ISIT'2013 1569719731

Quantum Stabilizer Codes From Difference Sets

Yixuan Xie, Jinhong Yuan, and Robert Malaney

School of Electrical Engineering and Telecommunications
The University of New South Wales, Sydney, Australia
Email: Yixuan.Xie@student.unsw.edu.au, J.Yuan@unsw.edu.au, R.Malaney@unsw.edu.au

***Abstract*—In this work we have developed a new method to construct general quantum stabilizer codes of variable block size by adopting the notion of a difference set. The proposed method comprises an efficient way to obtain the difference set, and from that set the construction of a quantum stabilizer code, which we refer to as a DSS (Difference Set Stabilizer) code. Our efficient method to generate the difference set requires no computer search, instead only a single parameter is required to generate the set.**

I. Introduction

Following the first quantum error correcting code discovered independently by Shor [1] and Steane [2], a general theory of quantum error correction was given in [3] - [5]. In these works it was realized that quantum error-correction can be formulated as a process in which quantum errors that occurred can be inferred without measuring the quantum state itself.

The important concept of the stabilizer in [6] yielded many useful insights into quantum error correction and permitted many new and powerful codes to be discovered. The key concept of the stabilizer formalism is that we work directly with the operators that stabilize the quantum state, rather than working with the quantum state itself. In [6] [7] it was further emphasized that the stabilizer formalism can be realized as a classical parity-check matrix in either $GF(2)$ or $GF(4)$, and that an orthogonal constraint referred to as the *symplectic inner product* (SIP) must be satisfied. Since then, many useful quantum error correcting codes have been designed based on the stabilizer formalism, such as [7]-[11].

In this work, we are specifically interested in the construction of stabilizer codes based on the notion of difference sets [12]-[14]. The use of difference sets for quantum code construction was first introduced in [7]. The method used in [7] was based on the use of *perfect* difference sets found by computer search. However, the use of perfect difference sets limits the number of constructed codes. Further, in [11] a construction method using a *joint* difference set was described. Similarly, a computer search to find the joint difference sets was required.

In this work, we propose a generalized construction method of quantum stabilizer codes based on a new method of directly generating difference sets. We name the proposed codes, *difference set stabilizer* (DSS) codes. The proposed construction method focuses on the use of cyclic difference sets which are often used in Hadamard matrix design [12]-[14]. The method guarantees that the simplectic inner product constraint is satisfied. The main point of our work is that the new construction method proposed allows for a wider range of difference set based quantum codes. This opens up the possibility for discovery of new efficient quantum codes. The organization of the paper is as follows. Section II briefly introduces the theory of quantum stabilizer codes. Our new systematic construction method is discussed in section III. We present some simulation results on the relative performance of codes constructed by our method in section IV. Finally, section V concludes the paper.

II. Quantum stabilizer and its formalism

In this section we briefly introduce the concepts of quantum stabilizer codes and how they detect an error during the error-correction procedure.

A. Pauli channel

Define the single Pauli operators (matrices) I, X, Y and Z as

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} Y = i \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \tag{1}$$

where $i = \sqrt{-1}$ is the imaginary unit. These operators form a Pauli group $\mathcal{P}_1$ that acts on single qubit. In (1), X and Z represent a bit-flip error and phase-flip error, respectively, and Y is a combination of both. The N-fold tensor product ($\otimes$) of single qubit Pauli operators form an N-qubit Pauli group

$$\mathcal{P}_N = \pm \{I, X, Y, Z\}^{\otimes N}. \tag{2}$$

The main property of $\mathcal{P}_N$ is that any two elements $\{A, B\} \in \mathcal{P}_N$ either *commute* or *anti-commute*. For N-qubit Pauli operators $\{A, B\} \in \mathcal{P}_N$, we have

$$A \circ B = \prod_{i=1}^{n} A_i \cdot B_i, \tag{3}$$

where $\circ$ represents the commutativity between two operators and

$$A_i \cdot B_i = \begin{cases} +1, & if \quad A_i \cdot B_i = B_i \cdot A_i \\ -1, & if \quad A_i \cdot B_i = -B_i \cdot A_i \end{cases}. \tag{4}$$

Two operators commute *iff* $A \circ B = +1$, otherwise, they anti-commute. This important feature of the Pauli group can be used to detect errors within stabilizer formalism, which we now outline in the following.

B. Stabilizer codes

Stabilizer codes [6] are a code space $\mathcal{C}_\mathcal{M}$ that is stabilized by an Abelian subgroup $\mathcal{M}$ of the n-qubit Pauli group $\mathcal{P}_n$, such that all the elements of $\mathcal{M}$ simultaneously generate eigenvalues $+1$. That is,

$$M_i |\psi\rangle = |\psi\rangle \qquad \forall M_i \in \mathcal{M}, \;\; |\psi\rangle \in \mathcal{C}_\mathcal{M},$$

where $|\psi\rangle$ is a quantum states. When an error operator E acts on the state $|\psi\rangle$, the corrupted state $E|\psi\rangle$ is diagnosed by the set of elements M_i from $\mathcal{M}$. The outcome of the diagnostic procedure is a vector of $\{+1, -1\}$ indicating whether E can be detected. More specifically,

$$M_i E |\psi\rangle = \begin{cases} EM_i |\psi\rangle = E|\psi\rangle & \text{Error undetected,} \\ -EM_i |\psi\rangle = -E|\psi\rangle & \text{Error detected.} \end{cases}$$

A quantum code denoted as $[[N, K]]$ encodes K qubits into N qubits. There are $N - K$ generators of the stabilizer, and the quantum code rate is $R^Q = \frac{K}{N}$.

Quantum stabilizer codes are often formalized in the binary field $GF(2)$ since any given Pauli operator on N qubits can be decomposed into an X-containing operator, a Z-containing operator and a phase factor $(+1, -1, i, -i)$. For example,

$$XYYZI = -(XXXII) \times (IZZZI). \tag{5}$$

Thus, we can directly reveal the X-containing operator and Z-containing operator as separate binary strings of length N. The resulting binary formalism of the set of stabilizer generators M_i, $i = 1...N - K$, which we refer to as M_g, is a matrix $H = (H_1|H_2)$ of $2N$ columns and $N - K$ rows, where H_1 and H_2 represent X-containing and Z-containing sub-matrices, respectively.

Example 1: A stabilizer generator M_g can be represented as the binary matrix H in the form of

$$\begin{aligned} M_g &= \begin{matrix} ZZXIX \\ XZZXI \\ IXXZZ \\ ZIXXZ \end{matrix} \Leftrightarrow H = (H_1|H_2) \\ &= \left(\begin{array}{ccccc|ccccc} 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right). \end{aligned} \tag{6}$$

Since there exists the requirement that stabilizers must commute, the following constraint, known as the *symplectic inner product* (SIP) [7], is applied to H,

$$H_1 H_2^T + H_2 H_1^T = 0 \pmod 2. \tag{7}$$

where (mod2) means mathematical logarithmic 2 operation. In this paper, we will propose a new method to construct general quantum stabilizer codes based on binary circulant matrices that satisfy the constraint (7). We call (7) the *SIP constraint*.

III. New Constructions

In this section we first introduce some preliminaries on theories of the cyclic group and difference sets which are the foundation of our proposed constructions. We then propose an efficient construction method that leads to our general quantum DSS codes.

A. Preliminaries

1) Cyclic group

A finite group $G_{\mathcal{Z}_p}$ is a set of numbers that is closed under a single operation, where $\mathcal{Z}$ denotes the domain of real integer numbers and the subscript p is the size of the group. Denote $\mathcal{T}_{\mathcal{Z}_p\setminus\{0\}}$ as a subgroup of $G_{\mathcal{Z}_p}$ with order p. $\mathcal{T}_{\mathcal{Z}_p\setminus\{0\}}$ forms a subgroup closed under modulo-p multiplication ($\odot$), namely the multiplicative group.

Definition 1: For any multiplicative group $\mathcal{T}_{\mathcal{Z}_p\setminus\{0\}}$ of order p, it is *cyclic* if there exists an element $\alpha \in \mathcal{T}_{\mathcal{Z}_p\setminus\{0\}}$ such that, any element $t \in \mathcal{T}_{\mathcal{Z}_p\setminus\{0\}}$ can be expressed as $t = \alpha^i$ for some integer i. Such an element α is named the generator of the cyclic group.

Consider the multiplicative group $\mathcal{T}_{\mathcal{Z}_7\setminus\{0\}} = \{1, 2, \ldots, 6\}$. Both elements 3 and 5 generate the entire group, *e.g.,*

$$\begin{aligned} &3^1 = 3, \; 3^2 = 3 \odot 3 = 2, \; 3^3 = 3^2 \odot 3 = 2 \odot 3 = 6, \\ &3^4 = 3^3 \odot 3 = 6 \odot 3 = 4, \; 3^5 = 3^4 \odot 3 = 4 \odot 3 = 5 \\ &3^6 = 3^5 \odot 3 = 5 \odot 3 = 1. \end{aligned}$$

A useful theorem is the following.

Theorem 1: [15] For every prime p, the multiplicative group $\mathcal{T}_{\mathcal{Z}_p\setminus\{0\}} = \{1, 2, \ldots, p-1\}$.

2) Difference sets

Definition 2: [13] A (p, k, λ) difference set is a subset D of a multiplicative group $\mathcal{T}_{\mathcal{Z}_p\setminus\{0\}}$ such that the order of the group is p, the size of D is k, and each element of $\mathcal{T}_{\mathcal{Z}_p\setminus\{0\}}$ can be expressed as a difference $(d_i - d_j) \bmod p$ of elements from D in exactly λ times.

As an example, $D = \{1, 2, 4\}$ is a $(p, k, \lambda) = (7, 3, 1)$ difference set because each element in $\mathcal{T}_{\mathcal{Z}_7\setminus\{0\}}$ can be written as the difference of two integers from the set D in exactly $\lambda = 1$ way, as can be seen below:

$$\left\{ \begin{array}{lll} 1-2=6 & 2-1=1 & 4-1=3 \\ 1-4=4 & 2-4=5 & 4-2=2 \end{array} \right\} \bmod 7.$$

3) Shift of a difference set

Lemma 1: For every difference set D of size k, we may construct $p - 1$ different shifts of the original set, such that each shift is also a difference set that generates elements of $\mathcal{T}_{\mathcal{Z}_p\setminus\{0\}}$. We denote such shift operations as $\mathcal{S}(D, s)$, where s is $s = \{1, 2, \ldots, p-1\}$.

For example, if $D = \{1, 2, 4\} \subset \mathcal{T}_{\mathcal{Z}_7\setminus\{0\}} = \{1, 2, \ldots, 6\}$, the 6 shifts of D are

$$\begin{aligned} &D = \{1, 2, 4\}, \\ &\mathcal{S}(D, 1) = \{2, 3, 5\}, \; \mathcal{S}(D, 2) = \{3, 4, 6\}, \\ &\mathcal{S}(D, 3) = \{4, 5, 0\}, \; \mathcal{S}(D, 4) = \{5, 6, 1\}, \\ &\mathcal{S}(D, 5) = \{6, 0, 2\}, \; \mathcal{S}(D, 6) = \{0, 1, 3\}. \end{aligned} \tag{8}$$

4) Circulant matrices

A circulant matrix is a square binary matrix of size $p \times p$ that has the form

$$I_{p\times p} = \begin{pmatrix} i_0 & i_1 & i_2 & \cdots & i_{p-1} \\ i_{p-1} & i_0 & i_1 & \cdots & i_{p-2} \\ i_{p-2} & i_{p-1} & i_0 & \cdots & i_{p-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ i_1 & i_2 & i_3 & \cdots & i_0 \end{pmatrix}, \quad (9)$$

where the entries of the matrix have the value of 1 or 0. It can be also represented in its polynomial form $I_{p\times p}(x) = x^{d_1} + x^{d_2} \ldots + x^{d_k}$, where $\{d_1, d_2, \ldots, d_k\}$ are positions of 1 in the first row of $I_{p\times p}$ such that, $d_1 \neq d_2 \neq \ldots \neq d_k$ and $d_1 < d_2 < \ldots < d_k < p$.

Denote a circulant matrix of the form

$$I\left(x\right)^{\mathcal{S}(D,1)} = x^{d_1} + x^{d_2} + x^{d_3}, \quad (10)$$

where $\{d_1 = 2, d_2 = 3, d_3 = 5\} \in \mathcal{S}(D, 1)$, thus, we generate a circulant matrix of row and column weight $k = 3$ which is equivalent to the size of D.

Our proposed method for constructing a DSS code is based on a series of circulant matrices, where each circulant matrix is generated from a difference set D, or its shift $\mathcal{S}(D, s)$, and the resulting parity-check matrix H satisfies the SIP constraint.

B. Proposed DSS code construction

We construct general stabilizer codes using the shift properties given in the previous section. Our proposed construction focusses on the difference sets with parameters [12]-[14]

$$(p, k, \lambda) = (4n - 1, 2n - 1, n - 1) \quad (11)$$

for an *even* integer $n \geq 2$ that results in a prime number $p = 4n - 1$.

To generate a difference set D, consider the multiplicative group $\mathcal{T}_{\mathcal{Z}_7\backslash\{0\}} = \{1, 2, \ldots, 6\}$. By taking the powers of a non-generator element $\beta \in \mathcal{T}_{\mathcal{Z}_7\backslash\{0\}}$, say $\beta = 4$, then we have $\beta^2 = (16 \bmod 7) = 2$ and $\beta^3 = \beta^2 \odot \beta = (2 \odot 4 \bmod 7) = 1$. An interesting feature of D is that by taking the powers of any element $d \in D\backslash\{1\}$, the new set $\{d^1, d^2, d^3\} = \{1, 2, 4\}$ and is equivalent to D. We now present the following theorem.

Theorem 2: For every prime p, the multiplicative group $\mathcal{T}_{\mathcal{Z}_p\backslash\{0\}}$ possesses one difference set $D = \{\beta, \beta^2, \ldots, \beta^k\}$ of size k such that each element of D is a non-generator element of $\mathcal{T}_{\mathcal{Z}_p\backslash\{0\}}$ and each element of $D\backslash\{1\}$ also generates the difference set D *iff* k is also a prime number.

Proof: Assume k is a prime number. Let $D = \{\beta, \beta^2, \ldots, \beta^k\}$, if $\theta = \beta^i$ for $i = \{1, 2, \ldots, k-1\}$, then $\theta^2 = \beta^{2(i)}$, $\theta^3 = \beta^{3(i)}$, ..., $\theta^j = \beta^{j(i)}$. To prove that when $j = k$, $\{\theta, \theta^2, \ldots \theta^j\} = D$, we consider the first case when $i = 1$ and $1 \leq j \leq k$, and we obtain $\{\theta, \theta^2, \ldots \theta^j\} = \{\beta, \beta^2, \ldots \beta^j\} = D$. For the second case when $i \neq 1$ and $1 \leq j \leq k$, if $ij < k$, we know that $\theta^j = \beta^{ij} \in D$, otherwise, for $ij > k$, $\theta^j = \beta^{ij} = \beta^{mk+r}$, where m is an multiple of k and $1 \leq r < k$ is a remainder. Since $\beta^k = 1$, $\theta^j = \beta^{ij} = \beta^{nk+r} = \beta^r$ will be an element in D. However, if k is not a prime number, hence, k can be decomposed into a series of factors $\Upsilon = \{\upsilon_1, \upsilon_2, \ldots, \upsilon_a\}$. These factors can be used to generate a unique sequence of divisors of k,

$$\Xi = \left\{ \xi_l : \forall \xi_l = \prod_{n=1}^{w} \upsilon_n, 1 \leq w \leq a, \exists m = \frac{k}{\xi_l} \right\}.$$

If $i = \xi_l \in \Xi$, then, $\theta^j = \beta^{j(i)} = \beta^{j\frac{k}{m}}$. When $j = m$, $\theta^j = \beta^k$ whereas $m \neq k$ is a divisor of k. In other words, if k is a non-prime number and $i = \xi_l \in \Xi$, β^i only generates a subset of D. ■

By using difference sets acquired from *Theorem 2*, the following theorem for designing DSS codes is now given.

Theorem 3: For any two shift operations of a difference set D, $\mathcal{S}(D, s_1)$, $\mathcal{S}(D, s_2)$, $\{s_1, s_2\} \in \{1, 2, \ldots p-1\}$ and $s_1 \neq s_2$, the corresponding circulant matrices $H_1(x) = I(x)^{\mathcal{S}(D,s_1)}$, $H_2(x) = I(x)^{\mathcal{S}(D,s_2)}$ satisfy the SIP constraint.

Proof: From (10), we denote

$$H_1\left(x\right) = I(x)^{\mathcal{S}(D,s_1)} = x^{d_1+s_1} + x^{d_2+s_1} + \cdots x^{d_t+s_1}$$
$$H_2\left(x\right) = I(x)^{\mathcal{S}(D,s_s)} = x^{d_1+s_2} + x^{d_2+s_2} + \cdots x^{d_t+s_2}.$$

Then

$$\begin{aligned} &H_1\left(x\right) H_2^T\left(x\right) \\ &= \left\{I(x)^{\mathcal{S}(D,s_1)}\right\} \cdot \left\{I(x)^{\mathcal{S}(D,s_2)}\right\}^T \\ &= x^{(d_1+s_1)-(d_1+s_2)} + x^{(d_1+s_1)-(d_2+s_2)} + \cdots \\ &x^{(d_1+s_1)-(d_t+s_2)} + \cdots \; x^{(d_t+s_1)-(d_{t-1}+s_2)} + x^{(d_t+s_1)-(d_t+s_2)} \\ &= kx^{(s_1-s_2)} + x^{(d_1-d_2)+(s_1-s_2)} + \cdots \\ &x^{(d_1-d_t)+(s_1-s_2)} + \cdots x^{(d_t-d_{t-1})+(s_1-s_2)}. \end{aligned} \quad (12)$$

Similarly, we have

$$\begin{aligned} &H_2\left(x\right) H_1^T\left(x\right) \\ &= \left\{I(x)^{\mathcal{S}(D,s_2)}\right\} \cdot \left\{I(x)^{\mathcal{S}(D,s_1)}\right\}^T \\ &= x^{(d_1+s_2)-(d_1+s_1)} + x^{(d_1+s_2)-(d_2+s_1)} + \cdots \\ &x^{(d_1+s_2)-(d_t+s_1)} + \cdots \; x^{(d_t+s_2)-(d_{t-1}+s_1)} + x^{(d_t+s_2)-(d_t+s_1)} \\ &= kx^{(s_2-s_1)} + x^{(d_1-d_2)+(s_2-s_1)} + \cdots \\ &x^{(d_1-d_t)+(s_2-s_1)} + \cdots x^{(d_t-d_{t-1})+(s_2-s_1)}. \end{aligned} \quad (13)$$

By combining equations (12) and (13), we obtain

$$\begin{aligned} &H_1\left(x\right) H_2^T\left(x\right) + H_2\left(x\right) H_1^T\left(x\right) \\ &= k\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right) + x^{d_1-d_2}\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right) \cdots \\ &+x^{d_1-d_t}\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right) + \cdots \\ &x^{d_t-d_{t-1}}\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right). \end{aligned} \quad (14)$$

By taking the modulo-2 sum, the first term in (14) is reduced to $k\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right) = \left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right)$ since k is always an odd number, as given in (11). The rest of the terms in (14) are distinct difference between two elements d_u, d_v of the difference set D. Thus, equation (14) can be rearranged as

$$\begin{aligned} &H_1(x)H_2^T(x) + H_2(x)H_1^T(x) \\ &= \left(1 + \sum_{u=1}^{k} \sum_{\{v=1, v\neq u\}}^{k} x^{d_u-d_v}\right)\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right). \end{aligned} \quad (15)$$

In (15), $\left(1 + \sum_{u=1}^{k} \sum_{\{v=1, v\neq u\}}^{k} x^{d_u-d_v}\right)$ represents an all-one square matrix, where each polynomial degree is a distinct

difference between two elements $\{d_u,\ d_v\} \in D$. Moreover, the second term $\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right)$ is also a circulant matrix of weight 2, so each entry of the resulting circulant matrix $H_1(x)H_2^T(x) + H_2(x)H_1^T(x)$ is a summation of the corresponding column of the second term. Thus, we have proved the theorem by showing that equation (15) is always a circulant matrix that contains only even integers, which is an all-zero square matrix when taking the modulo-2 sum. ■

From *Theorem 3*, we know that any two shifts of a difference set D would yield a trivial quantum stabilizer code with rate $R^Q = 0$. In order to construct non-trivial quantum stabilizer codes we introduce the following three constructions, A, B and C:

Construction A:

Let $H_1(x) = [I^{\mathcal{S}(D,s_1)}(x), I^{\mathcal{S}(D,s_2)}(x)]$ and $H_2(x) = [I^{\mathcal{S}(D,s_3)}(x),\ I^{\mathcal{S}(D,s_4)}(x)]$, where $s_i (i = 1,2,3,4)$ represents the shifts of D in construction, the circulant matrices $I^{\mathcal{S}(D,s_i)}(x)$ are not necessarily equal. Here the square bracket notation represents concatenation of the given interior matrices. This construction method generates a rate $R^Q = \frac{1}{2}$ quantum stabilizer code with parity-check matrix $H(x) = [H_1(x)|H_2(x)]$ that satisfies the SIP constraint.

Example 2: $H_1(x) = [I^{\mathcal{S}(D,1)}(x), I^{\mathcal{S}(D,3)}(x)]$ and $H_2(x) = [I^{\mathcal{S}(D,4)}(x),\ I^{\mathcal{S}(D,2)}(x)]$, where each shift $\mathcal{S}(D,s)$ is obtained from (8). The combined parity-check matrix has the form of

$$\begin{aligned} H(x) &= [H_1(x)|H_2(x)] \\ &= [\ x^2+x^3+x^5,\quad 1+x^4+x^5\ \ | \\ &\qquad x+x^5+x^6,\quad x^3+x^4+x^6\ ]. \end{aligned}$$

By *Theorem 1*,

$$\begin{aligned} &H_1(x)H_2^T(x) + H_2(x)H_1^T(x) \\ &= \left[\ I^{S(D,1)}(x),\quad I^{S(D,3)}(x)\ \right]\left[\begin{array}{c} \{I^{S(D,4)}(x)\}^T \\ \{I^{S(D,2)}(x)\}^T \end{array}\right] + \\ &\quad \left[\ I^{S(D,4)}(x),\quad I^{S(D,2)}(x)\ \right]\left[\begin{array}{c} \{I^{S(D,1)}(x)\}^T \\ \{I^{S(D,3)}(x)\}^T \end{array}\right] \\ &= \mathbf{0} \pmod 2, \end{aligned}$$

where '**0**' denotes all zeros square matrix.

To construct a quantum stabilizer code of rate greater than $\frac{1}{2}$, construction A can be extended as follows:

Construction B:

Let $H_1(x) = [I^{\mathcal{S}(D,s_1)}(x), I^{\mathcal{S}(D,s_2)}(x), \ldots, I^{\mathcal{S}(D,s_l)}(x)]$ be a serial concatenation of l circulant matrices. Similarly $H_2(x) = [I^{\mathcal{S}(D,q_1)}(x), I^{\mathcal{S}(D,q_2)}(x), \ldots, I^{\mathcal{S}(D,q_l)}(x)]$. Such a construction generates a quantum stabilizer code of rate $R^Q = \frac{(l-1)}{l}$ that satisfies the SIP constraint.

Example 3: If $l > 2$, say $l = 3$, $H_1(x) = [I^{\mathcal{S}(D,1)}(x),\ I^{\mathcal{S}(D,4)}(x),\ I^{\mathcal{S}(D,5)}(x)]$ and $H_2(x) = [I^{\mathcal{S}(D,2)}(x),\ I^{\mathcal{S}(D,3)}(x),\ I^{\mathcal{S}(D,6)}(x)]$, the quantum code has rate $R^Q = \frac{2}{3}$, and is of the form

$$\begin{aligned} H(x) &= [H_1(x)|H_2(x)] \\ &= [\ x^2+x^3+x^5,\quad x^1+x^5+x^6,\quad 1+x^2+x^6\ \ | \\ &\qquad x^3+x^4+x^6,\quad 1+x^4+x^5,\quad 1+x^1+x^3\ \ ]. \end{aligned}$$

C. Extension of DSS codes construction

Although the proposed construction methods satisfy the SIP constraint, the constructed quantum stabilizer codes are too dense in that both the performance and the decoding complexity can be affected. As such, we provide an improved construction method in order to reduce the weight of the circulant matrix. From *Theorem 2*, we know that if $\theta = \beta^i$ where i is a divisor of k, a cyclic subset $D' \subset D$ can be obtained. To generate a circulant matrix of low weight, we extend the constructions A and B as follows.

Construction C:

Let $H_1(x) = [I^{\mathcal{S}(D',s_1)}(x), I^{\mathcal{S}(D',s_2)}(x), \ldots, I^{\mathcal{S}(D',s_l)}(x)]$ and $H_2(x) = [I^{\mathcal{S}(D',q_1)}(x), I^{\mathcal{S}(D',q_2)}(x), \ldots, I^{\mathcal{S}(D,q_l)}(x)]$, where D' is a cyclic subset of D with cardinality $|D'| = k' < k$ and l needs to be an even number. The SIP constraint is satisfied *iff* $(s_1+s_2+\ldots+s_l) \mod p = (q_1+q_2+\ldots+q_l) \mod p$, and $(s_j + s_{j+1}) \mod p = (q_j + q_{j+1}) \mod p$ for every odd integer number $1 \leq j < l$.

IV. Simulations

Here we provide simulation results of some constructed DSS codes. We note that to reduce the decoding complexity, classical cyclic codes are commonly decoded using a majority-logic decoder, which is a type of hard-decision decoding algorithm. Since our DSS codes are constructed from circulant matrices, we performed majority-logic decoding [15] [16] on our codes. Note this decoding is used simply for simulation-speed issues, given that we are interested in relative performances only of the codes (similar relative performance will be found if slower BP decoders are utilized). Our simulations are carried out over the quantum depolarizing channel. This channel creates X, Y and Z errors independently with equal flip probability $\frac{f}{3}$. In our simulations an approximation has been made at the decoder side to further reduce the complexity of decoding by considering only the marginal flip probability $f_m = \frac{2f}{3}$ of each received bit.

Based on the proposed construction method, Table I illustrates a set of stabilizer codes with different size p. The performance of these sample codes is plotted in Fig. 1. The quantum code rate of all codes is $R^Q = \frac{1}{2}$. Here we see the relative performance of some DSS codes as a function of block length. Interestingly from Fig. 1, the qubit error rate (QBER) reduces significantly for decreasing block size. One possible explanation for this is that the distance property of DSS codes is irrelevant to the block size of the code, but is relevant to the size of the difference set. Note also, for comparison we have adopted one code $[[13, 7]]$ from [11] and passed it through our decoder. The main point here is that we can see that code performance is comparable to our closely equivalent $[[14, 7]]$ DSS code.

Fig. 2 illustrates the QBER of a DSS code of block size $N = 398$ with different weights. From this figure, we observe that the performance of the code improves when the weight of each circulant matrix is low. The subset D' for each circulant weight is provided in TABLE II.

n	(p, k, λ)	D
2	(7,3,1)	{1 2 4}
6	(23,11,5)	{1 2 3 4 6 8 9 12 13 16 18}
12	(47,23,11)	{1 2 3 4 6 7 8 9 12 14 16 17 18 21 24 25 27 28 32 34 36 37 42}
50	(199,99,49)	{1 2 4 5 7 8 9 10 13 14 16 18 20 23 25 26 28 29 31 32 33 35 36 40 43 45 46 47 49 50 51 52 53 56 57 58 61 62 63 64 65 66 70 72 79 80 81 86 89 90 91 92 94 98 100 102 103 104 106 111 112 114 115 116 117 121 122 123 124 125 126 128 130 131 132 139 140 144 145 151 155 157 158 160 161 162 165 169 172 175 177 178 180 182 184 187 188 193 196}

TABLE I
DIFFERENT BLOCK SIZE QUANTUM STABILIZER CODES CONSTRUCTED FROM OUR PROPOSED METHOD.

k'	D'
$k' = 3$	{1 92 106}
$k' = 9$	{1 43 58 92 106 162 175 178 180}
$k' = 11$	{1 18 61 62 63 103 114 121 125 139 188}
$k' = 33$	{1 5 8 18 25 28 40 52 61 62 63 64 90 92 98 103 106 111 114 116 117 121 123 125 132 139 140 144 157 172 182 187 188}

TABLE II
SUBSET $D' \subset D$ OF DIFFERENT SIZE FOR DSS CODES OF $N = 398$.

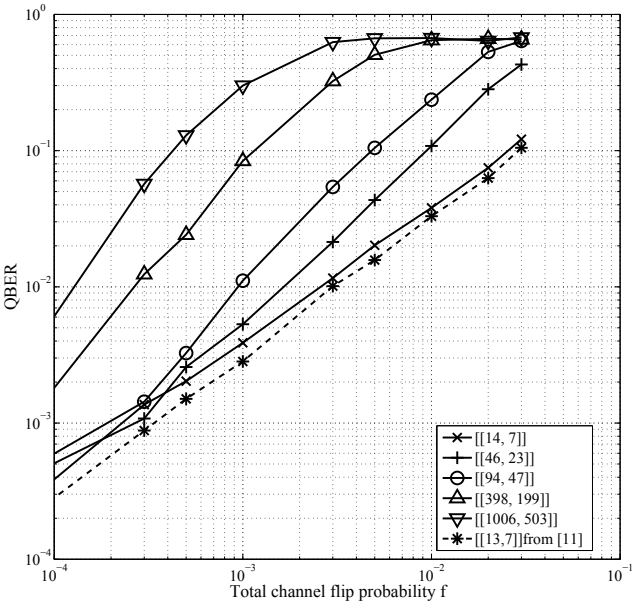

Fig. 1. Performance of DSS codes listed in TABLE II.

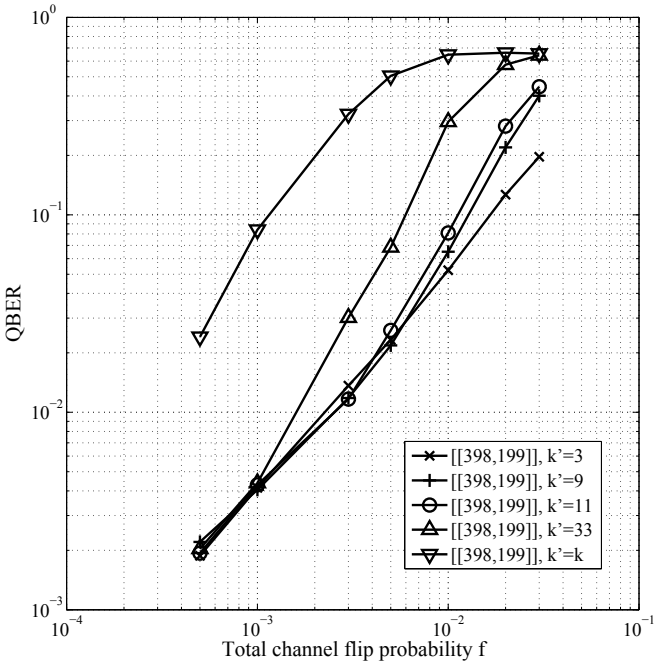

Fig. 2. Performance of DSS codes of block size $N = 398$ with different weights.

V. CONCLUSION

In this work we have developed a new method to construct general quantum stabilizer codes by adopting the notion of a difference set. The proposed method generates a difference set from a single input parameter and ensures the constructed codes satisfy the symplectic inner product constraint. An extension to this work is to develop improved DSS codes by constructing DSS codes possessing quasi-cyclic structure.

REFERENCES

[1] P. W. Shor, "Scheme for reducing decoherence in quantum memory," Phys. Rev. A, vol. 52, pp. 2493 - 2496, 1995.

[2] A. M. Steane, "Error Correcting Codes in Quantum Theory," *Phys. Rev. Lett.*, vol. 77, pp. 793-797, 1996.

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

[4] A. Steane, "Multiple particle interference and quantum error correction," *in Proc. Royal Society of London*, vol. 452, no. 1954, pp. 2551-2577, 1996.

[5] E. Knill and R. Laflamme, "A theory of quantum error correcting codes," *Phys. Rev. A*, vol. 55, pp. 900 - 911, 1997.

[6] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, vol. 54, pp. 1862-1868, 1996.

[7] D. MacKay, G. Mitchison, and P. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Trans. Infor. Theory*, vol. 50, pp. 2315-2330, 2004.

[8] P. Tan and J. Li, "Efficient quantum stabilizer codes: LDPC and LDPC-convolutional constructions," *IEEE Trans. Infor. Theory*, vol. 56, pp. 476-491, 2010.

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

[10] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, "Quantum Error Correction beyond the Bounded Distance Decoding Limit," *IEEE Trans. Infor. Theory*, vol. 58, no. 2, pp. 1223 - 1230, 2012.

[11] S. M Zhao, Y. Xiao, Y. Zhu, X. L. Zhu and M. H. Hsieh, " New class of quantum codes constructed from cyclic difference set", *Int. Jour. Quant. Infor.,* vol. 10, No. 1, 2012.

[12] L. D. Baumert, "Cyclic Difference Sets", *Lecture Notes in Mathematics 182,* New York: Springer-Verlag, 1971.

[13] T. Beth, D. Jungnickel and H. Lenz, "Design Theory", *Cambridge University Press*, New York, 1986.

[14] I. Anderson, "Combinatorial Designs: Construction Methods", *Ellis Horwood Limited*, 1990.

[15] W. E. Ryan, and S. Lin, "Channel Codes: classical and Modern," *Cambridge University Press*, 2009.

[16] S. Lin and D. J. Castello, Jr, " Error Control Coding, second edition" *Pearson Prentice Hall*, 2004.