. Let H' be a parity-check matrix of a classical binary linear code which yields a homogeneous quantum LDPC code of girth greater than four requiring only one ebit. Let $H'H'^T = (h'_{i,j})$ and write the ith row and jth column of $H'H'^T$ as r_i and c_j, respectively. Since $H'H'^T$ is not a zero matrix, there exists a nonzero entry $h'_{a,b}$. Let $I = \{i : h'_{i,b} = 1\}$. Because $H'H'^T$ is symmetric with respect to the diagonal representing the inner products of the same rows corresponding to parity-checks, we have $h'_{b,i} = 1$ for $i \in I$. Since rank $(H'H'^T) = 1$, the rows r_i and columns c_i, $i \in I$, induce the $|I| \times |I|$ all-one matrix in $H'H'^T$. Since H' has no 4-cycles, the all-one matrix corresponds to a set R of rows in H', where for any $r \in R$, the weight of r is odd and each pair of distinct rows in R has exactly one position in which both entries are ones. Hence, if $H' = R$, then H' satisfies all the three conditions in the statement. Suppose the contrary that H' has a row $r' \notin R$. Then, r' does not have a one in a position where $r \in R$ does. By assumption, every column of H' has at least two ones, and hence, there is another row r'' which is not in R and has a one in one of the positions in which r' has a one. Since rank $(H'H'^T) = 1$ and R generates all-one submatrix of $H'H'^T$, r' and r'' are orthogonal. Hence, the pair of rows induces a 4-cycle, a contradiction. This completes the proof. ∎

Combinatorial objects that are equivalent to the classical LDPC codes satisfying the conditions in Theorem 2.1 have been studied since the late 19th century in combinatorial design theory. Let K be a subset of positive integers. A *pairwise balanced design* of *order* v and *index* one with *block sizes* from K, denoted by $\mathrm{PBD}(v, K, 1)$, is an ordered pair $(V, \mathcal{B})$, where V is a finite set of v elements called *points*, and $\mathcal{B}$ is a family of subsets of V, called *blocks*, that satisfies the following two conditions:

  (i) each unordered pair of distinct elements of V is contained in exactly one block of $\mathcal{B}$,
  (ii) for every $B \in \mathcal{B}$ the cardinality $|B| \in K$.

When K is a singleton $\{\mu\}$, the PBD is a *Steiner* 2-*design* of *order* v and *block size* μ, denoted by $S(2, \mu, v)$. A PBD of order v is *trivial* if it has no blocks or consists of only one block of size v. When the cardinality of V is positive, a trivial PBD with no blocks means that V is a singleton.

Define $\alpha(K) = \gcd\{\mu - 1 : \mu \in K\}$ and $\beta(K) = \gcd\{\mu(\mu - 1) : \mu \in K\}$. Necessary conditions for the existence of a $\mathrm{PBD}(v, K, 1)$ are $v - 1 \equiv 0 \pmod{\alpha(K)}$ and $v(v - 1) \equiv 0 \pmod{\beta(K)}$. By a constructive proof, these conditions were shown to be asymptotically sufficient.

Theorem 2.2 (see [30]): There exists a constant v_K such that for every $v > v_K$ satisfying $v - 1 \equiv 0 \pmod{\alpha(K)}$ and $v(v-1) \equiv 0 \pmod{\beta(K)}$, there exists a $\mathrm{PBD}(v, K, 1)$. The *replication number* r_x of a point $x \in V$ of a PBD $(V, \mathcal{B})$ is the number of occurrences of x in the blocks of $\mathcal{B}$. A PBD is *odd-replicate* if for every $x \in V$, the replication number r_x is odd. If $r_x = r_y$ for any two points x and y, we say that the PBD is *equireplicate* (or *regular*) and has replication number r_x. While our result will show that regular PBDs give rise to LDPC codes that are right-regular in the language of coding theory, to avoid any confusion, we use the term equireplicate for

combinatorial designs. Every $S(2, \mu, v)$ is equireplicate and has replication number $\frac{v-1}{\mu-1}$. An *incidence matrix* of a PBD $(V, \mathcal{B})$ is a binary $v \times b$ matrix $H = (h_{i,j})$ with rows indexed by points, columns indexed by blocks, and $h_{i,j} = 1$ if the ith point is contained in the jth block, and $h_{i,j} = 0$ otherwise.

Theorem 2.3: There exists a homogeneous quantum LDPC code which requires only one ebit and has girth greater than four if and only if the corresponding parity-check matrix of the classical LDPC code is an incidence matrix of a nontrivial odd-replicate PBD with index one and smallest block size greater than one.

Proof: Let H be an incidence matrix of a nontrivial odd-replicate PBD with index one and smallest block size greater than one. It suffices to show that H is equivalent to a parity-check matrix satisfying the conditions on the classical LDPC code in Theorem 2.1. Because every pair of points appear exactly once in a block, for every pair of rows, there exists exactly one column where both rows have one. The number of appearances of a point is the weight of the corresponding row in H, which is odd and not equal to one. Because each block contains more than one point, the weight of each column is larger than one. By indexing rows of H by parity-checks and columns by bits, H can be regarded as a parity-check matrix satisfying the conditions as required. It is trivial that the converse also holds. ∎

Note that if we allow a column of weight one, without loss of generality, the parity-check matrix H of a classical LDPC code must be either an incidence matrix of an odd-replicate PBD with index one or of the form

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$$

where A is an incidence matrix of an odd-replicate PBD with index one and smallest block size greater than one, and B is of constant column weight one and satisfies $BB^T = 0$. Hence, in the latter case, H defines a classical code which is either of minimum distance two or consists of codewords with zeros added to each codeword defined by the PBD. Hence, we only consider the case when each row and column has at least two ones.

The necessary and sufficient condition given in Theorem 2.3 allows us to prove that homogeneous quantum LDPC codes requiring only one ebit must have girth less than or equal to six.

Theorem 2.4: There exists no homogeneous quantum LDPC code with girth greater than six which requires only one ebit.

Proof: Suppose the contrary that there exists a parity-check matrix H of a binary linear code which yields a homogeneous quantum LDPC code with girth greater than six requiring only one ebit. By Theorem 2.3, the parity-check matrix H is an incidence matrix of a PBD of index one. Take an arbitrary column c_1 of H. Write the block B_1 which corresponds to c_1 as $\{v_1, \ldots, v_{|B_1|}\}$. Since every row has at least two ones, we can find another column c_2 which corresponds to $B_2 = \{v_1, v_{|B_1|+1}, \ldots, v_{|B_1|+|B_2|-1}\}$, where $v_i \neq v_j$ for any i and j, $i \neq j$. Take the third column c_3 representing the block B_3 which contains the pair $\{v_2, v_{|B_1|+1}\}$. The three columns c_1, c_2, and c_3 induce a 6-cycle, a contradiction. ∎

Thus, a homogeneous quantum LDPC code requiring only one ebit has girth six, which is the largest possible, if and only if the code is obtained from an odd-replicate PBD of index one.

An important case is when the classical ingredient is a regular LDPC code. In this case, a simple necessary condition is asymptotically sufficient.

Theorem 2.5: A necessary condition for the existence of a regular homogeneous quantum LDPC code which requires only one ebit and is of length n, girth six, and column weight μ is that the number $\frac{-1+\sqrt{1+4n\mu(\mu-1)}}{2(\mu-1)}$ is an odd integer. Conversely, for any integer $\mu \geq 2$, there exists a constant n_μ such that for $n > n_\mu$ the necessary condition is sufficient.

Proof: Let H be a parity-check matrix of a classical LDPC code. Assume that H yields a regular homogeneous quantum LDPC code which requires only one ebit and is of length n, girth six, and column weight μ. By Theorem 2.3, H forms an incidence matrix of a PBD of index one. Because H can also be seen as a parity-check matrix of a classical regular LDPC code, the column weights are uniform. Hence, H can be viewed as an incidence matrix of an $S(2, \mu, v)$ for some v. Because the number of blocks of an $S(2, \mu, v)$ is $\frac{v(v-1)}{\mu(\mu-1)}$, we have $n = \frac{v(v-1)}{\mu(\mu-1)}$. Hence

$$v = \frac{1 + \sqrt{1 + 4n\mu(\mu-1)}}{2}. \tag{1}$$

The number of occurrences of each point of an $S(2, \mu, v)$ is $\frac{v-1}{\mu-1}$. Since H defines an odd-replicate design, a necessary condition for the existence of a homogeneous quantum LDPC code satisfying the stated properties is that

$$\frac{v-1}{\mu-1} = \frac{-1 + \sqrt{1 + 4n\mu(\mu-1)}}{2(\mu-1)}$$

is odd. Assume that the necessary condition holds. Then, we have

$$\frac{1 + \sqrt{1 + 4n\mu(\mu-1)}}{2} - 1 \equiv 0 \pmod{\mu-1}$$

and

$$\frac{1 + \sqrt{1 + 4n\mu(\mu-1)}}{2}\left(\frac{1 + \sqrt{1 + 4n\mu(\mu-1)}}{2} - 1\right)$$
$$= n\mu(\mu-1)$$
$$\equiv 0 \pmod{\mu(\mu-1)}.$$

Applying Theorem 2.2 by plugging $\alpha(K) = \mu - 1$ and $\beta(K) = \mu(\mu-1)$ completes the proof. ∎

As we have seen in this section, there is a strong relation between homogeneous quantum LDPC codes and Steiner 2-designs. This equivalence implies that the framework given in [10] encompasses all regular homogeneous quantum LDPC codes with girth six which require only one ebit.

Particularly useful facts are that the original proof of Theorem 2.2 is constructive and that there are many known explicit constructions for PBDs with various properties. For more details on explicit combinatorial constructions useful to entanglement-assisted quantum LDPC codes, we refer the reader to [10] and references therein.

III. RATES, DISTANCES, AND NUMBERS OF 6-CYCLES

Next we examine the possible code parameters. As shown in the proof of Theorem 2.3, the number of blocks of a $\mathrm{PBD}(v, K, 1)$ corresponds to the code length. The number of rows of the parity-check matrix of the underlying classical LDPC code is the number v of points. The number of points in each block is the weight of the corresponding column in the parity-check matrix. Hence, K determines the possible column weights. Because the parity-check equations are labeled by the points of the PBD, the weight of each row is the replication number of the corresponding point. If the corresponding classical LDPC code is regular, its parity-check matrix forms an incidence matrix of an $S(2, \mu, v)$, which means that the code is of length $\frac{v(v-1)}{\mu(\mu-1)}$, constant column weight μ, and constant row weight $\frac{v-1}{\mu-1}$. The number of rows is v. In the reminder of this section, we investigate code parameters further in detail.

We first consider the rates for the case when classical ingredients are regular. The dimension of a homogeneous quantum LDPC code is determined by the rank of the corresponding parity-check matrix of the classical LDPC code. By Theorem 2.3, we only need to know the rank of the incidence matrix of the combinatorial design equivalent to the classical code. Hillebrandt [14] gave a bound on the rank of an incidence matrix of a Steiner 2-design.

Theorem 3.1 (see [14]): The rank of an incidence matrix H of an $S(2, \mu, v)$ satisfies the following inequalities:

$$\left\lceil \frac{1}{2} + \sqrt{\frac{1}{4} + \frac{(v-1)(v-\mu)}{\mu}} \right\rceil \leq \mathrm{rank}(H) \leq v.$$

Hence, we have the following bound on the dimension.

Theorem 3.2: If there exists a regular homogeneous quantum LDPC code with girth six and column weight μ whose parameters are $[[n, k; 1]]$, then

$$n - \sqrt{1 + 4n\mu(\mu-1)} \leq k$$

and

$$k \leq n - 2\left\lceil \frac{1}{2} + \sqrt{\frac{1}{4} + \frac{(v-1)(v-\mu)}{\mu}} \right\rceil + 1$$

where

$$v = \frac{1 + \sqrt{1 + 4n\mu(\mu-1)}}{2}.$$

Proof: As is stated in (1), a regular homogeneous quantum LDPC code with length n, girth six, and column weight μ which requires only one ebit must be constructed from an incidence matrix H of a Steiner 2-design of order $\frac{1+\sqrt{1+4n\mu(\mu-1)}}{2}$ and block size μ. Since the incidence matrix requires only one ebit, the dimension of the quantum LDPC code is $k = n - 2\,\mathrm{rank}(H) + 1$. Applying Theorem 3.1 to this relation between the dimension k and the rank of H completes the proof. ∎

If one wishes to obtain a code of highest possible rate for a given length and row and column weights, the incidence matrix of the corresponding Steiner 2-design must be of minimum rank.

A Steiner 2-design $S(2, 3, 2^m - 1)$ has odd replication number equal to $2^{m-1} - 1$. It is known that the rank of any $S(2, 3, 2^m - 1)$ is greater than or equal to $2^m - 1 - m$, and the minimum $2^m - 1 - m$ is achieved if and only if the design is isomorphic to the classical design whose points and blocks are the points and blocks of the binary projective geometry $\mathrm{PG}(m - 1, 2)$ [9].

An odd-replicate $S(2, 3, v)$ exists if and only if $v \equiv 3, 7 \pmod{12}$[3]. The ranks of such designs were determined by Assmus [2].

Theorem 3.3 (see [2]): For any $v \equiv 3, 7 \pmod{12}$, where $v = 2^t u - 1$ and u is odd, and any integer i with $1 \leq i < t$, there exists an $S(2, 3, v)$ of rank equal to $v - t + i$.

As a corollary, we have the following necessary and sufficient conditions.

Theorem 3.4: Let $n > 7$ be an integer. There exists a regular homogeneous quantum LDPC code of length n, dimension k, girth six, and column weight three which requires only one ebit if and only if

$$\sqrt{24n + 1} \equiv 5 \pmod{8}$$

and

$$n - \sqrt{24n + 1} \leq k \leq n - \sqrt{24n + 1} + 2t - 2$$

where t is the integer satisfying $\sqrt{24n + 1} = 2^{t+1}u - 3$ with u odd.

Proof: For every $v \equiv 1, 3 \pmod{6}$, $v > 7$, there exists an $S(2, 3, v)$ of full rank [9]. Theorem 3.3 provides all possible $S(2, 3, v)$s with deficient ranks. ∎

It is notable that Theorems 3.2 and 3.4 suggest that homogeneous quantum LDPC codes requiring only one ebit typically have very high rates. In fact, because the number of columns in an incidence matrix of a Steiner 2-design is the largest possible for a matrix with a given number of rows that avoids 4-cycles, the rate of the corresponding classical LDPC code is the highest possible in a sense.

At the same time, however, the extremely high rates imply that it is impossible to obtain an infinite family of LDPC codes of rate bounded away from one for some reasonable degree distribution. Because the number of blocks in a PBD of order v is $c \cdot v^2$ for some constant c, the code length is $c \cdot v^2$ with v being the number of rows of the corresponding parity-check matrix. Hence, the combinatorial design-theoretic construction described here is more suitable when the code designer wishes to deterministically design a code of moderate length with specific properties desirable for a particular purpose.

For instance, it is known that redundant rows in a parity-check matrix can help improve error correction performance of the sum–product algorithm [21]. One might then wish to design a parity-check matrix with a large number of redundant rows while completely avoiding 4-cycles. The minimum distance should not be too small either in a normal situation. Such a highly structured matrix H would be nearly impossible to obtain by a random draw when there is another stringent condition that $c = \mathrm{rank}\,(HH^T)$ must be kept small. However, these conditions can easily be translated into the language of combinatorial designs, and hence, one might be able to tell whether

such H exists and, if it does, how to explicitly construct it. In fact, the above constraints were effectively exploited to demonstrate that high-performance EAQECCs do not necessarily require a lot of ebits [17]. The minimum distance of a binary linear code whose parity-check matrix forms an incidence matrix of an $S(2, \mu, v)$ is at least $\mu + 1$.[1] While it appears to be difficult to obtain the exact upper bound on the minimum distance in general, incidence matrices of $S(2, \mu, v)$s can give minimum distances large enough for the standard sum–product algorithm at moderate length (see [10] and [17]). In fact, the Desarguesian projective plane of order 2^t gives an entanglement-assisted quantum LDPC code of length $4^t + 2^t + 1$ and dimension $4^t + 2^t - 2 \times 3^t$ with the corresponding parity-check matrix being of minimum distance $2^t + 2$, which performs very well over the depolarizing channel.

To further study the minimum distances of LDPC codes based on Steiner 2-designs, we define combinatorial design-theoretic notions. A *configuration* $\mathcal{C}$ in an $S(2, \mu, v)$, $(V, \mathcal{B})$, is a subset $\mathcal{C} \subseteq \mathcal{B}$. The set of points appearing in at least one block of a configuration $\mathcal{C}$ is denoted by $V(\mathcal{C})$. Two configurations $\mathcal{C}$ and $\mathcal{C}'$ are *isomorphic* if there exists a bijection $\phi : V(\mathcal{C}) \to V(\mathcal{C}')$ such that for each block $B \in \mathcal{C}$, the image $\phi(B)$ is a block in $\mathcal{C}'$. When $|\mathcal{C}| = i$, a configuration $\mathcal{C}$ is an *i-configuration* . A configuration $\mathcal{C}$ is *even* if for every point a appearing in $\mathcal{C}$, the number $|\{B : a \in B \in \mathcal{C}\}|$ of blocks containing a is even.

The notion of minimum distance can be translated into the language of combinatorial designs. An $S(2, \mu, v)$ is *r-even-free* if for every integer i satisfying $1 \leq i \leq r$ it contains no even i-configurations. Because the minimum distance of a binary linear code is the size of a smallest linearly dependent set of columns in its parity-check matrix, the minimum distance of a linear code based on a Steiner 2-design is determined by its even-freeness.

Proposition 3.5: The minimum distance of a binary linear code whose parity-check matrix forms an incidence matrix of a Steiner 2-design is d if and only if the corresponding Steiner 2-design is $(d - 1)$-even-free but not d-even-free.

A fairly tight bound on the minimum distance is available for the special case when the parity-check matrix has constant column weight three and gives a regular LDPC code.

By definition, every r-even-free $S(2, 3, v)$, $r \geq 2$, is also $(r - 1)$-even-free. Every $S(2, 3, v)$ is trivially 3-even-free. For $v > 3$ an $S(2, 3, v)$ may or may not be 4-even-free. Up to isomorphism, the only even 4-configuration is the *Pasch* configuration. It can be written by six points and four blocks: $\{\{a, b, c\}, \{a, d, e\}, \{f, b, d\}, \{f, c, e\}\}$. For the list of all the small configurations in an $S(2, 3, v)$ and more complete treatments, we refer the reader to [6] and [7]. Because every block in an $S(2, 3, v)$ has three points, no i-configuration for i odd is even. Hence, a 4-even-free $S(2, 3, v)$ is 5-even-free as well, which means that an $S(2, 3, v)$ is 5-even-free if and only if it contains no Pasch configuration.

---

[1]This can be easily seen by taking an arbitrary block B and counting how many blocks it requires to form a linearly dependent set of columns in the corresponding parity-check matrix. Because no pair of points appear in more than one block, each additional column can share a one at at most one row with the column corresponding to B. Hence, any linearly dependent set of columns in the parity-check matrix is of size at least $\mu + 1$.

The minimum distance d of a classical LDPC code is the smallest number of columns in its parity-check matrix H that add up to the zero vector over $\mathbb{F}_2^v$. If H forms an incidence matrix of an $S(2,3,v)$, then a set of d columns that add up to the zero vector is equivalent to an even d-configuration in the $S(2,3,v)$. Hence, as an immediate corollary of Theorem 2.3 and (1), we have the following proposition.

Proposition 3.6: A classical LDPC code of length n, minimum distance d, and constant column weight three forms a homogeneous quantum LDPC code of girth greater than four requiring only one ebit if and only if $\frac{-1+\sqrt{1+24n}}{4}$ is an odd integer and the parity-check matrix forms an incidence matrix of a $(d-1)$-even-free $S(2,3,\frac{1+\sqrt{1+24n}}{2})$ that is not d-even-free.

As far as the authors are aware, the sharpest known upper bound on the even-freeness of an $S(2,3,v)$ is the one found in the study of X-tolerant circuits:

Theorem 3.7 (see [11]): For $v > 3$, there exists no nontrivial 8-even-free $S(2,3,v)$.

Hence, by Proposition 3.6, Theorem 3.7, and the fact that every $S(2,3,v)$ is 3-even-free, we obtain a bound on the minimum distance of the classical ingredient.

Theorem 3.8: If there exists a regular homogeneous quantum LDPC code with girth six and column weight three requiring only one ebit, then the minimum distance d of the corresponding classical LDPC code satisfies $4 \le d \le 8$.

As is the case with $S(2,3,v)$s, in general, odd-replicate $(d-1)$-even-free $S(2,\mu,v)$s that are not d-even-free are equivalent to classical regular LDPC codes of constant column weight μ, girth six, and minimum distance d that generate homogeneous quantum LDPC codes requiring only one ebit. However, there do not seem to exist many results on the even-freeness of $S(2,\mu,v)$s or equivalently the minimum distances of the corresponding classical regular LDPC codes in the literature. To the best of the authors' knowledge, the following explicit construction gives the highest known even-freeness for $\mu \ge 3$:

Theorem 3.9 (see [23]): For any odd prime power q and positive integer $m \ge 2$, the points and lines of affine geometry $AG(m,q)$ form a $(2q-1)$-even-free $S(2,q,q^m)$.

When m is odd, the $S(2,q,q^m)$ is odd-replicate, and the size of each parity-check is $\frac{q^m}{2}$. Hence, we obtain quantum LDPC codes requiring only one ebit in this case. For a more detailed treatment of explicit constructions and the performance of quantum LDPC codes obtained from finite geometry, we refer the reader to [10] and [17].

When an LDPC code is decoded by the standard sum-product algorithm, 6-cycles may affect error correction performance of an LDPC code in a negative manner. It is known that the number N_6 of 6-cycles in a parity-check matrix from an incidence matrix of an $S(2,\mu,v)$ is exactly $\frac{v(v-1)(v-\mu)}{6}$ (see, for example, [19]). Hence, by (1), if we decode a regular homogeneous quantum regular LDPC code which requires only one ebit and is of length n, girth six, and column weight μ in two separate steps by using the same parity-check matrix for both X and Z errors, each step involves

$$N_6 = \frac{n\mu(\mu-1)(1-2\mu+\sqrt{1+4n\mu(\mu-1)})}{12}$$

6-cycles.

IV. CONCLUSION

We have shown that homogeneous quantum LDPC codes requiring only one ebit and avoiding 4-cycles are equivalent to special classes of fundamental combinatorial designs. Various properties of entanglement-assisted quantum LDPC codes have been revealed by applying known theorems and techniques of combinatorial design theory. Our results also give theoretical insight into the known entanglement-assisted quantum LDPC codes presented as counterexamples to the conjecture on the required amount of entanglement.

We have demonstrated that combinatorial design theory may work as a useful mathematical tool to investigate homogeneous quantum LDPC codes consuming one ebit. It will be interesting to study the case when two or more ebits are allowed and investigate how much information we can extract about the structure of such quantum LDPC codes.

Another important direction would be to investigate quantum LDPC codes obtained from pairs of distinct classical LDPC codes. As we have seen in Section III, if we only allow one ebit, the rate of a homogeneous quantum LDPC code of girth six approaches one as the length becomes larger. Hence, it would be quite interesting to investigate whether heterogeneous quantum LDPC codes can overcome this fundamental limitation while avoiding short cycles and suppressing the number of required ebits. Another possible merit of studying the heterogenous case from the viewpoint of combinatorics would be that combinatorial methods appear to be helpful to design highly structured quantum LDPC codes. One possible direction would be to study how to optimize codes for an asymmetrical quantum channel where the probabilities of bit flips and phase flips are not equal (see [12], [18], and [26]). We hope that these questions will be answered in future work.

REFERENCES

[1] S. A. Aly, "A class of quantum LDPC codes constructed from finite geometries," in *Proc. IEEE GLOBECOM*, 2008, pp. 1–5.

[2] E. F. Assmus, Jr, "On 2-ranks of Steiner triple systems," *Electron. J. Combin.*, vol. 2, p. R9, 1995.

[3] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*. Cambridge, U.K.: Cambridge Univ. Press, 1999.

[4] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, pp. 436–439, 2006.

[5] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, 1996.

[6] C. J. Colbourn and Y. Fujiwara, "Small stopping sets in Steiner triple systems," *Cryptogr. Commun.*, vol. 1, no. 1, pp. 31–46, 2009.

[7] C. J. Colbourn and A. Rosa, *Triple Systems*. Oxford, U.K.: Oxford Univ. Press, 1999.

[8] I. B. Djordjevic, "Quantum LDPC codes from balanced incomplete block designs," *IEEE Commun. Lett.*, vol. 12, no. 5, pp. 389–391, May 2008.

[9] J. Doyen, X. Hubaut, and M. Vandensavel, "Ranks of incidence matrices of Steiner triple systems," *Math. Z.*, vol. 163, pp. 251–259, 1978.

[10] Y. Fujiwara, D. Clark, P. Vandendriessche, M. D. Boeck, and V. D. Tonchev, "Entanglement-assisted quantum low-density parity-check codes," *Phys. Rev. A*, vol. 82, pp. 042338-1–042338-19, 2010.

[11] Y. Fujiwara and C. J. Colbourn, "A combinatorial approach to X-tolerant compaction circuits," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3196–3206, Jul. 2010.

[12] Y. Fujiwara and M.-H. Hsieh, "Adaptively correcting quantum errors with entanglement," in *Proc. IEEE Int. Symp. Inf. Theory*, Aug. 2011, pp. 279–283.

[13] M. Hagiwara, K. Kasai, H. Imai, and K. Sakaniwa, "Spatially coupled quasi-cyclic quantum LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory*, 2011, pp. 638–642.

[14] G. Hillebrandt, "The *p*-rank of $(0, 1)$—matrices," *J. Combin. Theory Ser. A*, vol. 60, pp. 131–139, 1992.

[15] M.-H. Hsieh, T. A. Brun, and I. Devetak, "Entanglement-assisted quantum quasicyclic low-density parity-check codes," *Phys. Rev. A*, vol. 79, pp. 032340-1–032340-7, 2009.

[16] M.-H. Hsieh, I. Devetak, and T. A. Brun, "General entanglement-assisted quantum error-correcting codes," *Phys. Rev. A*, vol. 76, pp. 062313-1–062313-7, 2007.

[17] M.-H. Hsieh, W.-T. Yen, and L.-Y. Hsu, "High performance entanglement-assisted quantum LDPC codes need little entanglement," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1761–1769, Mar. 2011.

[18] L. Ioffe and M. Mézard, "Asymmetric quantum error-correcting codes," *Phys. Rev. A*, vol. 75, pp. 032345-1–032345-4, 2007.

[19] S. J. Johnson and S. R. Weller, "Resolvable 2-designs for regular low-density parity-check codes," *IEEE Trans. Commun.*, vol. 51, no. 9, pp. 1413–1419, Sep. 2003.

[20] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, "Quantum error correction beyond the bounded distance decoding limit," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 1223–1230, Feb. 2012.

[21] D. J. C. MacKay, *Information Theory, Inference, and Learning Algorithms*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[22] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2315–2330, Oct. 2004.

[23] M. Müller and M. Jimbo, "Erasure-resilient codes from affine spaces," *Discrete Appl. Math.*, vol. 143, pp. 292–297, 2004.

[24] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. New York, NY, USA: Cambridge Univ. Press, 2000.

[25] T. J. Richardson and R. L. Urbanke, *Modern Coding Theory*. New York, NY, USA: Cambridge Univ. Press, 2008.

[26] P. K. Sarvepalli, A. Klappenecker, and M. Rotteler, "Asymmetric quantum codes: Constructions, bounds and performance," *Proc. R. Soc. A*, vol. 465, pp. 1645–1672, 2009.

[27] A. M. Steane, "Error-correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, pp. 793–797, 1996.

[28] M. M. Wilde, "Logical operators of quantum codes," *Phys. Rev. A*, vol. 79, pp. 062322-1–062322-5, 2009.

[29] M. M. Wilde and T. A. Brun, "Optimal entanglement formulas for entanglement-assisted quantum coding," *Phys. Rev. A*, vol. 77, pp. 064302-1–064302-4, 2008.

[30] R. M. Wilson, "An existence theory for pairwise balanced designs II: The structure of PBD-closed sets and the existence conjectures," *J. Combin. Theory Ser. A*, vol. 13, pp. 246–273, 1972.

Yuichiro Fujiwara (M'10) received the B.S. and M.S. degrees in mathematics from Keio University, Japan, and the Ph.D. degree in information science from Nagoya University, Japan.

He was a JSPS postdoctoral research fellow with the Graduate School of System and Information Engineering, Tsukuba University, Japan, and a visiting scholar with the Department of Mathematical Sciences, Michigan Technological University. He is currently with the Division of Physics, Mathematics and Astronomy, California Institute of Technology, Pasadena, where he works as a visiting postdoctoral research fellow.

Dr. Fujiwara's research interests include combinatorics and its interaction with computer science and quantum information science, with particular emphasis on combinatorial design theory, algebraic coding theory, and quantum information theory.

Vladimir D. Tonchev graduated with PhD in Mathematics from the University of Sofia, Bulgaria, in 1980, and received the Dr. of Mathematical Sciences degree from the Bulgarian Academy of Sciences in 1987. After spending a year as a research fellow at the Eindhoven University of Technology, The Netherlands, (1987-88), and two years at the universities of Munich, Heidelberg and Giessen in Germany as an Alexander von Humboldt Research Fellow (1988-90), Dr. Tonchev joined Michigan Technological University, where he is currently a Professor of Mathematical Sciences. Tonchev has published over 160 papers, four books, three book chapters, and edited several volumes in the area of error-correcting codes, combinatorial designs, and their applications. Dr. Tonchev is a member of the editorial board of *Designs, Codes and Cryptography, Journal of Combinatorial Designs, Applications and Applied Mathematics*, and *Albanian Journal of Mathematics*, and a Founding Fellow of the Institute of Combinatorics and its Applications.