This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

Stabiliser codes over fields of even order

Simeon Ball[*], Edgar Moreno[†] and Robin Simoens[‡]

Abstract

We prove that the natural isomorphism $\mathbb{F}_{2^h} \cong \mathbb{F}_2^h$ induces a bijection between stabiliser codes on n quqits with local dimension $q = 2^h$ and binary stabiliser codes on hn qubits. This allows us to describe these codes geometrically: a stabiliser code over a field of even order corresponds to a so-called *quantum set of symplectic polar spaces*. Moreover, equivalent stabiliser codes have a similar geometry, which can be used to prove the uniqueness of a $[\![4, 0, 3]\!]_4$ stabiliser code and the nonexistence of both a $[\![7, 1, 4]\!]_4$ and an $[\![8, 0, 5]\!]_4$ stabiliser code.

1 Introduction

It has been known since the late nineties [6] that qubit stabiliser codes are equivalent to classical additive codes contained in their symplectic dual. It was proved in [19] that stabiliser codes over finite fields are equivalent to additive codes over finite fields which are contained in their trace symplectic dual. In this article, we look at stabiliser codes over finite fields of characteristic two in detail. We prove that there is a bijection between stabiliser codes on n quqits over the field $\mathbb{F}_{2^h}$ and stabiliser codes on hn qubits over the field $\mathbb{F}_2$. We prove that the geometrical object which best describes a stabiliser code over a finite field of even order is a set of n symplectic polar spaces of rank h in a projective space over $\mathbb{F}_2$. More precisely, a stabiliser code on n quqits with $q = 2^h$, with a stabiliser group of size 2^r, is equivalent to a set $\mathcal{X}$ of n projective $(2h-1)$-spaces in a projective $(r-1)$-space each equipped with a symplectic polarity, with the following property: every codimension two subspace intersects an even number of the elements of $\mathcal{X}$ in a subspace for which the perpendicular space (with respect to the symplectic polarity) is totally isotropic. This allows us to deduce new results concerning stabiliser codes over $\mathbb{F}_4$. We prove that the $[\![4, 0, 3]\!]_4$ code is unique, that there is no $[\![7, 1, 4]\!]_4$ code and no $[\![8, 0, 5]\!]_4$ code. This last case is of particular interest since it rules out the existence of a

[*]Supported by PID2020-113082GB-I00 financed by MCIN / AEI / 10.13039/501100011033, the Spanish Ministry of Science and Innovation.

[†]Supported by the Higher Interdisciplinary Training Center (CFIS) - Universitat Politècnica de Catalunya (UPC) and SANTANDER- UPC INITIAL RESEARCH GRANTS (INIREC).

[‡]Supported by the Research Foundation Flanders through the grant 11PG724N.

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

stabilised absolutely maximum entangled state on 8 quqits with local dimension 4, see [17].

This paper is structured as follows. In Section 2, we give a background on stabiliser codes, and make the link with classical additive codes. In Section 3, we establish the link between stabiliser codes over $\mathbb{F}_{2^h}$ and over $\mathbb{F}_2$. In Section 4, we provide a geometrical interpretation of stabiliser codes over fields of even order. Finally, in Section 5, these results are used to prove the uniqueness of a $[\![4, 0, 3]\!]_4$ code and the nonexistence of a $[\![7, 1, 4]\!]_4$ code.

2 Preliminaries

In order to define stabiliser codes over finite fields of even order, we first need the definition of the Pauli group.

2.1 The Pauli group

Let $n \in \mathbb{N}$ and let $q = 2^h$ be a power of two. Consider $\mathcal{H} = (\mathbb{C}^q)^{\otimes n}$. This Hilbert space provides a mathematical interpretation for n physical particles that are each in a superposition of q basis states (quqits). Its elements are linear combinations of n-dimensional tensors of q-dimensional complex vectors. A *quantum error-correcting code* is a subspace of $\mathcal{H}$. Let $\{|x\rangle \mid x \in \mathbb{F}_q\}$ be an orthonormal basis of $\mathbb{C}^q$, labelled by the elements of the finite field $\mathbb{F}_q$.

DEFINITION 1. For any $a, b \in \mathbb{F}_q$, let $X(a)$ and $Z(b)$ be the linear operators on $\mathbb{C}^q$ that are defined on the basis $\{|x\rangle \mid x \in \mathbb{F}_q\}$ by

$$\begin{aligned} X(a)\,|x\rangle &= |x + a\rangle \\ Z(b)\,|x\rangle &= (-1)^{\mathrm{tr}(bx)}\,|x\rangle \end{aligned}$$

where tr is the trace map $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_2 : x \mapsto x + x^2 + \cdots + x^{2^{h-1}}$. A *Pauli operator* is a linear operator on $\mathcal{H}$ of the form

$$E = cX(a_1)Z(b_1) \otimes \cdots \otimes X(a_n)Z(b_n)$$

for some $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{F}_q$ and $c \in \{\pm 1, \pm i\}$. Its *weight* is the number of nonidentity factors in its tensor product, i.e. the number of j's for which $(a_j, b_j) \neq (0, 0)$. The *Pauli group* $\mathcal{P}_n$ is the set of Pauli operators.

Note that

$$Z(b)X(a) = (-1)^{\mathrm{tr}(ab)}X(a)Z(b).$$

In particular, $(\mathcal{P}_n, \cdot)$ is indeed a group, and every two elements commute or anti-commute. Pauli operators are unitary and their squares are either I or $-I$ (where I denotes the identity operator).

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

REMARK 2. There are other possible definitions of the (generalised) Pauli group, see [20]. Ours is based upon a labelling with elements of a finite field, as introduced in [19]. Another common one uses a labelling with elements of the modular ring $\mathbb{Z}/q\mathbb{Z}$. However, if $q = 2$, they coincide: $X(1)$ and $Z(1)$ are the "ordinary" Pauli operators, represented by the matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

For general q, our results are specific to the definition of the Pauli operators based on the finite field.

2.2 Stabiliser codes

Stabiliser codes were introduced in [5] and [11] independently.

DEFINITION 3. A *stabiliser code* is a quantum error-correcting code of the form

$$\mathcal{Q} = \{|x\rangle \in \mathcal{H} \mid E\,|x\rangle = |x\rangle \text{ for all } E \in \mathcal{S}\}$$

for some subgroup $\mathcal{S}$ of the Pauli group $\mathcal{P}_n$. We assume that this subgroup is maximal with that property, i.e.

$$\mathcal{S} = \{E \in \mathcal{P}_n \mid E\,|x\rangle = |x\rangle \text{ for all } |x\rangle \in \mathcal{Q}\}.$$

It is called the *stabiliser* of $\mathcal{Q}$. We also assume that $\mathcal{Q}$ is nontrivial, i.e. $\mathcal{Q} \neq \{0\}$, or equivalently, $\mathcal{S} \neq \mathcal{P}_n$.

LEMMA 4 ([19, Lemma 10]). *$\mathcal{S}$ is a stabiliser if and only if $\mathcal{S}$ is an abelian subgroup of $\mathcal{P}_n$ and $-I \notin \mathcal{S}$.*

LEMMA 5. *Nonidentity elements of $\mathcal{S}$ have order* 2.

Proof. Choose any $E \in \mathcal{S}$ and let $|x\rangle$ be a nonzero vector of $\mathcal{Q}$. By definition, $E\,|x\rangle = |x\rangle$. Since $E \in \mathcal{P}_n$, either $E^2 = I$ or $E^2 = -I$. If $E^2 = -I$, then $|x\rangle = E\,|x\rangle = E^2\,|x\rangle = -\,|x\rangle$, a contradiction. So $E^2 = I$. □

The following property is not as trivial as it looks. For a relatively short proof, see the first part of [3, Theorem 5.4].

LEMMA 6 ([6]). *The dimension of $\mathcal{Q}$ is $q^n/|\mathcal{S}|$.*

The *normaliser* of $\mathcal{S}$ in $\mathcal{P}_n$ is $\mathcal{N}(\mathcal{S}) = \{E \in \mathcal{P}_n \mid E\mathcal{S}E^\dagger = \mathcal{S}\}$. It can be shown to equal the centraliser, see [12, Equation (3.6)]. Let $[\mathcal{S}] := \{cE \mid c \in \{\pm 1, \pm i\} \text{ and } E \in \mathcal{S}\}$. By Lemma 4, $[\mathcal{S}] \subseteq \mathcal{N}(\mathcal{S})$.

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

DEFINITION 7. If $|\mathcal{S}| = q^n$, we define the *minimum distance* d of $\mathcal{Q}$ as the minimum nonzero weight of the elements of $\mathcal{S}$. If $|\mathcal{S}| \neq q^n$, we define d as the minimum nonzero weight of the elements of $\mathcal{N}(\mathcal{S}) \setminus [\mathcal{S}]$. We define $k := \log_q(\dim \mathcal{Q})$ and say that $\mathcal{Q}$ is an $[\![n, k, d]\!]_q$ code.

The motivation for this definition comes from the fact that a stabiliser code with minimum distance d can detect all errors up to weight $d - 1$. See [19, Lemma 11].
Note that $|\mathcal{P}_n| = 4 \cdot q^{2n} = 2^{2hn+2}$ and that $\mathcal{S}$ is a subgroup of $\mathcal{P}_n$, so the size of $\mathcal{S}$ is a power of two. By Lemma 6, $|\mathcal{S}| = 2^{h(n-k)}$, so kh must be an integer, though k need not be an integer.

DEFINITION 8. A code is *pure* if d is the minimum nonzero weight of the elements of $\mathcal{N}(\mathcal{S})$, or, equivalently, if the minimum nonzero weight of the elements of $\mathcal{S}$ is at least d.

THEOREM 9 (Quantum Singleton bound [21, Theorem 2]). *Let $\mathcal{Q}$ be an $[\![n, k, d]\!]_q$ code. Then*

$$k \leq n - 2d + 2.$$

If equality holds, the minimum nonzero weight of $\mathcal{S}$ is $n - d + 2$. In particular, $\mathcal{Q}$ is pure.

2.3 Equivalent stabiliser codes

DEFINITION 10. A *Clifford operator* is a unitary operator on $\mathcal{H}$ that normalises the Pauli group. In other words, it is an operator U for which

$$UU^\dagger = I \qquad \text{and} \qquad U\mathcal{P}_n U^\dagger = \mathcal{P}_n.$$

The *Clifford group* $\mathcal{C}_n$ is the set of Clifford operators on $\mathcal{P}_n$. A Clifford operator is called *local* if it is the n-fold tensor product of elements of $\mathcal{C}_1$. The *local Clifford group* $\mathcal{C}_n^l$ is the set of local Clifford operators, i.e. $\mathcal{C}_n^l = (\mathcal{C}_1)^{\otimes n}$.

Note that $\mathcal{P}_n \subseteq \mathcal{C}_n^l \subseteq \mathcal{C}_n$.

DEFINITION 11. Two stabiliser codes are *equivalent* if their stabilisers can be obtained from one another by a sequence of the following operations:

(i) A permutation on the positions of the tensor product.

(ii) Multiplying elements by ± 1 while preserving the group structure.

(iii) Conjugation with a local Clifford operator, i.e. $\mathcal{S} \mapsto U\mathcal{S}U^\dagger$ for some $U \in \mathcal{C}_n^l$.

We only allow multiplication of an element of $\mathcal{S}$ by ± 1 and not by $\pm i$, since the latter would increase its order to 4, contradicting Lemma 5.
Note that a more general notion of equivalence exists, where the conjugation is not necessarily with a local Clifford operator, but rather with any unitary operator, see [18].

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

LEMMA 12. *Equivalent codes have the same parameters.*

Proof. The three operations in Definition 11 preserve the size of the stabiliser and the length and weight of Pauli operators. □

EXAMPLE 13. Note that conjugation with a *nonlocal* Clifford operator does not necessarily preserve the weight. For example, if $n = 2$ and $q = 2$, then

$$U = \frac{1}{2}\left(I \otimes I + X \otimes I + I \otimes Z - X \otimes Z\right)$$

is a Clifford operator sending $I \otimes X$ to $X \otimes X$.

2.4 Stabiliser codes as additive symplectic self-orthogonal codes

Since $\mathcal{S}$ is a subgroup of $\mathcal{P}_n$ of size q^{n-k}, it generated by a set $\{E_1, \ldots, E_r\}$ of $r = h(n-k)$ Pauli operators.

DEFINITION 14. Let τ be the map

$$\begin{aligned}&\tau : \mathcal{P}_n \to \mathbb{F}_{2^h}^{2n} : \\ &\quad cX(a_1)Z(b_1) \otimes \cdots \otimes X(a_n)Z(b_n) \mapsto (a_1, \ldots, a_n, b_1, \ldots, b_n).\end{aligned}$$

Using this map, $\mathcal{S}$ can be represented by its *stabiliser matrix*, an $r \times 2n$-matrix whose rows are the vectors $\tau(E_j)$ for each E_j in the generating set:

$$\left(\begin{array}{cccc|cccc} a_{11} & a_{12} & \cdots & a_{1n} & b_{11} & b_{12} & \cdots & b_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} & b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rn} & b_{r1} & b_{r2} & \cdots & b_{rn} \end{array}\right)$$

where $E_j = c_j X(a_{j1})Z(b_{j1}) \otimes \cdots \otimes X(a_{jn})Z(b_{jn})$. We disregard the phase factors c_j, since stabilisers that differ in only these constants, are equivalent.

LEMMA 15. *τ is a group morphism from $(\mathcal{P}_n, \cdot)$ to $(\mathbb{F}_{2^h}^{2n}, +)$, i.e.*

$$\tau(E_1 E_2) = \tau(E_1) + \tau(E_2).$$

Proof. Since $X(a)X(b) = X(a+b)$ and $Z(a)Z(b) = Z(a+b)$, together with the fact that Pauli operators either commute or anti-commute (and τ ignores the factor ± 1). □

The fact that the elements of $\mathcal{S}$ commute, translates into the property that the rows of this matrix are orthogonal with respect to the *trace-symplectic inner product*

$$\langle (a|b), (a'|b') \rangle_s = \operatorname{tr}(a \cdot b' + a' \cdot b) = \sum_{i=1}^{n} \operatorname{tr}(a_i b'_i + a'_i b_i).$$

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

LEMMA 16 ([6]). *Let $E_1, E_2 \in \mathcal{P}_n$. Then $E_1E_2 = E_2E_1 \iff \langle \tau(E_1), \tau(E_2)\rangle_s = 0$.*

Proof. Denote $E_1 = X(a_1)Z(b_2) \otimes \cdots \otimes X(a_n)Z(b_n)$ and $E_2 = X(a'_1)Z(b'_2) \otimes \cdots \otimes X(a'_n)Z(b'_n)$. Since

$$Z(b)X(a) = (-1)^{\mathrm{tr}(ab)}X(a)Z(b),$$

we have

$$E_1E_2 = (-1)^{\sum_{i=1}^n \mathrm{tr}\left(a'_ib_i\right)} X(a_1 + a'_1)Z(b_1 + b'_1) \otimes \cdots \otimes X(a_n + a'_n)Z(b_n + b'_n)$$

and

$$E_2E_1 = (-1)^{\sum_{i=1}^n \mathrm{tr}\left(a_ib'_i\right)} X(a_1 + a'_1)Z(b_1 + b'_1) \otimes \cdots \otimes X(a_n + a'_n)Z(b_n + b'_n)$$

so

$$E_1E_2 = (-1)^{\langle (a|b),(a'|b')\rangle_s} E_2E_1.$$

□

In other words, the stabiliser matrix is a generator matrix of a code C that is contained in its *symplectic dual*

$$C^{\perp_s} = \{(a|b) \in \mathbb{F}_q^{2n} \mid \langle (a|b), (a'|b')\rangle_s = 0 \text{ for all } (a'|b') \in C\}.$$

The *symplectic weight* of a vector $(a|b) \in \mathbb{F}_q^{2n}$ is defined as

$$\mathrm{swt}(a|b) = \left|\{j \in \{1, \ldots, n\} \mid (a_j, b_j) \neq (0, 0)\}\right|.$$

So the weight of a Pauli operator $E \in \mathcal{P}_n$ is equal to $\mathrm{swt}(\tau(E))$. The symplectic weight of a set of vectors is defined as the minimum among those weights, not including the zero weight.

THEOREM 17 ([19, Theorem 13]). *Let $\mathcal{Q}$ be an $[\![n, k, d]\!]_q$ code with stabiliser $\mathcal{S}$. Then $C = \tau(\mathcal{S})$ is an additive code $C \subseteq \mathbb{F}_q^{2n}$ of size $|C| = q^{n-k}$ such that $C \subseteq C^{\perp_s}$ for which $\mathrm{swt}(C^{\perp_s}) = d$ if $k = 0$ and $\mathrm{swt}(C^{\perp_s} \setminus C) = d$ if $k > 0$. Conversely, given such a code C, there is an $[\![n, k, d]\!]_q$ code with stabiliser $\mathcal{S}$ such that $C = \tau(\mathcal{S})$.*

We should mention that the inverse operation is a bit trickier. Given a vector $(a|b) \in \mathbb{F}_q^{2n}$, there are four Pauli operators E such that $\tau(E) = (a|b)$. They differ in a phase factor. However, this phase factor cannot be chosen arbitrarily. For example, if $n = 1$ and $q = 2$, the vector $(1, 1)$ should not be mapped to XZ but rather to iXZ or $-iXZ$ since XZ has order 4 instead of the required order 2 (see Lemma 5). For each vector of the code, we have two options for the phase factor. However, up to equivalence, there is only one pre-image of τ. We will therefore use the notation $\tau^{-1}(C)$ for the *class* of all stabilisers whose image is C. In other words,

$$\tau^{-1}(C) = [\mathcal{S}] \qquad \text{where } \tau(\mathcal{S}) = C.$$

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

3 Stabiliser codes over fields of even order as binary stabiliser codes

In this section, we work with multiple values of n and h. We will therefore denote the Hilbert space $(\mathbb{C}^{2^h})^{\otimes n}$ by $\mathcal{H}_{n,h}$, the corresponding Pauli group by $\mathcal{P}_{n,h}$, its Clifford group by $\mathcal{C}_{n,h}$ and the local Clifford group by $\mathcal{C}^l_{n,h}$. The map τ becomes $\tau_{n,h}$.
From now on, we also use i as an index, and not necessarily the complex unit.

3.1 The trace-orthogonal trick

Stabiliser codes over fields of even order are connected to binary stabiliser codes by Theorem 21 below. It is a reformulation of [19, Lemma 76], a result that was already implicitly contained in [1]. For the sake of completeness, we include proofs of this theorem and its preparatory lemmas. To this end, we use a so-called trace-orthogonal basis, which was introduced in [1]. See for example also [8].
A basis $\{e_1, \ldots, e_h\}$ of $\mathbb{F}_{2^h} \cong \mathbb{F}_2^h$ over $\mathbb{F}_2$ is called *trace-orthogonal* if it has the property that $\operatorname{tr}(e_i e_j) = \delta_{ij}$ for all $i, j \in \{1, \ldots, h\}$. Note that such a basis always exists [23, Theorem 4].
Recall that $\{|x\rangle \mid x \in \mathbb{F}_{2^h}\}$ is an orthonormal basis of $\mathbb{C}^{2^h}$, labelled by the elements of the finite field $\mathbb{F}_{2^h}$. This allows us to translate the isomorphism $\mathbb{F}_{2^h} \cong \mathbb{F}_2^h$ into a bijective linear map between $\mathcal{H}_{n,h}$ and $\mathcal{H}_{hn,1}$.

DEFINITION 18. Let $\{e_1, \ldots, e_h\}$ be a trace-orthogonal basis of $\mathbb{F}_{2^h}$ over $\mathbb{F}_2$. Let $\Psi_{n,h}$ be the linear transformation $\mathcal{H}_{n,h} \to \mathcal{H}_{hn,1}$ that is defined on the basis $\{|x\rangle \mid x \in \mathbb{F}_{2^h}\}^{\otimes n}$ by

$$\begin{aligned}\Psi_{n,h} \left|x_{11}e_1 + \cdots + x_{1h}e_h\right\rangle \otimes \cdots \otimes \left|x_{n1}e_1 + \cdots + x_{nh}e_h\right\rangle \\ = \left|x_{11}\right\rangle \otimes \cdots \otimes \left|x_{1h}\right\rangle \otimes \cdots \otimes \left|x_{n1}\right\rangle \otimes \cdots \otimes \left|x_{nh}\right\rangle .\end{aligned}$$

For an operator A on $\mathcal{H}_{n,h}$, define

$$\psi_{n,h}(A) := \Psi_{n,h} A \Psi_{n,h}^{-1}$$

to be the corresponding operator on $\mathcal{H}_{hn,1}$.

LEMMA 19. *$\psi_{n,h}(cAB) = c\psi_{n,h}(A)\psi_{n,h}(B)$ and $\psi_{n,h}(A^\dagger) = \psi_{n,h}(A)^\dagger$.*

Proof. The first equality is true by definition. The second one follows from the fact that $\Psi_{n,h}$ is a unitary transformation (it maps an orthonormal basis to an orthonormal basis). □

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

LEMMA 20. $\psi_{n,h}(\mathcal{P}_{n,h}) = \mathcal{P}_{hn,1}$. *More precisely,* $\psi_{n,h}$ *maps*

$$cX(a_{11}e_1 + \cdots + a_{1h}e_h)Z(b_{11}e_1 + \cdots + b_{1h}e_h) \otimes \cdots \\ \cdots \otimes X(a_{n1}e_1 + \cdots + a_{nh}e_h)Z(b_{n1}e_1 + \cdots + b_{nh}e_h)$$

to

$$cX(a_{11})Z(b_{11}) \otimes \cdots \otimes X(a_{1h})Z(b_{1h}) \otimes \cdots \otimes X(a_{n1})Z(b_{n1}) \otimes \cdots \otimes X(a_{nh})Z(b_{nh}).$$

Proof. It suffices to prove this for $n = 1$ because $\psi_{n,h} = \psi_{1,h}^{\otimes n}$ and $\mathcal{P}_{n,h} = \mathcal{P}_{1,h}^{\otimes n}$. Moreover, since $X(a + b) = X(a)X(b)$ and $Z(a + b) = Z(a)Z(b)$, and since $\psi_{n,h}$ is product-preserving (Lemma 19), it is enough to prove that $\psi_{1,h}(X(e_i)) = X_i$ and $\psi_{1,h}(Z(e_i)) = Z_i$, where X_i resp. Z_i denotes the weight one Pauli operator with an X resp. Z in the i-th position. Let $x_1, \ldots, x_h \in \mathbb{F}_2$. Then

$$\begin{aligned}
\psi_{1,h}(X(e_i)) \left|x_1\right\rangle \otimes \cdots \otimes \left|x_h\right\rangle &= \Psi_{1,h} X(e_i) \left|x_1 e_1 + \cdots + x_h e_h\right\rangle \\
&= \Psi_{1,h} \left|x_1 e_1 + \cdots + (x_i + 1)e_i + \cdots + x_h e_h\right\rangle \\
&= \left|x_1\right\rangle \otimes \cdots \otimes \left|x_i + 1\right\rangle \otimes \cdots \otimes \left|x_h\right\rangle \\
&= X_i \left|x_1\right\rangle \otimes \cdots \otimes \left|x_h\right\rangle
\end{aligned}$$

and

$$\begin{aligned}
\psi_{1,h}(Z(e_i)) \left|x_1\right\rangle \otimes \cdots \otimes \left|x_h\right\rangle &= \Psi_{1,h} Z(e_i) \left|x_1 e_1 + \cdots + x_h e_h\right\rangle \\
&= \Psi_{1,h} (-1)^{\operatorname{tr}(e_i \cdot (x_1 e_1 + \cdots + x_h e_h))} \left|x_1 e_1 + \cdots + x_h e_h\right\rangle \\
&= (-1)^{x_i} \left|x_1\right\rangle \otimes \cdots \otimes \left|x_h\right\rangle \\
&= Z_i \left|x_1\right\rangle \otimes \cdots \otimes \left|x_h\right\rangle
\end{aligned}$$

where we used the fact that $\{e_1, \ldots, e_h\}$ is a trace-orthogonal basis. □

The following theorem is a restatement of [19, Lemma 76], but was already implicitly contained in [1] and was extended to arbitrary characteristic in [14], see also [15]. We include a short proof for the sake of completeness.

THEOREM 21 ([19, Lemma 76]). $\Psi_{n,h}$ *induces a bijection between* $[\![n, k, d]\!]_{2^h}$ *codes and* $[\![hn, hk, d']\!]_2$ *codes and* $\psi_{n,h}$ *induces a bijection between their respective stabilisers. Moreover,* $d \leq d' \leq hd$.

Proof. $\mathcal{Q}$ is an $[\![n, k, d]\!]_{2^h}$ code with stabiliser $\mathcal{S}$ for some d if and only if

$$\mathcal{Q} = \{\left|x\right\rangle \in \mathcal{H}_{n,h} \mid E \left|x\right\rangle = \left|x\right\rangle \text{ for all } E \in \mathcal{S}\}$$
$$\mathcal{S} = \{E \in \mathcal{P}_{n,h} \mid E \left|x\right\rangle = \left|x\right\rangle \text{ for all } \left|x\right\rangle \in \mathcal{Q}\}$$

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

and $\dim \mathcal{Q} = (2^h)^k$. Since $\Psi_{n,h}$ is a bijection, and by Lemma 19 and Lemma 20, this is equivalent to saying that

$$\Psi_{n,h}(\mathcal{Q}) = \{|x\rangle \in \mathcal{H}_{hn,1} \mid E\,|x\rangle = |x\rangle \text{ for all } E \in \psi_{n,h}(\mathcal{S})\}$$
$$\psi_{n,h}(\mathcal{S}) = \{E \in \mathcal{P}_{hn,1} \mid E\,|x\rangle = |x\rangle \text{ for all } |x\rangle \in \Psi_{n,h}(\mathcal{Q})\}$$

where $\dim \Psi_{n,h}(\mathcal{Q}) = \dim \mathcal{Q} = 2^{hk}$. In other words, $\mathcal{Q}' := \Psi_{n,h}(\mathcal{Q})$ is an $[\![hn, hk, d']\!]_2$ code with stabiliser $\mathcal{S}' := \psi_{n,h}(\mathcal{S})$.
$d \leq d'$. There is an element of weight d' in $\mathcal{N}(\mathcal{S}') \setminus \mathcal{S}'$ (or $\mathcal{S}'$ if $k = 0$). From Lemma 20, it follows that applying $\Psi_{n,h}^{-1}$ yields an element of weight at most d' in $\mathcal{N}(\mathcal{S}) \setminus \mathcal{S}$ (resp. $\mathcal{S}$).
$d' \leq hd$. There is an element of weight d in $\mathcal{N}(\mathcal{S}) \setminus \mathcal{S}$ (or $\mathcal{S}$ if $k = 0$). Lemma 20 tells us that applying $\Psi_{n,h}$ results in an element of weight at most hd in $\mathcal{N}(\mathcal{S}') \setminus \mathcal{S}'$ (resp. $\mathcal{S}'$). □

Though $\Psi_{n,h}$ induces a bijection, it does not preserve equivalence. See Section 3.2 below.

DEFINITION 22. Let $\{e_1, \ldots, e_h\}$ be a trace-orthogonal basis of $\mathbb{F}_{2^h} \cong \mathbb{F}_2^h$ over $\mathbb{F}_2$. Define

$$\begin{aligned}\varphi_{n,h} : (\mathbb{F}_{2^h})^{2n} &\to (\mathbb{F}_2)^{2hn} : \\ &(x_{11}e_1 + \cdots + x_{1h}e_h, \ldots, x_{2n,1}e_1 + \cdots + x_{2n,h}e_h) \\ &\mapsto (x_{11}, \ldots, x_{1h}, \ldots, x_{2n,1}, \ldots, x_{2n,h}).\end{aligned}$$

COROLLARY 23. *The following diagram commutes:*

$$\begin{array}{ccc} \mathcal{P}_{n,h} & \xrightarrow{\psi_{n,h}} & \mathcal{P}_{hn,1} \\ \downarrow{\scriptstyle \tau_{n,h}} & & \downarrow{\scriptstyle \tau_{hn,1}} \\ \mathbb{F}_{2^h}^{2n} & \xrightarrow{\varphi_{n,h}} & \mathbb{F}_2^{2hn} \end{array}$$

Proof. This follows from Lemma 20 and from the definitions. □

COROLLARY 24. *$\varphi_{n,h}$ induces a bijection between symplectic self-orthogonal additive codes over $\mathbb{F}_{2^h}$ of length $2n$ and size $2^{h(n-k)}$ and binary symplectic self-orthogonal additive codes of length $2hn$ and size $2^{h(n-k)}$. In particular, $\varphi_{n,h}$ preserves the trace-symplectic inner product.*

Proof. C is a symplectic self-orthogonal additive code $C \subseteq \mathbb{F}_{2^h}^{2n}$ of size $2^{h(n-k)}$ if and only if $\mathcal{S} := \tau_{n,h}^{-1}(C)$ is the stabiliser of an $[\![n, k, d]\!]_{2^h}$ code, by Theorem 17. By Theorem 21, this is equivalent to $\mathcal{S}' := \psi_{n,h}(\mathcal{S})$ being the stabiliser of an $[\![hn, hk, d']\!]_2$ code. We can now apply Theorem 17 again to see that, equivalently, $C' := \tau_{hn,1}(\mathcal{S}')$ is a symplectic self-orthogonal additive code $C' \subseteq \mathbb{F}_2^{2hn}$ of size $2^{h(n-k)}$. Finally, note that $C' = \varphi_{n,h}(C)$ by Corollary 23. □

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

Alternatively, we could have proved the above corollary by showing that $\varphi_{n,h}$ preserves the trace-symplectic inner product (which follows from the trace-orthogonality), and then deducing Theorem 21 from it by using Corollary 23.

The above theorem provides a construction for new quantum codes from old ones. Applying $\Psi_{n,h}$ corresponds to the following operation. We start from an $[\![n,k,d]\!]_{2^h}$ code and split the columns of the corresponding symplectic self-orthogonal code according to a trace orthonormal basis to obtain an $[\![hn,hk,d']\!]_2$ code.

EXAMPLE 25. Let $\alpha \in \mathbb{F}_4 \setminus \{0,1\}$. Then $\alpha^2 = \alpha + 1$ and $\{\alpha, \alpha^2\}$ is a trace-orthogonal basis of $\mathbb{F}_4$ over $\mathbb{F}_2$. Consider the $[\![2,1,2]\!]_4$ code with stabiliser matrix

$$\left(\begin{array}{cc|cc} 1 & 1 & \alpha & 0 \\ 0 & 1 & 1 & 1 \end{array}\right).$$

Applying $\Psi_{2,2}$ on this code, or, in other words, applying $\varphi_{2,2}$ on the rows of this matrix, results in the $[\![4,2,2]\!]_2$ code with stabiliser matrix

$$\left(\begin{array}{cc:cc|cc:cc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right).$$

We can also apply $\Psi_{n,h}^{-1}$: we start from an $[\![hn,hk,d']\!]_2$ code and partition the columns into sets of h columns which we merge together to obtain an $[\![n,k,d]\!]_{2^h}$ code.

EXAMPLE 26. Consider the $[\![12,6,3]\!]_2$ code with stabiliser matrix

$$\left(\begin{array}{cccccccccccc|cccccccccccc} 1&0&0&0&0&0&0&1&0&1&0&1&0&0&1&0&1&1&1&0&0&0&0&0 \\ 0&1&0&0&0&0&1&0&1&0&1&0&1&0&0&1&1&1&0&1&0&1&0&0 \\ 0&0&1&0&0&0&0&1&0&1&1&0&0&1&0&0&1&0&0&0&1&0&0&1 \\ 0&0&0&1&0&0&0&1&1&0&0&0&1&0&1&0&1&0&1&1&0&0&1&0 \\ 0&0&0&0&1&0&1&1&0&0&0&1&1&1&1&1&0&1&0&0&0&0&1&1 \\ 0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&1&1&0&1&1&1&1&1&1 \end{array}\right).$$

If we merge every two columns with $\varphi_{6,2}^{-1}$ according to the basis $\{\alpha, \alpha^2\}$ from before, we get the stabiliser matrix

$$\left(\begin{array}{cccccc|cccccc} \alpha & 0 & 0 & \alpha^2 & \alpha^2 & \alpha^2 & 0 & \alpha & 1 & \alpha & 0 & 0 \\ \alpha^2 & 0 & 0 & \alpha & \alpha & \alpha & \alpha & \alpha^2 & 1 & \alpha^2 & \alpha^2 & 0 \\ 0 & \alpha & 0 & \alpha^2 & \alpha^2 & \alpha & \alpha^2 & 0 & \alpha & 0 & \alpha & \alpha^2 \\ 0 & \alpha^2 & 0 & \alpha^2 & \alpha & 0 & \alpha & \alpha & \alpha & 1 & 0 & \alpha \\ 0 & 0 & \alpha & 1 & 0 & \alpha^2 & 1 & 1 & \alpha^2 & 0 & 0 & 1 \\ 0 & 0 & \alpha^2 & 0 & 0 & \alpha & 0 & 1 & \alpha & 1 & 1 & 1 \end{array}\right)$$

of a $[\![6,3,2]\!]_4$ code. Let $\beta \in \mathbb{F}_8$ such that $\beta^3 = \beta^2 + 1$. Then $\{\beta, \beta^2, \beta^4\}$ is a trace-orthogonal basis of $\mathbb{F}_8$ over $\mathbb{F}_2$. If we merge every three columns according to this basis,

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

we get the stabiliser matrix

$$\left(\begin{array}{cccc|cccc} \beta & 0 & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta & 0 \\ \beta^2 & 0 & \beta^3 & \beta^2 & \beta & 1 & \beta^2 & \beta \\ \beta^4 & 0 & \beta^2 & \beta^6 & \beta^2 & \beta^2 & \beta^4 & \beta^4 \\ 0 & \beta & \beta^5 & 0 & \beta^3 & \beta^2 & \beta^6 & \beta^2 \\ 0 & \beta^2 & \beta^6 & \beta^4 & 1 & \beta^3 & 0 & \beta^5 \\ 0 & \beta^4 & 0 & \beta^2 & \beta^4 & \beta^6 & 1 & 1 \end{array}\right).$$

of a $[\![4, 2, 2]\!]_8$ code.

In a similar fashion, we can construct a $[\![6, 2, 3]\!]_4$ code and a $[\![3, 1, 2]\!]_{16}$ code from a $[\![12, 4, 4]\!]_2$ code. One can also construct a $[\![7, 1, 3]\!]_4$ code from a $[\![14, 2, 5]\!]_2$ code and a $[\![8, 0, 4]\!]_4$ code from a $[\![16, 0, 6]\!]_2$ code.

Not all partitions of the columns into h-sets are interesting however. We are only interested in those h-sets that contain linearly independent columns. Otherwise, $\mathcal{N}(\mathcal{S})$ contains elements of weight one. See Lemma 36 below.

The minimum distance can be calculated exactly using Definition 7 or via Theorem 17. Theorem 21 already indicates which values of the minimum distance we might expect.

We can also combine both maps $\Psi_{n,h}$ and $\Psi^{-1}_{n',h'}$ for possibly different n, h, n' and h'.

COROLLARY 27. *Let π denote a permutation on hn elements. Then $\Psi^{-1}_{n',h'} \circ \pi \circ \Psi_{n,h}$ maps an $[\![n, k, d]\!]_{2^h}$ code to an $[\![n', k', d']\!]_{2^{h'}}$ code, where $h'n' = hn$ and $h'k' = hk$.*

Proof. This follows from Theorem 21, and the fact that a permutation of tensor positions gives an equivalent code. □

3.2 Equivalence of stabiliser codes over fields of even order

Although $\Psi_{n,h}$ is a bijection between $[\![n, k, d]\!]_{2^h}$ codes and $[\![hn, hk, d']\!]_2$ codes, it does not necessarily preserve the equivalence of codes. In this section, we establish what this equivalence translates to in the underlying binary code, and in the corresponding symplectic self-orthogonal code.

We start by showing that a local Clifford operator on $\mathcal{P}_{h,n}$ is equivalent to the tensor product of n (global) Clifford operators on $\mathcal{P}_{h,1}$.

LEMMA 28. $\psi_{n,h}\left(\mathcal{C}^l_{n,h}\right) = \mathcal{C}^{\otimes n}_{h,1}$.

Proof. It suffices to show that $\psi_{1,h}\left(\mathcal{C}_{1,h}\right) = \mathcal{C}_{h,1}$, since $\psi_{n,h} = \psi^{\otimes n}_{1,h}$ and $\mathcal{C}^l_{n,h} = \mathcal{C}^{\otimes n}_{1,h}$. Let U be an operator on $\mathcal{H}_{1,h}$. Then

$$\begin{aligned} U \in \mathcal{C}_{1,h} &\Leftrightarrow UU^\dagger = I \text{ and } U\mathcal{P}_{1,h}U^\dagger = \mathcal{P}_{1,h} \\ &\Leftrightarrow \psi_{1,h}(U)\psi_{1,h}(U)^\dagger = I \text{ and } \psi_{1,h}(U)\mathcal{P}_{h,1}\psi_{1,h}(U)^\dagger = \mathcal{P}_{h,1} \\ &\Leftrightarrow \psi_{1,h}(U) \in \mathcal{C}_{h,1} \end{aligned}$$

by Lemma 19 and Lemma 20. □

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

THEOREM 29. *Two $[\![n, k, d]\!]_{2^h}$ codes are equivalent if and only if the stabilisers of the corresponding $[\![hn, hk, d']\!]_2$ codes, obtained by $\psi_{n,h}$, can be converted into one another by a sequence of the following operations:*

(i) A permutation on the n groups of h-fold tensors in the tensor product.

(ii) Multiplying elements by ± 1 while preserving the group structure.

(iii) Conjugation with a Clifford operator of $(\mathcal{C}_{h,1})^{\otimes n}$.

Proof. We show that the operations (i)–(iii) in Definition 11 for equivalent $[\![n, k, d]\!]_{2^h}$ codes correspond to the operations stated above for $[\![hn, hk, d']\!]_2$ codes.

(i) This follows from Lemma 20.

(ii) By linearity of $\psi_{n,h}$ (Lemma 19).

(iii) Suppose that $\mathcal{S}, \mathcal{S}' \leqslant \mathcal{P}_{n,h}$ are stabilisers. Then

$$\begin{aligned}
&\mathcal{S}' = U\mathcal{S}U^\dagger \text{ for some } U \in \mathcal{C}_{n,h}^l \\
&\Leftrightarrow \psi_{n,h}(\mathcal{S}') = \psi_{n,h}(U)\psi_{n,h}(\mathcal{S})\psi_{n,h}(U)^\dagger \text{ for some } U \in \mathcal{C}_{n,h}^l \\
&\Leftrightarrow \psi_{n,h}(\mathcal{S}') = U\psi_{n,h}(\mathcal{S})U^\dagger \text{ for some } U \in \mathcal{C}_{h,1}^{\otimes n}
\end{aligned}$$

by Lemma 19 and Lemma 28.

□

The following theorem tells us what a conjugation with a Clifford operator looks like for the corresponding additive symplectic self-orthogonal code. Here, a *symplectic transformation* on $\mathbb{F}_2^{2n}$ is a change of basis that preserves the symplectic inner product.

THEOREM 30 ([16]). *Binary stabilisers are conjugated by a Clifford operator if and only if the corresponding symplectic self-orthogonal codes are the same up to a symplectic transformation.*

Proof. This was proved in [16] more generally for stabiliser codes over $\mathbb{Z}/d\mathbb{Z}$. If $d = 2$, these coincide with binary stabiliser codes, see also Remark 2.
An alternative proof can be found in Appendix A. □

COROLLARY 31. *Two $[\![n, k, d]\!]_{2^h}$ codes are equivalent if and only if the stabiliser matrices of the corresponding $[\![hn, hk, d']\!]_2$ codes, obtained by $\varphi_{n,h}$, are the same up to:*

(i) Row operations (i.e. left multiplication with an invertible $h(n-k) \times h(n-k)$ matrix).

(ii) Permutations on the n blocks of $2h$ columns.

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

(iii) Symplectic transformations on the $2h$ columns of one of these n blocks.

Here, a "block" denotes a set of h consecutive columns in the X part (obtained from one column by applying $\varphi_{n,h}$) and the corresponding h columns in the Z part.

Proof. This follows from Theorem 29 and Theorem 30. The generators are determined up to linear combinations, so the rows of the matrix are determined up to row operations. □

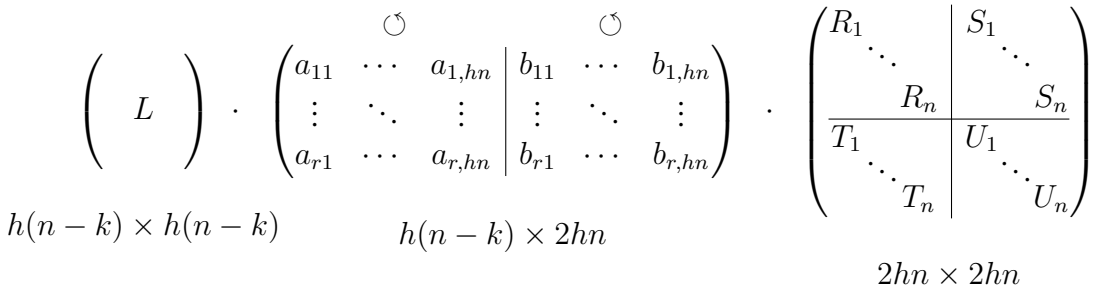


Figure 1: Operations that give an equivalent stabiliser matrix, where L is invertible and each $2h \times 2h$ block matrix $\begin{pmatrix} R_i & S_i \\ T_i & U_i \end{pmatrix}$ is a symplectic matrix.

4 The geometry of stabiliser codes over fields of even order

Looking at stabiliser codes geometrically, provides a powerful tool to understand better what is going on. In fact, the previous results were found after investigating this link with finite geometry.

We refer to [3] for an overview of some links between quantum error-correcting codes and finite geometry.

For convenience, we will treat stabiliser codes with the same stabiliser matrix as the same code (though they differ in phase factors).

4.1 Binary stabiliser codes as quantum sets of lines

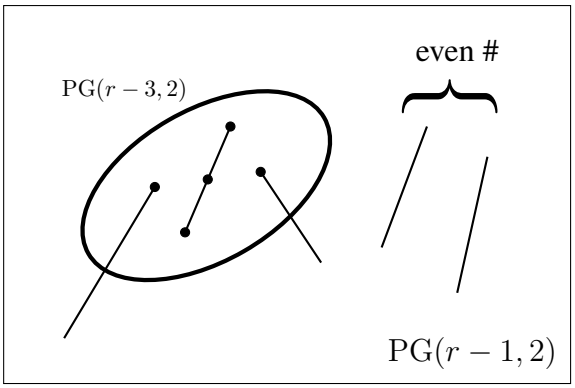
Let $\mathcal{Q}$ be a binary stabiliser code with minimum distance $d \geq 2$. Recall that $\mathcal{Q}$ can be represented by a stabiliser matrix, whose rows are the vectors $\tau(S)$ for every S in a given generating set of the stabiliser (see Definition 14). We can interpret the columns of this matrix as points of the projective space $\mathrm{PG}(r-1, q)$. For each $i = 1, \ldots, n$, the span of the i-th column and the $(n+i)$-th column is a line (and not a point, because the columns are different as $\mathcal{N}(\mathcal{S})$ has no elements of weight one, see [3, Lemma 3.6]). This set of lines

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

defines a so-called *quantum set of lines*, as defined below. This concept was introduced in [10] and refined in [3]. Vice versa, a quantum set of lines defines a stabiliser code by considering them as columns of a stabiliser matrix. This correspondence is made concrete in Theorem 33 below.

DEFINITION 32. A *quantum set of n lines* in $\mathrm{PG}(r-1,2)$ is a set X of n lines spanning $\mathrm{PG}(r-1,2)$ such that every codimension two subspace is skew to an even number of the lines.



If $k=0$, we define the *minimum distance* d of X as the minimum size of a set of dependent points on distinct lines of X. If $k>0$, we define d as the minimum size of a set of dependent points on distinct lines of X such that there is no hyperplane containing these points and all the lines of X that do not contain one of these points.

THEOREM 33 ([10, Proposition 1.13]). *Let $d \geq 2$. There is a bijection between:*

(i) $[\![n,k,d]\!]_2$ *stabiliser codes.*

(ii) Quantum sets of n lines in $\mathrm{PG}(n-k-1,2)$ *with minimum distance d.*

Moreover, binary stabiliser codes are equivalent if and only if their quantum sets of lines are projectively equivalent.

The last sentence of the above theorem ensures that these lines really are the same objects as binary stabiliser codes.

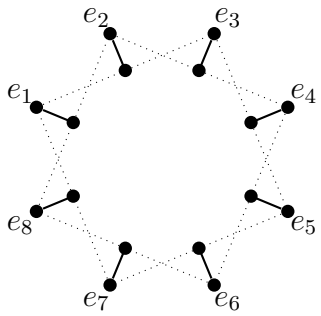
EXAMPLE 34. Consider the matrix

$$\left(I_8 \mid A\right) = \left(\begin{array}{cccccccc|cccccccc} 1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\ 0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0\\ 0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0\\ 0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&0\\ 0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&0\\ 0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1\\ 0&0&0&0&0&0&0&1&1&0&0&0&0&0&1&0 \end{array}\right)$$

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

where A is the adjacency matrix of the 8-cycle. It is the stabiliser matrix of an $[\![8, 0, 3]\!]_2$ code (more precisely, it is the *graph state* of the 8-cycle). The corresponding quantum set of lines looks like this:

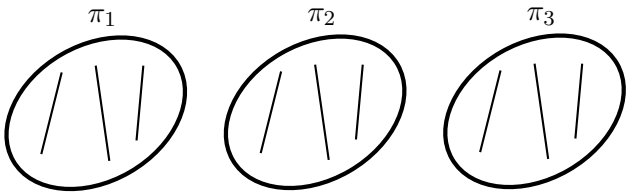


Its minimum distance is $d = 3$, since every two lines are in general position ($d > 2$) and the three points e_1, e_3 and $e_1 + e_3$ lie on different lines and are linearly dependent ($d \leq 3$).

4.2 Stabiliser codes over fields of even order as quantum sets of sets of lines

We introduce the following new concept, extending Definition 32 to arbitrary $q = 2^h$.

DEFINITION 35. A *quantum set of n sets of h lines* in $\mathrm{PG}(r-1, 2)$ is a partitioning $\mathcal{X}$ of a quantum set of hn lines in $\mathrm{PG}(r-1, 2)$ into n subsets of h lines that span a projective $(2h-1)$-space. Denote these projective $(2h-1)$-spaces by $\pi_1, \pi_2, \ldots, \pi_n$.



If $k = 0$, we define the *minimum distance* d of $\mathcal{X}$ as the minimum size of a set of dependent points in distinct π_i's. If $k > 0$, we define d as the minimum size of a set of dependent points in distinct π_i's such that there is no hyperplane containing these points and all π_i's that do not contain one of these points.

Recall that the stabiliser matrix of an $[\![n, k, d]\!]_{2^h}$ stabiliser code is an $h(n-k) \times 2n$ matrix G with entries in $\mathbb{F}_{2^h}$. If we replace every column of this matrix by h columns according to a trace-orthogonal basis of $\mathbb{F}_{2^h} \cong \mathbb{F}_2^h$ over $\mathbb{F}_2$, we obtain an $h(n-k) \times 2hn$ matrix G' with entries in $\mathbb{F}_2$. Let π_i be the subspace of $\mathrm{PG}(h(n-k)-1, 2)$ that is spanned by the h columns from the original i-th column and the h columns from the original $(n+i)$-th column.

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

LEMMA 36 ([3, Lemma 5.8]). *The subspace π_i is a $(2h-1)$-dimensional subspace for all $i = 1, \ldots, n$ if and only if the minimum nonzero weight of $\mathcal{N}(\mathcal{S})$ is at least two.*

We can now state Theorem 21 geometrically, thereby generalising Theorem 33.

THEOREM 37. *Let $d \geq 2$. There is a bijection between:*

(i) $[\![n, k, d]\!]_{2^h}$ stabiliser codes.

(ii) Quantum sets of n sets of h lines $\mathcal{X}$ in PG$(h(n-k)-1, 2)$ with minimum distance d.

Proof. Let G be the stabiliser matrix of an $[\![n, k, d]\!]_{2^h}$ code. If we apply $\varphi_{n,h}$ on each of its rows, we obtain the stabiliser matrix G' of an $[\![hn, hk, d']\!]_2$ code by Theorem 21. By Theorem 33, the rows of G' correspond to a quantum set of lines X in $\mathrm{PG}(h(n-k)-1)$ with $|X| = hn$. The lines of X are spanned by pairs of points whose coordinates are the i-th and $(hn+i)$-th column of G'. If we partition the quantum set of lines X into subsets X_i of the h lines that result from the i-th and $(n+i)$-th column in G, we get a quantum set of n sets of h lines. Indeed, by Lemma 36, and since $d \geq 2$, the lines of every such h-set span a $(2h-1)$-space.

Conversely, every quantum set of n sets of h lines $\mathcal{X}$ in PG$(h(n-k)-1, 2)$ with $|\mathcal{X}| = n$, can be mapped to the stabiliser matrix of an $[\![hn, hk, d']\!]_2$ code, after which one can apply $\varphi_{n,h}^{-1}$ (i.e. group every h columns together) to obtain a stabiliser matrix of an $[\![n, k, d]\!]_{2^h}$ code.

We now prove that the minimum distances are the same. (For this part, we follow the proof of [3, Theorem 3.8] with some adjustments.) Let C be the code with generator matrix G. By Theorem 17, $\mathrm{swt}(C^{\perp_s}) = d$ if $k = 0$ and $\mathrm{swt}(C^{\perp_s} \setminus C) = d$ if $k > 0$.

If $k = 0$, then $d = \mathrm{swt}(C^{\perp_s})$. Choose $(a|b) \in C^{\perp_s}$ with $\mathrm{swt}(a|b) = d$ and write its entries as $a_i = \sum_{j=1}^{h} a_{ij} e_j$ and $b_i = \sum_{j=1}^{h} b_{ij} e_j$. Let W be the set of indices that contribute to the symplectic weight, i.e.

$$W = \{i \in \{1, \ldots, n\} \mid (a_i, b_i) \neq (0, 0)\}.$$

Let v_i denote the i-th column of G, and write it as a span of the corresponding h columns in G', $v_i = \sum_{j=1}^{h} v_{ij} e_j$. Since $(a|b)$ is in $C^{\perp_s}$, we have

$$\begin{aligned}
\vec{0} &= \sum_{i \in W} \mathrm{tr}(a_i v_{n+i} + v_i b_i) \\
&= \sum_{i \in W} \sum_{j,l=1}^{h} (a_{ij} v_{n+i,l} + v_{il} b_{ij}) \mathrm{tr}(e_j e_l) \\
&= \sum_{i \in W} \sum_{j=1}^{h} (a_{ij} v_{n+i,j} + v_{ij} b_{ij}).
\end{aligned}$$

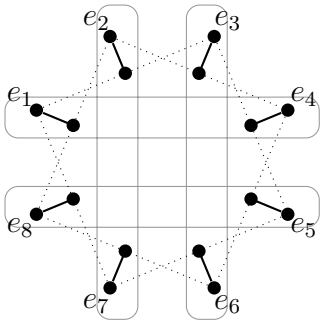
© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

Each summand $\sum_{j=1}^{h}(a_{ij}v_{n+i,j} + v_{ij}b_{ij})$ is a point in the space π_i spanned by the i-th set of h lines of $\mathcal{X}$. Thus, there are $|W| = \mathrm{swt}(a|b) = d$ points on distinct $(2h-1)$-spaces spanned by an h-set that are dependent. Conversely, every point in π_i can be written as $\sum_{j=1}^{h}(a_{ij}v_{n+i,j} + v_{ij}b_{ij})$ for some a_i and b_i. Hence, the existence of a set of d dependent points in distinct π_i's also implies the existence of a vector $(a|b) \in C^{\perp_s}$ with $\mathrm{swt}(a|b) = d$.

If $k > 0$, then $d = \mathrm{swt}(C^{\perp_s} \setminus C)$. Choose $(a|b) \in C^{\perp_s} \setminus C$ with $\mathrm{swt}(a|b) = d$. Since $(a|b) \in C^{\perp_s}$, the above reasoning implies that there are d points on distinct $(2h-1)$-spaces spanned by an h-set that are dependent. However, since $(a|b) \notin C$, we should disregard the case where $(a|b) = x \cdot G$ for some $x \in \mathbb{F}_2^{h(n-k)}$. Consider the hyperplane $\pi : x \cdot X = 0$ in $\mathrm{PG}(h(n-k)-1, 2)$. If $i \in W$, then $x \cdot \sum_{j=1}^{h}(a_{ij}v_{n+i,j} + v_{ij}b_{ij}) = \sum_{j=1}^{h}(a_{ij}b_{ij} + a_{ij}b_{ij}) = 0$, so the dependent points are contained in π. If $i \notin W$, then $a_i = x \cdot v_i = 0$ and $b_i = x \cdot v_{n+i} = 0$ are both zero, which is the case if and only if the i-th $(2h-1)$-space is contained in π. □

EXAMPLE 38. Here is an example of a pairing of lines to make a $[\![4, 0, 3]\!]_4$ code.



The minimum distance is $d = 3$, since every two solids (projective 3-spaces) span the entire space ($d > 2$) and the three points e_1, e_3 and $e_1 + e_3$ lie in different solids and are linearly dependent ($d \leq 3$). We will prove in Section 5 that this code is unique.

This provides a geometrical interpretation of the map $\Psi_{n,h}$ defined earlier. It sends a quantum set of sets of lines to its underlying quantum set of lines. The inverse map $\Psi_{n,h}^{-1}$ groups a quantum set of lines into sets of h lines, but only if the lines in one group are in general position.

4.3 Equivalent quantum sets of sets of lines

Although stabiliser codes over finite fields of characteristic two can be seen as quantum sets of sets of lines, the equivalence of codes is not necessarily translated into projective equivalence. We can do more. Conjugation with a Clifford operator now corresponds to a symplectic transformation of each of the $(2h-1)$-spaces. To understand this better, we introduce the notion of a symplectic polar space.

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

DEFINITION 39. Let V be a vector space. A *bilinear form* on V is a map $f : V^2 \to V$ that is linear in both arguments. A *totally isotropic subspace* of f is a subspace $W \leqslant V$ such that $f(v, w) = 0$ for any $v, w \in W$.
An *symplectic form* (or *alternating form*) on V is a bilinear form $f : V^2 \to V$ such that $f(v, v) = 0$ for all $v \in V$. It is *degenerate* if there exists a $v \in V \setminus \{0\}$ such that $f(v, \cdot) \equiv 0$. A *symplectic transformation* is a change of basis of V that preserves f.

If $V = \mathbb{F}_2^n$, one can show that f is symplectic if and only if $f(v, w) = v^T A w$ for some symmetric $(n \times n)$-matrix A with zeroes on the diagonal. The matrix A is singular if and only if f is degenerate.

DEFINITION 40. A *symplectic polar space of rank* h, denoted by $W(2h-1, 2)$, is the set of totally isotropic subspaces of a nondegenerate symplectic form f on $\mathbb{F}_2^{2h}$. We associate with it a *symplectic polarity* on $\mathrm{PG}(2h-1, 2)$, defined by

$$\pi \mapsto \pi^\perp := \{v \in \mathbb{F}_2^{2h} \mid f(v, w) = 0 \text{ for all } w \in \pi\}.$$

LEMMA 41. *Let $\ell_1, \ldots, \ell_h$ be h lines that span a $(2h-1)$-space. There is a unique symplectic polarity on this space such that $\ell_i^\perp = \langle \ell_j \mid i \neq j \rangle$ for all $i = 1, \ldots, h$.*

Proof. Choose a basis $\{e_1, \ldots, e_{2h}\}$ of $\mathbb{F}_2^{2h}$ such that $\ell_i = \langle e_i, e_{h+i} \rangle$ for all i. The symplectic inner product

$$f(v, w) = \langle v, w \rangle_s = v_1 w_{h+1} + v_{h+1} w_1 + \cdots + v_h w_{2h} + v_{2h} w_h$$

is the unique nondegenerate symplectic form for which the associated symplectic polarity fulfils the condition in the statement. □

With regard to the previous lemma, we use the notation $f_{\{\ell_1, \ldots, \ell_h\}}$ for the unique symplectic form determined by the lines $\ell_1, \ldots, \ell_h$.

THEOREM 42. *Stabiliser codes over fields of even order are equivalent if and only if their quantum sets of sets of lines are the same up to a projective equivalence and, for each set of lines $\{\ell_1, \ldots, \ell_h\}$, a symplectic transformation on $\langle \ell_1, \ldots, \ell_h \rangle$ with respect to $f_{\{\ell_1, \ldots, \ell_h\}}$.*

Proof. Recall that every two consecutive columns in the stabiliser matrix correspond to a line, and every block of $2h$ columns determines a set of h lines. The statement then follows from Corollary 31:

(i) Row operations on the stabiliser matrix are equivalent to projective transformations.

(ii) Permutations of the blocks are exactly the permutations on the $(2h-1)$-spaces.

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

(iii) A symplectic transformation on the $2h$ columns of one block is a change of basis that preserves the symplectic inner product. But the lines are ordered in such a way that $\ell_i = \langle e_i, e_{h+i} \rangle$, where $\{e_1, \ldots, e_h\}$ is the standard basis of $\langle \ell_1, \ldots, \ell_h \rangle$. Following the proof of Lemma 41, $f_{\{\ell_1,\ldots,\ell_h\}}$ is therefore also the symplectic inner product. So a symplectic transformation in the sense of Corollary 31 is the same as a symplectic transformation with respect to $f_{\{\ell_1,\ldots,\ell_h\}}$.

□

4.4 Stabiliser codes over fields of even order as quantum sets of symplectic polar spaces

The following lemma is a special case of Witt's theorem. A *hyperbolic* line is a line that is not totally isotropic.

LEMMA 43 ([24, Theorem 3.4]). *The group of symplectic transformations acts transitively on the totally isotropic (resp. hyperbolic) lines.*

Note that a recursive application of this lemma allows one to prove that the group of symplectic transformations on $W(2h-1, 2)$ acts transitively on the sets of h lines $\{\ell_1, \ldots, \ell_h\}$ for which $\ell_i^\perp = \langle \ell_j \mid i \neq j \rangle$.

LEMMA 44. *A line ℓ is hyperbolic if and only if $\ell \cap \ell^\perp = \{0\}$.*

Proof. It suffices to prove that $\ell \cap \ell^\perp$ is never a point. Suppose it were. Choose any $p \in \ell \backslash \ell^\perp$. Then $\ell^\perp \subseteq p^\perp$, but also $p \in p^\perp$, so $\ell \subseteq p^\perp$ and thus $p \in \ell^\perp$, a contradiction. □

THEOREM 45. *Let $\ell_1, \ldots, \ell_h$ be h lines such that $\ell_i^\perp = \langle \ell_j \mid i \neq j \rangle$ and let π be a codimension two space. The property "π is skew to an even number of the lines $\ell_1, \ldots, \ell_h$" is preserved under symplectic transformations with respect to $f_{\{\ell_1,\ldots,\ell_h\}}$.*

Proof. From the proof of Theorem 33 (see [10, Proposition 1.13]), this property is equivalent to saying that a certain pair of rows of the associated stabiliser, is symplectic orthogonal. By Corollary 31, this property is preserved under symplectic transformations. Part (iii) of the proof of Theorem 42 tells us that these are exactly the symplectic transformations with respect to $f_{\{\ell_1,\ldots,\ell_h\}}$. □

THEOREM 46. *Let π be a subspace of $\mathrm{PG}(2h-1, 2)$ of codimension 0,1 or 2. Let $\ell_1, \ldots, \ell_h$ be h lines such that $\ell_i^\perp = \langle \ell_j \mid i \neq j \rangle$. The following are equivalent.*

(i) π is skew to an even number of the lines $\ell_1, \ldots, \ell_h$.

(ii) $\pi^\perp$ is totally isotropic.

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

Proof. If the codimension of π is 0 or 1, both properties are always true, since π is skew to no line, and every point is totally isotropic. So assume that $\pi^\perp$ is a line.
If $\pi^\perp$ is a totally isotropic line, choose two points $p, p' \in \pi^\perp \subseteq \pi$ and a point $q \notin p^\perp$. Then pq is a hyperbolic line and there exists a symplectic transformation σ such that $\sigma(\ell_1) = pq$ by Lemma 43. Moreover, $(pq)^\perp = \sigma(\ell_1)^\perp = \langle \sigma(\ell_2), \ldots, \sigma(\ell_h) \rangle$. Now, $(pq)^\perp \cap \pi = (pq)^\perp \cap p'^\perp$ is a hyperplane of $(pq)^\perp$, so all lines $\sigma(\ell_1), \ldots, \sigma(\ell_h)$ intersect π. Thus, π is skew to none of the lines $\sigma(\ell_1), \ldots, \sigma(\ell_h)$. By Theorem 45, π is skew to an even number of the lines $\ell_1, \ldots, \ell_h$.
If $\pi^\perp$ is a hyperbolic line, then $\pi \cap \pi^\perp = \{0\}$ by Lemma 44. There exists a symplectic transformation σ such that $\sigma(\ell_1) = \pi^\perp$ by Lemma 43. Then $\pi = \langle \sigma(\ell_2), \ldots, \sigma(\ell_h) \rangle$ and hence, π is skew to exactly one of the lines $\sigma(\ell_1), \ldots, \sigma(\ell_h)$, namely $\sigma(\ell_1)$. By Theorem 45, π is skew to an odd number of the lines $\ell_1, \ldots, \ell_h$.

□

DEFINITION 47. A *quantum set of n symplectic polar spaces of rank h* in $\mathrm{PG}(r-1,2)$ is a set X of n projective $(2h-1)$-spaces spanning $\mathrm{PG}(r-1,2)$, each equipped with a symplectic polarity with the following property: every codimension two subspace intersects an even number of the elements of X in a subspace π for which $\pi^\perp$ is totally isotropic.
If $k = 0$, we define the *minimum distance* d of X as the minimum size of a set of dependent points in distinct $(2h-1)$-spaces of X. If $k > 0$, we define d as the minimum size of a set of dependent points on distinct $(2h-1)$-spaces of X such that there is no hyperplane containing these points and all $(2h-1)$-spaces of X that do not contain one of these points.

THEOREM 48. *Let $d \geq 2$. There is a bijection between:*

(i) $[\![n, k, d]\!]_{2^h}$ *stabiliser codes.*

(ii) Quantum sets of n symplectic polar spaces of rank h in PG$(h(n-k)-1, 2)$ with minimum distance d.

Moreover, stabiliser codes over fields of even order are equivalent if and only if their quantum sets of symplectic polar spaces are projectively equivalent.

Proof. This follows from Theorem 37, Theorem 42 and Theorem 46. □

If $h = 1$, a symplectic polar space of rank h is a line and we get Theorem 33 (a symplectic transformation of a line is a projective transformation of the line).
Note that, if a code is pure, then the minimum distance of the corresponding set of symplectic polar spaces is minimum size of a set of dependent points in distinct $(2h-1)$-spaces of X.

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

5 Applications

In this section, we prove the uniqueness of a $[\![4,0,3]\!]_4$ code and the nonexistence of a $[\![7,1,4]\!]_4$ code and an $[\![8,0,5]\!]_4$ code.

Note that, as stabiliser codes over $\mathbb{Z}/4\mathbb{Z}$ (see Remark 2), codes with these parameters do not exist, since they would imply the existence of a $[\![4,0,3]\!]_2$, a $[\![7,1,4]\!]_2$ and an $[\![8,0,5]\!]_2$ code, which do not exist [13].

Our approach is the following. By Theorem 48, an $[\![n, n-2(d-1), d]\!]_4$ code is equivalent to a set of n solids (projective 3-spaces) in $\mathrm{PG}(4d-5,2)$, each equipped with a symplectic polarity, such that every $d-1$ solids span the entire space, and such that every codimension two space intersects an even number of solids in a hyperbolic line. Note that the minimum distance being d, is equivalent to every $d-1$ solids spanning the whole space. We do not have the more elaborate definition of minimum distance because the code is pure, as it meets the quantum Singleton bound in Theorem 9.

For $d=3$, we classify sets of n solids in $\mathrm{PG}(7,2)$, for $n \in \{4,5,6\}$. We then look for symplectic polarities with the property that every codimension two subspace intersects an even number of these solids in a hyperbolic line. This allows us to prove that a $[\![4,0,3]\!]_4$ is unique and to determine all $[\![6,2,3]\!]_4$ codes. We observe that it is not feasible computationally for $d=4$ and $n=7$. However, we use a projection argument to rule out the $[\![7,1,4]\!]_4$ code, see Section 5.2.

5.1 There is a unique $[\![4,0,3]\!]_4$ code

It was proved in [7] that the $[\![4,0,3]\!]_4$ stabiliser code is unique. Here, we reprove this, and demonstrate how our method applies to these parameters.

By Theorem 48, a $[\![4,0,3]\!]_4$ code is equivalent to a set of four solids (projective 3-spaces) in $\mathrm{PG}(7,2)$, each equipped with a symplectic polarity, such that every two solids span the entire space, and such that every codimension two space intersects an even number of solids in a hyperbolic line.

We first show that there are only three configurations of four solids in $\mathrm{PG}(7,2)$ such that every two solids span the entire space. Without loss of generality, the four solids are spanned by the four column blocks of a block matrix of the form

$$\left(\begin{array}{c|c|c|c} I & O & I & I \\ O & I & I & A \end{array}\right).$$

Indeed, we can first perform row operations (i.e. projective transformations) to bring it into the form

$$\left(\begin{array}{c|c|c|c} * & * & * & * \\ * & * & * & * \end{array}\right) \mapsto \left(\begin{array}{c|c|c|c} I & O & * & * \\ O & I & * & * \end{array}\right)$$

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

and then perform column operations within each block (which do not change the span of the columns) to get

$$\mapsto \left(\begin{array}{c|c|c|c} I & O & I & I \\ O & I & * & * \end{array}\right) \mapsto \left(\begin{array}{c|c|c|c} I & O & I & I \\ O & * & I & * \end{array}\right) \mapsto \left(\begin{array}{c|c|c|c} I & O & I & I \\ O & I & I & * \end{array}\right).$$

Now, A is still determined up to a conjugation $A \mapsto XAX^{-1}$, as we can do

$$\left(\begin{array}{c|c|c|c} I & O & I & I \\ O & I & I & A \end{array}\right) \mapsto \left(\begin{array}{c|c|c|c} X & O & X & X \\ O & X & X & XA \end{array}\right) \mapsto \left(\begin{array}{c|c|c|c} I & O & I & I \\ O & I & I & XAX^{-1} \end{array}\right)$$

and up to a permutation of the four solids. Together with the condition that every two column blocks form an invertible matrix, one can check by computer that there are only three different configurations (five up to conjugation and three up to conjugation and permutation):

$$A_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad \text{and} \quad A_3 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

For each of them, we check whether they can be equipped with a symplectic polarity such that every codimension two space intersects an even number of solids in a hyperbolic line. Suppose that this is the case. For each line ℓ in each of the four solids (so $4 \cdot 35 = 140$ lines), let

$$x_\ell = \begin{cases} 0 \text{ if } \ell \text{ is totally isotropic} \\ 1 \text{ if } \ell \text{ is hyperbolic} \end{cases}.$$

Then for each codimension two space π, the sum of the x_ℓ's for which ℓ is the intersection of π with one of the four solids, equals zero modulo 2. So it suffices to check a system of homogeneous equations over $\mathbb{F}_2$. This can be done by computer. Given such a solution, one still has to check whether the lines ℓ for which $x_\ell = 1$, really are hyperbolic lines of a symplectic polarity. Now, $W(3,2)$ contains 15 totally isotropic lines and 20 hyperbolic lines, so we first of all check that $|\{\ell \in \pi \mid x_\ell = 1\}| = 20$. Then, we choose a (potential) hyperbolic line ℓ_1 and loop over all (potential) hyperbolic lines ℓ_2 to check whether $\ell_2 = \ell_1^\perp$ (we can fix ℓ_1 by Lemma 43). This is true if and only if every other (potential) hyperbolic line intersects exactly one of them, by Theorem 46. If we find such a line ℓ_2, then these lines are indeed the hyperbolic lines of a symplectic polarity (and it is unique by Lemma 41).

Implementing these constraints on a computer results in three solutions for A_3 and no solutions for A_1 and A_2. However, the three solutions can be checked to be equivalent up to a projective transformation that fixes the solids.

The code for this can be found on `https://github.com/robinsimoens/stabiliser-codes-over-fields-of-even-order`. We used the mathematics software system Sage [22].

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

5.2 A $[\![7,1,4]\!]_4$ code does not exist

By Theorem 48, a $[\![7,1,4]\!]_4$ code is equivalent to a set of seven solids (projective 3-spaces) in $\mathrm{PG}(11,2)$, each equipped with a symplectic polarity, such that every three solids span the entire space, and such that every codimension two space intersects an even number of solids in a hyperbolic line. (Recall that the minimum distance being four, is equivalent to every three solids spanning the whole space. We do not have the more elaborate definition of minimum distance because the code is pure, as a $[\![7,1,4]\!]_4$ code meets the quantum Singleton bound in Theorem 9.)

LEMMA 49. *Let $\mathcal{X}$ be a quantum set of n symplectic polar spaces of rank h in $\mathrm{PG}(r-1,2)$ with minimum distance d. If we project from one of its spaces, we get a quantum set of $n-1$ symplectic polar spaces of rank h in $\mathrm{PG}(r-2h-1,2)$ with minimum distance $d-1$ or d.*

Proof. By definition. □

In particular, if there exists an $[\![n,k,d]\!]_{2^h}$ code, then there also exists an $[\![n-1,k+1,d-1]\!]_{2^h}$ code. For this reason, we first generate all $[\![6,2,3]\!]_4$ codes. We do this in a similar way as in the previous section. We may assume that the six solids are spanned by the column blocks of a block matrix of the form

$$\left(\begin{array}{c|c|c|c|c|c} I & O & I & I & I & I \\ \hline O & I & I & A & B & C \end{array}\right).$$

A computer program tells us that, up to conjugation and permutation, there are 341 configurations of six solids in $\mathrm{PG}(7,2)$ such that every two solids span the entire space. This was done by first determining all A-blocks up to conjugation and permutation, then all B-blocks given these A-blocks, and then the C-blocks.

Then, we equip each solid with a symplectic polarity such that every codimension two space is skew to an even number of hyperbolic lines. In a similar way as for the previous example, we find 1311 solutions for this. So there are at most 1311 different $[\![6,2,3]\!]_4$ codes.

Now, to rule out the existence of a $[\![7,1,4]\!]_4$ code, we may assume that its solids are spanned by a matrix of the form

$$\left(\begin{array}{c|c|c|c|c|c|c} X_0 & O & O & Y & A_0 & B_0 & C_0 \\ \hline O & X_1 & O & Y & A_1 & B_1 & C_1 \\ \hline O & O & X_2 & Y & A_2 & B_2 & C_2 \end{array}\right)$$

where A_0, A_1, B_0, B_1, C_0 and C_1 are solutions to the $[\![6,2,3]\!]_4$ codes found before, and such that every two columns span a hyperbolic line and its perpendicular line. In particular, every two rows of

$$\left(Y \mid A_2 \mid B_2 \mid C_2\right)$$

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

have to be symplectic orthogonal to the rows of the matrix

$$\left(\begin{array}{c|c|c|c} Y & A_0 & B_0 & C_0 \\ \hline Y & A_1 & B_1 & C_1 \end{array}\right)$$

with respect to the symplectic form

$$f(v,w) = v_1w_2 + v_2w_1 + \cdots + v_{15}w_{16} + v_{16}w_{15}.$$

Moreover, every submatrix of 3×3 blocks is invertible. This implies extra conditions on A_2, B_2 and C_2. For every solution for A_2, B_2 and C_2 obtained by computer, we observe that the rows of $\left(Y \mid A_2 \mid B_2 \mid C_2\right)$ are pairwise symplectic orthogonal. This implies that every two rows of X_2 must be symplectic orthogonal. This is a contradiction, since X_2 has full rank. So there does not exist a $[\![7, 1, 4]\!]_4$ code.
The code for this can be found on `https://github.com/robinsimoens/stabiliser-codes-over-fields-of-even-order`. We used the mathematics software system Sage [22]. We also wrote the same program in GAP [9], using in particular the FinInG package [4], to check the validity of the program. It gave the same results.
By Lemma 49, the nonexistence of a $[\![7, 1, 4]\!]_4$ code implies the nonexistence of an $[\![8, 0, 5]\!]_4$ code.

6 Conclusion

We showed that every stabiliser code over a field of even order can be seen as a binary stabiliser code. Geometrically, they correspond to quantum sets of symplectic polar spaces, up to projective equivalence. This allowed us to prove the uniqueness of a $[\![4, 0, 3]\!]_4$ code and the nonexistence of a $[\![7, 1, 4]\!]_4$ code and an $[\![8, 0, 5]\!]_4$ code.
We present some open problems and directions for future work:

(i) It is known that one-dimensional binary stabiliser codes can be seen as graphs (hence they are also called *graph states*). Moreover, equivalent codes correspond to graphs up to *local complementation*. The notion of local complementation extends to stabiliser codes over fields of prime order, see [2]. What about stabiliser codes over fields of even order? They can be seen as graphs where we group the vertices into n sets of h vertices. The question remains what a conjugation with a Clifford operator translates to on these graphs.

(ii) We solved [3, Research Problem 4] in the case when q is even. Can we do something similar for codes over finite fields of odd characteristic? There are two drawbacks. First, there does not always exist a trace-orthogonal basis in odd characteristic. However, one can circumvent this using a so-called polarisation of the phase space, see

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

[14, 15]. Second, it has not been established what these codes correspond to geometrically. Multiplying a column with -1 does not affect the projective geometry, but it does not come from a conjugation with a Clifford operator. This suggests that, instead of looking at the projective points determined by the columns, we should rather look at them as affine points.

(iii) We can do something similar for stabiliser codes over modular rings, reducing them to binary codes with certain properties.

Acknowledgements

We would like to thank the referees, Markus Grassl and Markus Heinrich for their useful comments.

References

[1] A. Ashikhmin and E. Knill, *Nonbinary quantum stabilizer codes*, IEEE Trans. Inf. Theory **47** (2001) no. 7, 3065–3072.

[2] M. Bahramgiri and S. Beigi, *Graph states under the action of local Clifford group in non-binary case*, arXiv preprint quant-ph/0610267 (2006).

[3] S. Ball, A. Centelles and F. Huber, *Quantum error-correcting codes and their geometries*, Ann. Henri Poincaré D **10** (2023) no. 2, 337–405.

[4] J. Bamberg, A. Betten, P. Cara, J. De Beule, M. Lavrauw, M. Neunhoeffer and M. Horn, *FinInG, Finite Incidence Geometry, Version 1.5.6* (2023) (Refereed GAP package), `https://gap-packages.github.io/FinInG`.

[5] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, *Quantum Error Correction and Orthogonal Geometry*, Phys. Rev. Lett. **78** (1997) 405-–409.

[6] A.R. Calderbank, E.M. Rains, P.W. Shor, and N. Sloane, *Quantum error correction via codes over* $\mathrm{GF}(4)$, IEEE Trans. Inf. Theory **44** (1998) 1369–1387.

[7] L.E. Danielsen, *Graph-based classification of self-dual additive codes over finite fields*, Adv. Math. Commun. **3** (2009) no. 4, 329–348.

[8] C. Galindo, F. Hernando, M. Ryutaroh and R. Diego, *Entanglement-assisted quantum error-correcting codes over arbitrary finite fields*, Quantum Inf. Process. **18** (2019) no. 116.

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

[9] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.12.2* (2022) https://www.gap-system.org.

[10] D.G. Glynn, T.A. Gulliver, J.G. Maks and M.K. Gupta, *The Geometry of Additive Quantum Codes*, unpublished manuscript (2014) available online at https://www.academia.edu/17980449/.

[11] D. Gottesman, *Class of quantum error-correcting codes saturating the quantum Hamming bound*, Phys. Rev. A **54** (1996), 1862–1868.

[12] D. Gottesman, *Stabilizer codes and quantum error correction*, Caltech PhD Thesis (1997).

[13] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, unpublished tables, available online at http://www.codetables.de.

[14] D. Gross, K. Audenaert and J. Eisert, *Evenly distributed unitaries: On the structure of unitary designs*, J. Math. Phys. **48** (2007) no. 5.

[15] M. Heinrich, *On stabiliser techniques and their application to simulation and certification of quantum devices*, University of Cologne PhD Thesis (2021).

[16] E. Hostens, J. Dehaene and B. De Moor, *Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic*, Phys. Rev. A **71** (2005) 042315.

[17] F. Huber and N. Wyderka, *Table of AME states*, unpublished tables, available online at https://www.tp.nt.uni-siegen.de/+fhuber/ame.html.

[18] Z. Ji, J. Chen, Z. Wei and M. Ying, *The LU-LC conjecture is false*, Quantum Inf. Comput. **10** (2010) no. 1, 97–108.

[19] A. Ketkar, A. Klappenecker, S. Kumar and P.K. Sarvepalli, *Nonbinary Stabilizer Codes Over Finite Fields*, IEEE Trans. Inf. Theory **52** (2006) no. 11, 4892–4914.

[20] A Klappenecker and M. Rotteler, *Beyond stabilizer codes .I. Nice error bases*, IEEE Trans. Inf. Theory **48** (2002) no. 8, 2392–2395.

[21] E.M. Rains, *Nonbinary quantum codes*, IEEE Trans. Inf. Theory **45** (1999) 1827.

[22] The Sage Developers, *SageMath, the Sage Mathematics Software System, Version 10.1* (2023) https://www.sagemath.org.

[23] G. Seroussi and A. Lempel, *Factorization of symmetric matrices and trace-orthogonal bases in finite fields*, SIAM J. Comput. **9** (1980) no. 4, 758–10.

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

[24] D. Sprehn and N. Wahl, *Forms over fields and Witt's lemma*, Math. Scand. **126** (2020) no. 3, 401–423.

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

Appendix A An algebraic proof of Theorem 30

Theorem 30 was proved in [16] more generally for stabiliser codes over $\mathbb{Z}/d\mathbb{Z}$. In this appendix, we provide an alternative, more algebraic proof instead of a constructive proof. Let τ be the map

$$\begin{aligned}&\tau : \mathcal{P}_n \to \mathbb{F}_2^{2n} : \\ &\quad cX(a_1)Z(b_1) \otimes \cdots \otimes X(a_n)Z(b_n) \mapsto (a_1, \ldots, a_n, b_1, \ldots, b_n).\end{aligned}$$

as defined in Definition 14 (with $q = 2$). Recall that a symplectic transformation on $\mathbb{F}_2^{2n}$ is a change of basis that preserves the symplectic inner product.

THEOREM 50 ([16]). *Binary stabilisers are conjugated by a Clifford operator if and only if the corresponding symplectic self-orthogonal codes are the same up to a symplectic transformation.*

Proof. Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be two binary stabilisers and let $C_1 = \tau(\mathcal{S}_1)$ and $C_2 = \tau(\mathcal{S}_2)$ be the corresponding symplectic self-orthogonal codes.
First suppose that $\mathcal{S}_1$ and $\mathcal{S}_2$ are conjugated by any linear operator U, i.e. $\mathcal{S}_2 = U\mathcal{S}_1U^{-1}$. Define the bijection $\sigma : C_1 \to C_2$ that sends $(a|b)$ to $\tau(U\tau^{-1}(a|b)U^{-1})$. It is well-defined because conjugation preserves phase factors. It is linear by Lemma 15. Choose arbitrary $(a|b), (a'|b') \in \mathbb{F}_2^{2n}$. Let $E_1, E_2 \in \mathcal{P}_n$ with $\tau(E_1) = (a|b)$ and $\tau(E_2) = (a'|b')$. Then by the proof of Lemma 16,

$$E_1E_2 = (-1)^{\langle (a|b),(a'|b')\rangle_s} E_2E_1.$$

On the other hand, $\sigma(a|b) = \tau(UE_1U^{-1})$ and $\sigma(a'|b') = \tau(UE_2U^{-1})$, so

$$\begin{aligned}E_1E_2 &= U^{-1}\left(UE_1U^{-1}\right)\left(UE_2U^{-1}\right)U \\ &= U^{-1}(-1)^{\langle \sigma(a|b),\sigma(a'|b')\rangle_s}\left(UE_2U^{-1}\right)\left(UE_1U^{-1}\right)U \\ &= (-1)^{\langle \sigma(a|b),\sigma(a'|b')\rangle_s} E_2E_1,\end{aligned}$$

so $\langle (a|b), (a'|b')\rangle_s = \langle \sigma(a|b), \sigma(a'|b')\rangle_s$ and thus, σ is a symplectic transformation.
Conversely, assume that C_1 and C_2 are the same up to a symplectic transformation σ. Consider the map $g : \mathcal{S}_1 \to \mathcal{S}_2$ defined by $g = \tau^{-1} \circ \sigma \circ \tau$. Its image is a class of four stabilisers that are the same up to a phase factor. We therefore define a new map h for which $g(E) = [h(E)]$ as follows. Denote X_i resp. Z_i for the weight one Pauli operator with an X resp. Z in the i-th position and let $W = \{X_1, \ldots, X_n, Z_1, \ldots, Z_n\}$. Note that it spans about half the Pauli group. For every X_i, choose and fix its image $h(X_i)$ in $g(X_i)$ such that it has order two again (and similar for the Z_i's). There is a unique way to extend this map to a homomorphism of the group generated by W, i.e. such that

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2024.3454480

$h(E_1E_2) = h(E_1)h(E_2)$. Indeed, the product relations between the X_i's and Z_i's are preserved because

$$h(X_i)^2 = h(Z_i)^2 = I$$

and

$$h(E_1)h(E_2) = (-1)^{\langle\sigma(\tau(E_1)),\sigma(\tau(E_2))\rangle_s}h(E_2)h(E_1) = (-1)^{\langle\tau(E_1),\tau(E_2)\rangle_s}h(E_2)h(E_1)$$

for all $E_1, E_2 \in W$, where we used that σ preserves the symplectic inner product. In particular, $g(E) = [h(E)]$ for every such operator, since $g(E_1E_2) = g(E_1)g(E_2)$ by Lemma 15. Since W forms a basis for $\mathcal{H}$, we can extend h uniquely to a linear map on $\mathcal{H}$ that fulfils $h(E_1 + E_2) = h(E_1) + h(E_2)$, which makes h an algebra morphism. We can now apply the Skolem-Noether theorem to conclude that $h(E) = UEU^{-1}$ for some U. Choose an arbitrary Pauli operator $E \in \mathcal{P}_n$. Then $h(E)$ is again a Pauli operator, so $h(E)h(E)^\dagger = I$. Therefore, $UU^\dagger$ commutes with E, and because E was chosen arbitrarily, it commutes with all Pauli operators. Hence, $UU^\dagger = cI$ for some constant c. Now, $UU^\dagger$ is positive semidefinite, so c is real positive and we can replace U by $\frac{1}{\sqrt{c}}U$ to obtain the desired Clifford operator. □

Note that the above proof can be generalised easily to stabiliser codes over any prime field $\mathbb{F}_p$ or, equivalently, stabiliser codes over $\mathbb{Z}/p\mathbb{Z}$ (we refer to [19] and [16] for their respective definitions).

SIMEON BALL
DEPARTMENT OF MATHEMATICS
UNIVERSITAT POLITÈCNICA DE CATALUNYA
C. PAU GARGALLO 14, 08028 BARCELONA, SPAIN
E-mail address: simeon.michael.ball@upc.edu

EDGAR MORENO
HIGHER INTERDISCIPLINARY TRAINING CENTER (CFIS)
UNIVERSITAT POLITÈCNICA DE CATALUNYA
C. PAU GARGALLO 14, 08028 BARCELONA, SPAIN
E-mail address: edgar.moreno.martinez@estudiantat.upc.edu

ROBIN SIMOENS
DEPARTMENT OF MATHEMATICS: ANALYSIS, LOGIC AND DISCRETE MATHEMATICS
GHENT UNIVERSITY
KRIJGSLAAN 281, 9000 GENT, BELGIUM
DEPARTMENT OF MATHEMATICS
UNIVERSITAT POLITÈCNICA DE CATALUNYA
C. PAU GARGALLO 14, 08028 BARCELONA, SPAIN
E-mail address: Robin.Simoens@UGent.be

© 2024 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.