

On Steane-Enlargement of Quantum Codes from Cartesian Product Point Sets

René Bødker Christensen  and Olav Geil 

Department of Mathematical Sciences, Aalborg University, Denmark.
`{rene,olav}@math.aau.dk`

Abstract

In this work, we study quantum error-correcting codes obtained by using Steane-enlargement. We apply this technique to certain codes defined from Cartesian products previously considered by Galindo et al. in [8]. We give bounds on the dimension increase obtained via enlargement, and additionally give an algorithm to compute the true increase. A number of examples of codes are provided, and their parameters are compared to relevant codes in the literature, which shows that the parameters of the enlarged codes are advantageous. Furthermore, comparison with the Gilbert-Varshamov bound for stabilizer quantum codes shows that several of the enlarged codes match or exceed the parameters promised by the bound.

Keywords: Cartesian product, Quantum code, Steane-enlargement, Finite fields

2000 MSC: 94B27, 81Q99

1 Introduction

Quantum computers promise to deliver computational power far exceeding what can be achieved by classical computers, see for instance [26, 28]. Naturally, this has led to much interest in the construction of large scale quantum computers. The quantum bits used in such a system would, however, be prone to errors caused by interaction with the environment. Therefore, methods for correcting such errors are essential, and quantum error correcting codes provide a possible solution.

As in classical coding theory, the performance of a quantum code is assessed based on parameters such as the size of the underlying field, the length of the code and its dimension, and the number of errors that the code can correct. Some of the earliest quantum codes such as [2, 3, 27] were binary, but just as in classical coding theory it is also possible to study codes over arbitrary finite fields [14, 24]. When working over \mathbb{F}_q – i.e. the finite field of q elements – a quantum code of length n and dimension k is a q^k -dimensional subspace of \mathbb{C}^{q^n} .

One important difference between classical and quantum error correction lies in the types of errors that can happen. Whereas classical bits are susceptible only to *bit flip* errors, quantum bits are also affected by *phase shift* errors.

This is a post-peer-review, pre-copyedit version of an article published in *Quantum Information Processing*. The final authenticated version is available online at:
<https://doi.org/10.1007/s11128-020-02691-9>

Thus, we can consider two measures of minimal distance for quantum codes: d_x for bit flips, and d_z for phase shifts. Some authors treat the two types of errors equally, and in this case only a single minimal distance $d = \min\{d_x, d_z\}$ is associated to the quantum code. The code is then called *symmetric*. Alternatively, the two types of errors can be treated separately – e.g. to account for the two types of errors happening with different probabilities [12]. In this case both of the distances are of interest, and the codes are called *asymmetric*. Clearly, the parameters in the asymmetric setting can be translated into the symmetric setting by ignoring the highest distance.

Traditionally, quantum codes were only studied in the symmetric case, but by now the literature contains a great number of works studying either of the two types of codes. In this work, we only consider symmetric codes, and some recent developments in this field are [7, 18, 19, 21, 22, 25, 31]. In this setting, the code parameters are commonly written in the form $[[n, k, d]]_q$, and we will follow this convention.

In [8], Galindo et al. gave two constructions of asymmetric quantum error-correcting codes constructed by applying the CSS-construction to nested classical codes based on Cartesian product point sets. The resulting codes have good parameters compared to existing constructions when investigating which combinations of n , k , d_x , and d_z are possible for various values of q . In addition, these codes compare favourably to the Gilbert-Varshamov bound for asymmetric quantum codes. As mentioned above, someone interested in symmetric codes could use the results from [8] by discarding the highest distance, but this essentially wastes coding space which could instead be used to increase the dimensions of the codes. In this work, we take an alternative approach and apply Steane-enlargement to that family of codes in order to produce symmetric codes directly. We thereby produce quantum error-correcting codes with good – sometimes even optimal – parameters.

The classical codes considered in this work are special cases of what is called *monomial Cartesian codes* in a recent work [21]. In that paper, the authors derived a way to determine if a monomial Cartesian code is dual-containing, and used this to construct quantum codes via the CSS-construction. The classical codes used in their construction are, however, different from the ones used in the current paper. In particular, the improved codes considered in this work have the best possible dimension given any designed distance.

This work is structured as follows: Section 2 recalls the definitions and results needed in subsequent sections. This includes the CSS-construction and Steane-enlargement as well as results from the theory of classical algebraic geometry codes. Afterwards, Section 3 describes a new construction of quantum codes, including bounds on and exact values of the dimension increase. The section ends by comparing the resulting parameters to other known constructions. Finally, Section 4 contains the conclusion and outlines open problems for future work.

2 Preliminaries

In this section, we recall two results on the CSS-construction and Steane-enlargement that allow construction of quantum codes from classical codes. Then we give a description of a family of codes and the corresponding improved codes, both of which were previously considered in [8]. In our analysis, we will rely on the notion of relative distances of nested pairs of classical linear codes. Thus, recall that for codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1$ their relative distance is defined as

$$d(\mathcal{C}_1, \mathcal{C}_2) = \min\{w_H(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}_1 \setminus \mathcal{C}_2\},$$

where w_H denotes the usual Hamming weight. In general, however, the relative distance is difficult to determine, and the bound $d(\mathcal{C}_1, \mathcal{C}_2) \geq d(\mathcal{C}_1)$ is commonly used instead.

2.1 The CSS-construction and Steane-enlargement

One way to construct quantum error-correcting codes is by using the so-called CSS-construction [3, 29] named after Calderbank, Shor, and Steane. The original construction uses a dual-containing classical linear code to construct a symmetric quantum error-correcting code.

Theorem 1. *If the $[n, k, d]$ linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ contains its Euclidean dual, then an*

$$[[n, 2k - n, d]]_q$$

symmetric quantum code exists.

Steane [30] proposed a variation on this procedure, which in some cases allows an increase in dimension compared to the corresponding CSS-code but without reducing the minimal distance. Below, we state the q -ary generalization of this procedure, which may be found in [11, 20].

Theorem 2. *Consider a linear $[n, k]$ code $\mathcal{C} \subseteq \mathbb{F}_q^n$ that contains its Euclidean dual \mathcal{C}^\perp . If \mathcal{C}' is an $[n, k']$ code such that $\mathcal{C} \subsetneq \mathcal{C}'$ and $k' \geq k + 2$, then an*

$$\left[\left[n, k + k' - n, \geq \min \left\{ d, \lceil (1 + \frac{1}{q})d' \rceil \right\} \right] \right]_q$$

quantum code exists with $d = d(\mathcal{C}, \mathcal{C}'^\perp)$ and $d' = d(\mathcal{C}', \mathcal{C}'^\perp)$.

Remark 3. *Here we note that if \mathcal{C} and \mathcal{C}' are codes that satisfy the conditions of Theorem 2, then the inclusions $\mathcal{C}'^\perp \subsetneq \mathcal{C}^\perp \subseteq \mathcal{C} \subsetneq \mathcal{C}'$ hold, which implies $d(\mathcal{C}'^\perp) \geq d(\mathcal{C})$. In particular, this means that whenever $d(\mathcal{C}') < d(\mathcal{C})$, it must be the case that $d' = d(\mathcal{C}', \mathcal{C}'^\perp) = d(\mathcal{C}')$. For the specific enlargements considered in Section 3, it turns out that this observation allows us to use the usual minimal distances rather than the relative distances while still obtaining the same parameters of the quantum codes.*

2.2 Codes from Cartesian product point sets

Let $q = p^r$ where p is a prime number, and let r_1, r_2, \dots, r_m be positive integers such that $r_i \mid r$. Then we have the inclusions $\mathbb{F}_{p^{r_i}} \subseteq \mathbb{F}_q$, and it is possible to consider the Cartesian product $S = \mathbb{F}_{p^{r_1}} \times \mathbb{F}_{p^{r_2}} \times \cdots \times \mathbb{F}_{p^{r_m}} \subseteq \mathbb{F}_q^m$. Now, define the polynomials

$$F_i(X_i) = \prod_{\alpha \in \mathbb{F}_{p^{r_i}}} (X_i - \alpha) = X_i^{p^{r_i}} - X_i,$$

and consider the ring $R = \mathbb{F}_q[X_1, X_2, \dots, X_m]/I$ where

$$I = \langle F_1(X_1), F_2(X_2), \dots, F_m(X_m) \rangle$$

is the vanishing ideal of the F_i 's. Letting $n = |S| = \prod_{i=1}^m p^{r_i}$ and $S = \{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_n\}$, we obtain a vector space homomorphism $\text{ev}: R \rightarrow \mathbb{F}_q^n$ given by

$$\text{ev}(F + I) = (F(\boldsymbol{\alpha}_1), F(\boldsymbol{\alpha}_2), \dots, F(\boldsymbol{\alpha}_n))$$

as described in [8]. Adopting a vectorized version of their notation, we define for $\mathbf{r} = (r_1, r_2, \dots, r_m)$ the set

$$\Delta(\mathbf{r}) = \{X^\mathbf{a} \mid \mathbf{a} \in \mathbb{N}^m, 0 \leq a_j < p^{r_j}, j = 1, 2, \dots, m\},$$

where we use the multi-index notation $X^\mathbf{a} = X_1^{a_1} X_2^{a_2} \cdots X_m^{a_m}$. For a subset $L \subseteq \Delta(\mathbf{r})$, define the code

$$C(L) = \text{Span}_{\mathbb{F}_q} \{ \text{ev}(X^\mathbf{a} + I) \mid X^\mathbf{a} \in L \}, \quad (1)$$

which clearly has length n . To describe the distance of $C(L)$, we use the map $\sigma: \Delta(\mathbf{r}) \rightarrow \mathbb{N}$ given by

$$\sigma(X^\mathbf{a}) = \prod_{j=1}^m (p^{r_j} - a_j).$$

Proposition 4. *Let $C(L)$ be defined as in (1). Then $\dim C(L) = |L|$, and*

$$d(C(L)) \geq \min\{\sigma(X^\mathbf{a}) \mid X^\mathbf{a} \in L\} \quad (2)$$

with equality if $X^\mathbf{a} \in L$ implies $X^\mathbf{b} \in L$ for all choices of $b_1 \leq a_1, b_2 \leq a_2, \dots, b_m \leq a_m$.

Proof. The claim about the dimension is for instance shown in the proof of [8; Thm. 16]. The inequality (2) can be proved by using the footprint bound as done in [10; Prop. 1].

To see the equality, write $\mathbb{F}_{p^{r_i}} = \{v_1^{(i)}, v_2^{(i)}, \dots, v_{p^{r_i}}^{(i)}\}$, let $X^\mathbf{a} \in L$, and observe that the expansion of the polynomial

$$f = \prod_{j=1}^m \prod_{i=1}^{a_j} (X_j - v_i^{(j)})$$

contains only monomials $X^\mathbf{b}$ with \mathbf{b} as described in the proposition. This means that $\text{ev}(f + I) \in C(L)$. Moreover, f possesses exactly $\prod_{j=1}^m (p^{r_i} - a_j) = \sigma(X^\mathbf{a})$ non-zeros. \square

This proposition not only allows us to determine the exact minimal distance of the codes considered in the following section, but more importantly it also enables us to determine certain relative distances when combined with the observations in Remark 3.

2.3 Improved codes

The information on the minimal distance provided by σ leads to improved code constructions in a straightforward manner. By defining

$$L(\delta) = \{X^{\mathbf{a}} \in \Delta(\mathbf{r}) \mid \sigma(X^{\mathbf{a}}) \geq \delta\}, \quad (3)$$

the code $C(L(\delta))$ has designed distance δ by Proposition 4. In addition, this is the true minimal distance since $\sigma(X^{\mathbf{b}}) \geq \sigma(X^{\mathbf{a}})$ if $b_1 \leq a_1, b_2 \leq a_2, \dots, b_m \leq a_m$. The dual of $C(L(\delta))$ can be described by studying the map $\mu: \Delta(\mathbf{r}) \rightarrow \mathbb{N}$ defined as

$$\mu(X^{\mathbf{a}}) = \prod_{j=1}^m (a_j + 1).$$

In particular, by letting $L^\perp(\delta) = \{X^{\mathbf{a}} \in \Delta(\mathbf{r}) \mid \mu(X^{\mathbf{a}}) < \delta\}$ we obtain the following result.

Proposition 5. *Let $L(\delta)$ be defined as in (3). Then $C(L(\delta))^\perp = C(L^\perp(\delta))$.*

Proof. First, note that $\sigma(X^{\mathbf{a}}) = \mu(X^{\mathbf{b}})$ for $b_i = p^{r_i} - a_i - 1$. This implies that the number of monomials with a given σ -value δ is exactly the number of monomials with μ -value δ . As a consequence,

$$\begin{aligned} \dim C(L^\perp(\delta)) &= |\{X^{\mathbf{a}} \in \Delta(\mathbf{r}) \mid \sigma(X^{\mathbf{a}}) < \delta\}| \\ &= n - \dim C(L(\delta)) \\ &= \dim C(L(\delta))^\perp. \end{aligned}$$

Hence, it suffices to show that $C(L^\perp(\delta)) \subseteq C(L(\delta))^\perp$, and we do so by proving that the evaluation of any $X^{\mathbf{b}}$ with $\mu(X^{\mathbf{b}}) < \delta$ must be in $C(L(\delta))^\perp$.

Using contraposition, assume that $X^{\mathbf{b}} \notin C(L(\delta))^\perp$. Then some $\text{ev}(X^{\mathbf{a}}) \in C(L(\delta))$ satisfies $\text{ev}(X^{\mathbf{a}}) \cdot \text{ev}(X^{\mathbf{b}}) \neq 0$. As shown in [9; Prop. 1], this happens if and only if¹ $a_i + b_i > 0$ and $a_i + b_i \equiv 0 \pmod{p^{r_i} - 1}$ holds true for each index $i \in \{1, 2, \dots, m\}$. In other words, we have $a_i + b_i = p^{r_i} - 1$ or $a_i + b_i = 2(p^{r_i} - 1)$. In each case, this implies $p^{r_i} - a_i \leq b_i + 1$. In combination with the fact that $\sigma(X^{\mathbf{a}}) \geq \delta$ since $\text{ev}(X^{\mathbf{a}}) \in C(L(\delta))$, we obtain the inequalities

$$\delta \leq \sigma(X^{\mathbf{a}}) = \prod_{i=1}^m (p^{r_i} - a_i) \leq \prod_{i=1}^m (b_i + 1) = \mu(X^{\mathbf{b}}).$$

In conclusion, if $\mu(X^{\mathbf{b}}) < \delta$, we have $\text{ev}(X^{\mathbf{b}}) \in C(L(\delta))^\perp$, which proves the proposition by the observations in the beginning of the proof. \square

¹In their notation, the situation in consideration has $J = \emptyset$ and $p \mid N_j$ for each j

3 Steane-enlargement of improved codes

We are now ready to apply Steane-enlargement to the codes defined in Section 2.3. Our results rely on a simple, but crucial, observation: for each index $i = 1, 2, \dots, m$, $\sigma(\Delta(\mathbf{r}))$ contains an ‘edge’ with values $1, 2, \dots, p^{r_i}$. This is illustrated in Figures 1 and 2. This means that we can easily give a lower bound on the dimension increase when enlarging the code $C(L(\delta))$. To ease the notation in the following, we will order the exponents r_i such that $r_1 \geq r_2 \geq \dots \geq r_m$.

Proposition 6. *Let $q = p^r$, and let $\mathbf{r} \in \mathbb{Z}_+^m$ be a vector such that $r_i \mid r$ for each i and $r_1 \geq r_2 \geq \dots \geq r_m$. Additionally, let $2 < \delta \leq p^{r_2} + 1$, and let K be the largest index such that $\delta - 1 \leq p^{r_K}$. Then if $C(L(\delta))$ is a dual-containing $[n, k]$ code, there exists a quantum error-correcting code with parameters*

$$[[n, \geq 2k - n + K, \geq \delta]]_q. \quad (4)$$

Proof. Write $\mathcal{C} = C(L(\delta))$, and let $\mathcal{C}' = C(L(\delta - 1))$. Since $1 < \delta - 1 \leq p^{r_K}$, the observation at the start of this section implies that there are at least $K \geq 2$ monomials $X^\mathbf{a} \in \Delta(\mathbf{r})$ such that $\sigma(X^\mathbf{a}) = \delta - 1$. Thus, \mathcal{C}' has dimension $k' \geq k + K$. As described in Section 2.3, \mathcal{C} and \mathcal{C}' have minimal distances δ and $\delta - 1$, respectively. Thus the observation in Remark 3 ensures that $d(\mathcal{C}', \mathcal{C}'^\perp) = d(\mathcal{C}') = \delta - 1$, and we obtain

$$\lceil (1 + \frac{1}{q})d(\mathcal{C}') \rceil = \lceil (1 + \frac{1}{q})(\delta - 1) \rceil = \delta,$$

where the last equality stems from the assumption that $\delta - 1 \leq p^{r_2} \leq q$. The claim now follows by applying Theorem 2 to \mathcal{C} and \mathcal{C}' , and by using the bound $d(\mathcal{C}, \mathcal{C}'^\perp) \geq d(\mathcal{C}) = \delta$. \square

A few additional remarks can be made about the Steane-enlargement described in Proposition 4.

9	8	7	6	5	4	3	2	1
18	16	14	12	10	8	6	4	2
27	24	21	18	15	12	9	6	3

Figure 1. The values of $\sigma(\Delta(\mathbf{r}))$ for $p = 3$ and $\mathbf{r} = (2, 1)$. The shaded region shows the edges with values $1, 2, \dots, 9 = p^{r_1}$ and $1, 2, 3 = p^{r_2}$, respectively.

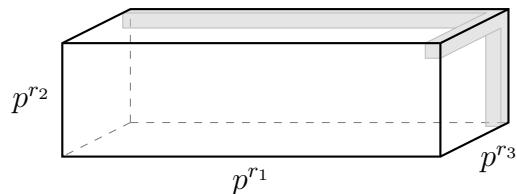


Figure 2. A sketch of $\Delta(\mathbf{r})$ in the case $m = 3$. As in the 2-dimensional case in Figure 1, the shaded region shows the edges where the σ -values are $1, 2, \dots, p^{r_i}$ for each i .

Remark 7. The observation that leads to Proposition 4 does not help in the case $\delta > q + 1$ since we require $\delta \leq p^{r_2} + 1 \leq q + 1$. This does not mean that Steane-enlargement is impossible for $\delta > q + 1$, but merely that we cannot guarantee that it is possible.

Remark 8. The increase in dimension when applying Steane-enlargement to the code $C(L(\delta))$ may be greater than the K specified in Proposition 6 since this K is determined by considering monomials along the ‘edges’ as in Figure 2. There may be several other monomials that have σ -value $\delta - 1$, yielding a quantum error-correcting code with even better parameters. In Section 3.1, we characterize the situations where this may happen, and give an improved bound in such cases.

Before studying the dimension increase more thoroughly, we illustrate Proposition 6 through an example.

Example 1. Let $q = 3^2 = 9$ and $\mathbf{r} = (2, 2, 1)$. The classical code $C(L(4))$ has parameters $[243, 236, 4]_9$, whence the CSS-construction, Theorem 1, gives a $[[243, 229, 4]]_9$ quantum code. Since $\delta - 1 = 3 = p^{r_3}$, Proposition 6 ensures that Steane-enlargement will instead provide a code with parameters $[[243, \geq 232, \geq 4]]_9$. In this case, the true dimension is in fact 232.

Using the same q and \mathbf{r} , the code $C(L(7))$ is a $[243, 221, 7]_9$ classical code, yielding a $[[243, 199, 7]]_9$ quantum code via the CSS-construction. This time, Proposition 6 only guarantees a dimension increase of 2 when applying Steane-enlargement, but the actual parameters of the enlarged code are $[[243, 207, \geq 7]]_9$, meaning that the dimension has been increased by 8.

3.1 Determining the exact dimension increase

As mentioned in Remark 8, the dimension of an enlarged code may be greater than predicted in (4). In this section, we will generalize the map $\tau^{(q)}$ from [4] to provide an algorithm for computing the exact dimension increase when applying Steane-enlargement to the code $C(L(\delta))$. This generalization will also aid in characterizing those values of δ where Proposition 6 underestimates the dimension.

Definition 9. For $s \in \mathbb{Z}_+$ and $\mathbf{r} \in \mathbb{Z}_+^m$, we let $\tau^{(\mathbf{r})}(s)$ denote the number of tuples (d_1, d_2, \dots, d_m) such that $1 \leq d_i \leq p^{r_i}$ for every i , and such that $s = \prod_{i=1}^m d_i$.

Proposition 10. Let s and \mathbf{r} be as in Definition 9, and assume that $r_1 \geq r_2 \geq \dots \geq r_m$. Let K be the largest index such that $s \leq p^{r_K}$. Then if s is...

- ... prime, we have $\tau^{(\mathbf{r})}(s) = K$.
- ... square, we have $\tau^{(\mathbf{r})}(s) \geq K + \binom{K}{2}$.
- ... non-prime and non-square, we have $\tau^{(\mathbf{r})}(s) \geq K^2$.

Proof. Assume first that s is prime. Then any tuple $(d_1, d_2, \dots, d_m) \in \mathbb{Z}_+$ with $s = \prod_{i=1}^m d_i$ must have $d_i = s$ for some i and $d_j = 1$ for $j \neq i$. Hence, in

this case $\tau^{(\mathbf{r})}(s)$ is the number of indices i such that $d_i \leq p^{r_i}$, which is exactly K .

If s is non-prime, there are still K tuples with a single entry greater than 1 as in the prime case. But we may also split s in two factors $s = f_1 f_2$ such that $f_1, f_2 < s \leq p^{r_K}$. Now, for any distinct indices $i_1, i_2 \in \{1, 2, \dots, K\}$, the tuple (d_1, d_2, \dots, d_m) with $d_{i_1} = f_1$, $d_{i_2} = f_2$, and $d_i = 1$ for $i \notin \{i_1, i_2\}$ is one of the tuples counted by $\tau^{(\mathbf{r})}(s)$. The number of ways to choose the indices i_1, i_2 is $K(K - 1)$. If s is not a square number, f_1 and f_2 are distinct, and each of the $K(K - 1)$ choices of i_1, i_2 leads to a distinct tuple. If s is a square, we may have $f_1 = f_2$, and the number of distinct tuples is instead $K(K - 1)/2 = \binom{K}{2}$. In both cases, we obtain the claimed inequality by adding K . \square

Proposition 11. *Let $s \in \mathbb{Z}_+$. Then the number of monomials $X^\mathbf{a} \in \Delta(\mathbf{r})$ that have $\sigma(X^\mathbf{a}) = s$ is $\tau^{(\mathbf{r})}(s)$.*

Proof. We have $\sigma(X^\mathbf{a}) = s$ if and only if $\prod_{i=1}^m (p^{r_i} - a_i) = s$. Since $0 \leq a_i < p^{r_i}$, this is equivalent to $\prod_{i=1}^m d_i = s$ for $1 \leq d_i \leq p^{r_i}$, proving the proposition. \square

Combining Propositions 10 and 11, we obtain the following immediate corollary.

Corollary 12. *Let q , \mathbf{r} , and δ be as in Proposition 6. Then (4) gives the true dimension if and only if $\delta - 1$ is a prime number. If $\delta - 1$ is not a prime, the bound on the dimension may be increased by $\binom{K}{2}$ if $\delta - 1$ is a square number and by $K(K - 1)$ otherwise.*

Example 2. We now return to the codes in Example 1. In the case of $C(L(4))$, we saw that Proposition 6 gave the true minimal distance. Having established Corollary 12, we now know that this is no coincidence since $\delta - 1 = 3$ is a prime number.

For the code $C(L(7))$, $\delta - 1 = 6$ is neither prime nor square. Consequently, Corollary 12 tells us that the dimension must increase by at least $K^2 = 2^2 = 4$, which is 2 more than the bound from Proposition 6. Both bounds are, however, still smaller than the true value of 8.

Since it may not be obvious how to compute $\tau^{(\mathbf{r})}$, we give the following recursive algorithm. Its correctness can be shown by a simple inductive argument.

Algorithm 1. On input $\mathbf{r} = (r_1, r_2, \dots, r_m)$ and $s \in \mathbb{Z}_+$, this algorithm computes $\tau^{(\mathbf{r})}(s)$:

1. Check if \mathbf{r} is a single value r_1 . If this is the case, return 1 if $s \leq r_1$, and 0 otherwise.
2. Initialize a counter variable $c := 0$.
3. For each integer $d \in \{1, 2, \dots, p^{r_1}\}$ with $d | s$, do the following:
 - Let $\mathbf{r}' = (r_2, r_3, \dots, r_m)$, and compute $\tau^{(\mathbf{r}')}(s/d)$.
 - Update c to be $c := c + \tau^{(\mathbf{r}')}(s/d)$.
4. Return c .

Since the number of d 's considered in Algorithm 1 is at most $\prod_{i=1}^{m-1} p^{r_i} = n/p^{r_m}$, the total number of operations is $\mathcal{O}(n/p^{r_m})$. This is a factor p^{r_m} better than considering all $X^{\mathbf{a}} \in \Delta(\mathbf{r})$ and counting the ones with $\sigma(X^{\mathbf{a}}) = s$. We collect these observations on Algorithm 1 and its relation to Proposition 6 in the following proposition.

Proposition 13. *Let q , \mathbf{r} , and δ be as in Proposition 6. Then the true dimension of the quantum code in (4) is $2k - n + \tau^{(\mathbf{r})}(\delta)$. Furthermore, Algorithm 1 correctly computes $\tau^{(\mathbf{r})}(\delta)$ in $\mathcal{O}(n/p^{r_m})$ operations, where $n = \prod_{i=1}^m p^{r_i}$.*

3.2 Examples of parameters

To conclude our exposition, we give concrete parameters of Steane-enlarged codes in several examples. We then compare the parameters of these codes to those of other known constructions and bounds. For each code presented here, we will compare it to the Gilbert-Varshamov bound from [6].

Theorem 14. *Let $n > k \geq 2$ with $n \equiv k \pmod{2}$, and let $d \geq 2$. Then there exists a pure stabilizer quantum code $[[n, k, d]]_q$ if the inequality*

$$\sum_{i=1}^{d-1} (q^2 - 1)^i \binom{n}{i} < q^{n-k+2} - 1 \quad (5)$$

is satisfied.

In the same way as [23], we will use the notation $[[n, k, d]]_q^\ddagger$ in the following to indicate that the parameters (n, k, d) exceed the Gilbert-Varshamov bound – i.e. that (5) is not satisfied – and we will write $[[n, k, d]]_q^\dagger$ if (n, k, d) satisfies (5), but $(n, k, d+1)$ does not. This is only possible for $n \equiv k \pmod{2}$, which is always the case for CSS-codes from dual-containing codes, but not necessarily for Steane-enlarged codes. Thus, for code parameters (n, k, d) with $n \not\equiv k \pmod{2}$, we will use the same notation, albeit with the bound applied to the parameters $(n, k-1, d)$.

Remark 15. *There is another bound, [13; Cor. 4.3], which covers all values of n and k . For the parameters presented in the current work, however, that bound is weaker than (5), and several of the codes in the examples below exceed [13; Cor. 4.3] but not Theorem 14. For this reason, we shall use Theorem 14 throughout.*

In addition to the Gilbert-Varshamov bound, we will refer to the quantum Singleton bound in some cases. This bound is

$$2d \leq n - k + 2, \quad (6)$$

and its proof can be found in [15, 24].

Example 3. This is a continuation of Examples 1 and 2. When compared with the Gilbert-Varshamov bound, Theorem 14, the CSS-code with parameters $[[243, 229, 4]]_9^\dagger$ and the Steane-enlarged code with parameters $[[243, 232, 4]]_9^\dagger$ meet the bound, whereas the two codes of minimal distance 7 neither meet nor exceed the bound.

Example 4. Consider $q = 3^2 = 9$ and $\mathbf{r} = (2, 1)$ as in Figure 1. Here, Proposition 6 guarantees that we can enlarge the CSS-codes $[[27, 21, 3]]_9^\dagger$ and $[[27, 17, 4]]_9^\dagger$ to codes of parameters $[[27, 23, \geq 3]]_9^\dagger$ and $[[27, 19, \geq 4]]_9^\dagger$, respectively. Furthermore, Corollary 12 ensures that these are the true dimensions. In fact, the code $[[27, 23, 3]]_9^\dagger$ is optimal since it meets the Singleton-bound (6).

There are two additional Steane-enlarged codes that are not captured by Proposition 6. These are $[[27, 13, 5]]_9$ enlarged to $[[27, 15, \geq 5]]_9^\dagger$, and $[[27, 5, 7]]_9$ enlarged to $[[27, 8, \geq 7]]_9$, where the increases in dimension have been computed using Algorithm 1. In both cases, the technique in Proposition 6 fails because $\delta > 4 = p^{r_2} + 1$.

Initially, we compare the parameters that can be achieved by using the CSS-construction, Theorem 1, and those from Steane-enlargement, Theorem 2. At the same time, the difference in dimension between these two constructions is compared with the bounds that were given in Propositions 6 and Corollary 12.

Example 5. In Tables 1–4, we list parameters of quantum codes in various cases where Proposition 6 guarantees that enlargement is possible. The tables contain both the original CSS-code and its Steane-enlarged code along with the predicted dimension increases from Proposition 6 and Corollary 12.

In these tables, the first column shows the parameters of quantum codes obtained by applying Theorem 1 to dual-containing codes of the form $\mathcal{C} = C(L(\delta))$. The second column shows the results of enlarging the codes in the first column using $\mathcal{C}' = C(L(\delta - 1))$ in Theorem 2. Both of these columns contain the true dimensions of the codes, and the three final columns highlight the bounds on the dimension increase provided in Proposition 6, Corollary 12, and Proposition 13. More precisely, the third column gives the dimension increase guaranteed by Proposition 6, and the fourth shows the bound provided by Corollary 12. Any number marked with an asterisk is known to be the true value since $\delta - 1$ is a prime. The final column shows the actual increase as computed by Algorithm 1.

Studying the tables, it is evident that Corollary 12 provides a better bound for the dimension than Proposition 6, but that the actual increase in dimension may be significantly higher. In any case, however, Proposition 13 ensures that the true increase can be computed using Algorithm 1.

Having compared the two methods considered in this work, we now turn our attention to other constructions of quantum codes. Thus, Examples 6–9 illustrate how the parameters given in Tables 1–4 compare against existing parameters in the literature. First, we consider the codes obtained from cyclic codes in [16, 17].

Construction		Dimension increase		
Th.m 1	Thm. 2	Prop. 6	Cor. 12	Prop. 13
$[[729, 721, 3]]_9^\dagger$	$[[729, 724, 3]]_9^\ddagger$	3	3*	3
$[[729, 715, 4]]_9^\dagger$	$[[729, 718, 4]]_9^\ddagger$	3	3*	3
$[[729, 703, 5]]_9$	$[[729, 709, 5]]_9^\dagger$	3	6	6
$[[729, 697, 6]]_9$	$[[729, 700, 6]]_9$	3	3*	3
$[[729, 679, 7]]_9$	$[[729, 688, 7]]_9$	3	9	9
$[[729, 673, 8]]_9$	$[[729, 676, 8]]_9$	3	3*	3
$[[729, 653, 9]]_9$	$[[729, 663, 9]]_9$	3	9	10
$[[729, 641, 10]]_9$	$[[729, 647, 10]]_9$	3	6	6

Table 1. Code parameters from the Cartesian product with $q = 3^2 = 9$ and $\mathbf{r} = (2, 2, 2)$. The first and second columns contain CSS-codes and Steane-enlarged codes, respectively. The third and fourth columns contain lower bounds on the dimension increase with * denoting a value that is known to be the true value. The final column contains the true value as computed from Proposition 13.

Construction		Dimension increase		
Thm. 1	Thm. 2	Prop. 6	Cor. 12	Prop. 13
$[[64, 58, 3]]_8^\dagger$	$[[64, 60, 3]]_8^\ddagger$	2	2*	2
$[[64, 54, 4]]_8^\dagger$	$[[64, 56, 4]]_8^\ddagger$	2	2*	2
$[[64, 48, 5]]_8$	$[[64, 51, 5]]_8^\dagger$	2	3	3
$[[64, 44, 6]]_8$	$[[64, 46, 6]]_8^\dagger$	2	2*	2
$[[64, 36, 7]]_8$	$[[64, 40, 7]]_8$	2	4	4
$[[64, 32, 8]]_8$	$[[64, 34, 8]]_8$	2	2*	2

Table 2. Code parameters from the Cartesian product with $q = 2^3 = 8$ and $\mathbf{r} = (3, 3)$. The first and second columns contain CSS-codes and Steane-enlarged codes, respectively. The third and fourth columns contain lower bounds on the dimension increase with * denoting a value that is known to be the true value. The final column contains the true value as computed from Proposition 13.

Example 6. For $\delta < 8$ the parameters of the codes in Table 1 surpass those presented in [17; Tables 1 and 3]. There, codes with parameters $[[728, 714, \geq 3]]_9$, $[[728, 704, \geq 4]]_9$, $[[728, 690, \geq 6]]_9$, $[[728, 679, \geq 7]]_9$, and $[[728, 678, \geq 8]]_9$ are given. Apart from the one with $\delta = 8$, the Steane-enlarged codes in Table 1 are one symbol longer, but have a dimension that is at least 9 higher than the corresponding code in [17]. Likewise, the codes in Table 2 have better parameters than those in [16; Tables 1 and 2] whenever $\delta \leq 6$. More concretely, [16] lists quantum codes with parameters $[[63, 57, \geq 3]]_8^\dagger$, $[[63, 53, \geq 4]]_8^\dagger$, $[[63, 49, \geq 5]]_8^\dagger$, and $[[63, 45, \geq 6]]_8^\dagger$. For larger values of δ , however, [16] outperforms the codes in Table 2.

All the codes in Tables 1 and 2 have $q = p^r$ and $r_i = r$, which are in fact hyperbolic codes. It seems to be a general pattern for such codes, that the Steane-enlargements with small distances outperform the codes in [16, 17], but that this relation is reversed for larger distances.

The codes in Tables 3 and 4 have parameters that cannot be achieved using the method from [16, 17] since those codes all have lengths $q^m - 1$ for some

$m \geq 2$, where q is the field size.

As a second comparison, we consider the parameters of quantum twisted codes that have been compiled in [5].

Example 7. *Based on [1], the webpage [5] contains lists of quantum code parameters derived from twisted codes. For instance, the list for $q = 9$ contains the codes $[[730, 718, 3]]_9^\dagger$, $[[730, 712, 4]]_9$, $[[730, 706, 5]]_9$, and $[[730, 700, 6]]_9$. The comparable codes in Table 1 are both one symbol shorter and have higher dimension. It may also be noted that two of the codes in Table 1 exceed the Gilbert-Varshamov bound, while this is not the case for any of the codes listed in this example.*

The codes $[[730, 694, 7]]_9$, $[[730, 688, 8]]_9$, and $[[730, 682, 9]]_9$ from [5] have better parameters than those in Table 1, but they are included in the table for completeness.

A previous version of this paper contained an example of quantum codes over \mathbb{F}_5 of length 625. As pointed out by a reviewer, however, the parameters of those codes did not exceed the parameters of the codes listed in [5].

Next, we compare the quantum codes derived from the Suzuki curve in [23] to the Steane-enlarged codes presented in Table 2.

Example 8. *The codes in Table 2 have favourable parameters compared to those given in [23; Ex. 5], which are defined from the Suzuki curve. Specifically, the codes in [23] have parameters $[[64, 54, 3]]_8$, $[[64, 52, 4]]_8^\dagger$, $[[64, 42, 5]]_8$, $[[64, 40, 6]]_8$, $[[64, 38, 7]]_8$, and $[[64, 36, 8]]_8$, which are all worse than those in Table 2 except the one with distance 8. As a final remark, the code with parameters $[[64, 60, 3]]_8^\ddagger$ meets the quantum Singleton bound (6).*

As a final example, we consider the monomial Cartesian codes from [21] that are guaranteed to be MDS.

Example 9. *Among the codes presented in this Tables 1–4, two were MDS-codes: $[[27, 23, 3]]_9^\ddagger$ and $[[64, 60, 3]]_8^\ddagger$. From recent work [21; Cor. 3.10] the same lengths, dimensions, and minimal distances can be achieved, but the field size is much larger. In particular, they require $q > n$ so the corresponding field sizes are at least 29 and 67, respectively.*

4 Conclusion

In this work, we showed how Steane-enlargement can be applied to codes defined from Cartesian product point sets. Concretely, Proposition 6 contains a simple condition that, when satisfied, guarantees that Steane-enlargement produces a higher dimension when compared to the CSS-construction without reducing the distance. Furthermore, we gave an improved, but still easily computable, bound on the dimension increase during this enlargement, and provided an algorithm to compute the true value.

Comparing the resulting quantum code parameters to existing constructions revealed several cases where the Steane-enlarged codes from Cartesian

Construction		Dimension increase		
Thm. 1	Thm. 2	Prop. 6	Cor. 12	Prop. 13
$[[1024, 1016, 3]]_8^\dagger$	$[[1024, 1019, 3]]_8^\ddagger$	3	3*	3
$[[1024, 1010, 4]]_8^\dagger$	$[[1024, 1013, 4]]_8^\ddagger$	3	3*	3
$[[1024, 998, 5]]_8$	$[[1024, 1004, 5]]_8$	3	6	6
$[[1024, 994, 6]]_8$	$[[1024, 996, 6]]_8$	2	2*	2
$[[1024, 978, 7]]_8$	$[[1024, 986, 7]]_8$	2	4	8
$[[1024, 974, 8]]_8$	$[[1024, 976, 8]]_8$	2	2*	2
$[[1024, 956, 9]]_8$	$[[1024, 965, 9]]_8$	2	4	9
$[[1024, 946, 10]]_8$	$[[1024, 951, 10]]_8$	2	3	5
$[[1024, 934, 11]]_8$	$[[1024, 940, 11]]_8$	2	4	6
$[[1024, 930, 12]]_8$	$[[1024, 932, 12]]_8$	2	2*	2
$[[1024, 900, 13]]_8$	$[[1024, 915, 13]]_8$	2	4	15
$[[1024, 896, 14]]_8$	$[[1024, 898, 14]]_8$	2	2*	2
$[[1024, 884, 15]]_8$	$[[1024, 890, 15]]_8$	2	4	6
$[[1024, 872, 16]]_8$	$[[1024, 878, 16]]_8$	2	4	6
$[[1024, 848, 17]]_8$	$[[1024, 860, 17]]_8$	2	3	12

Table 3. Code parameters from the Cartesian product with $q = 2^4 = 16$ and $\mathbf{r} = (4, 4, 2)$. The first and second columns contain CSS-codes and Steane-enlarged codes, respectively. The third and fourth columns contain lower bounds on the dimension increase with * denoting a value that is known to be the true value. The final column contains the true value as computed from Proposition 13.

Construction		Dimension increase		
Thm. 1	Thm. 2	Prop. 6	Cor. 12	Prop. 13
$[[1024, 1014, 3]]_8^\dagger$	$[[1024, 1018, 3]]_8^\ddagger$	4	4*	4
$[[1024, 1008, 4]]_8^\dagger$	$[[1024, 1011, 4]]_8^\ddagger$	3	3*	3
$[[1024, 990, 5]]_8$	$[[1024, 999, 5]]_8$	3	6	9
$[[1024, 984, 6]]_8$	$[[1024, 987, 6]]_8$	3	3*	3
$[[1024, 960, 7]]_8$	$[[1024, 972, 7]]_8$	3	9	12
$[[1024, 954, 8]]_8$	$[[1024, 957, 8]]_8$	3	3*	3
$[[1024, 922, 9]]_8$	$[[1024, 938, 9]]_8$	3	9	16

Table 4. Code parameters from the Cartesian product with $q = 2^3 = 8$ and $\mathbf{r} = (3, 3, 3, 1)$. The first and second columns contain CSS-codes and Steane-enlarged codes, respectively. The third and fourth columns contain lower bounds on the dimension increase with * denoting a value that is known to be the true value. The final column contains the true value as computed from Proposition 13.

product point sets provide better parameters than comparable constructions. Such improvements were especially common for small designed distances, where the Steane-enlarged codes also exceed the Gilbert-Varshamov bound in many cases.

This work and the work [4] shows that Steane-enlargement can provide quantum codes with good parameters when the underlying classical codes are defined from relatively simple point sets. Thus, it is natural to ask whether other, more complicated point sets lead to good parameters in the same way. We leave this question for future research.

Acknowledgements

The authors express their gratitude to Diego Ruano for delightful discussions in relation to this work. In addition, the authors thank the anonymous reviewers for their comments, which led to a better manuscript.

References

- [1] J. Bierbrauer and Y. Edel. “Quantum twisted codes”. In: *J. Comb. Des.* 8.3 (2000), pp. 174–188. DOI: 10.1002/(SICI)1520-6610(2000)8:3<174::AID-JCD3>3.0.CO;2-T.
- [2] A. R. Calderbank, E. M. Rains, P. M. Shor and N. J. A. Sloane. “Quantum error correction via codes over GF(4)”. In: *IEEE Trans. Inf. Theory* 44.4 (1998), pp. 1369–1387. DOI: 10.1109/18.681315.
- [3] A. R. Calderbank and P. W. Shor. “Good quantum error-correcting codes exist”. In: *Phys. Rev. A* 54 (2 1996), pp. 1098–1105. DOI: 10.1103/PhysRevA.54.1098.
- [4] R. B. Christensen and O. Geil. “Steane-enlargement of quantum codes from the Hermitian function field”. In: *Des. Codes Cryptogr.* (2020). To appear. DOI: 10.1007/s10623-019-00709-7.
- [5] Y. Edel. *Some good quantum twisted codes*. Accessed on 13th November 2019. URL: <https://www.mathi.uni-heidelberg.de/~yves/Matritzen/QTBCN/QTBCNIndex.html>.
- [6] K. Feng and Z. Ma. “A finite Gilbert-Varshamov bound for pure stabilizer quantum codes”. In: *IEEE Trans. Inf. Theory* 50.12 (2004), pp. 3323–3325. ISSN: 0018-9448. DOI: 10.1109/TIT.2004.838088.
- [7] C. Galindo, F. Hernando and D. Ruano. “Classical and Quantum Evaluation Codes at the Trace Roots”. In: *IEEE Trans. Inf. Theory* 65.4 (2019), pp. 2593–2602. DOI: 10.1109/TIT.2018.2868442.
- [8] C. Galindo, O. Geil, F. Hernando and D. Ruano. “Improved Constructions of Nested Code Pairs”. In: *IEEE Trans. Inf. Theory* 64.4 (2018), pp. 2444–2459. DOI: 10.1109/TIT.2017.2755682.
- [9] C. Galindo, F. Hernando and D. Ruano. “Stabilizer quantum codes from J -affine variety codes and a new Steane-like enlargement”. In: *Quantum Inf. Process.* 14.9 (2015), pp. 3211–3231. ISSN: 1573-1332. DOI: 10.1007/s11128-015-1057-2.

- [10] O. Geil and T. Høholdt. “On Hyperbolic Codes”. In: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 14th International Symposium, AAECC-14, Melbourne, Australia November 26-30, 2001, Proceedings*. 2001, pp. 159–171. DOI: 10.1007/3-540-45624-4_17.
- [11] M. Hamada. “Concatenated Quantum Codes Constructible in Polynomial Time: Efficient Decoding and Error Correction”. In: *IEEE Trans. Inf. Theory* 54.12 (2008), pp. 5689–5704. ISSN: 0018-9448. DOI: 10.1109/TIT.2008.2006416.
- [12] L. Ioffe and M. Mézard. “Asymmetric quantum error-correcting codes”. In: *Phys. Rev. A* 75 (3 2007), p. 032345. DOI: 10.1103/PhysRevA.75.032345.
- [13] L. Jin and C. Xing. “Quantum Gilbert-Varshamov bound through symplectic self-orthogonal codes”. In: *2011 IEEE International Symposium on Information Theory Proceedings*. 2011, pp. 455–458. DOI: 10.1109/ISIT.2011.6034167.
- [14] A. Ketkar, A. Klappenecker, S. Kumar and P. K. Sarvepalli. “Nonbinary Stabilizer Codes Over Finite Fields”. In: *IEEE Trans. Inf. Theory* 52.11 (2006), pp. 4892–4914. DOI: 10.1109/TIT.2006.883612.
- [15] E. Knill and R. Laflamme. “Theory of quantum error-correcting codes”. In: *Phys. Rev. A* 55 (2 1997), pp. 900–911. DOI: 10.1103/PhysRevA.55.900.
- [16] G. G. La Guardia and M. M. S. Alves. “On cyclotomic cosets and code constructions”. In: *Linear Algebra Appl.* 488 (2016), pp. 302 – 319. ISSN: 0024-3795. DOI: 10.1016/j.laa.2015.09.034.
- [17] G. G. La Guardia and R. Palazzo. “Constructions of new families of nonbinary CSS codes”. In: *Discrete Mathematics* 310.21 (2010), pp. 2935 – 2945. ISSN: 0012-365X. DOI: 10.1016/j.disc.2010.06.043.
- [18] G. G. La Guardia and F. R. F. Pereira. “Good and asymptotically good quantum codes derived from algebraic geometry”. In: *Quantum Inf. Process.* 16.6 (2017), p. 165. ISSN: 1573-1332. DOI: 10.1007/s11128-017-1618-7.
- [19] R. Li, J. Wang, Y. Liu and G. Guo. “New quantum constacyclic codes”. In: *Quantum Inf. Process.* 18.5 (2019), p. 127. ISSN: 1573-1332. DOI: 10.1007/s11128-019-2242-5.
- [20] S. Ling, J. Luo and C. Xing. “Generalization of Steane’s enlargement construction of quantum codes and applications”. In: *IEEE Trans. Inf. Theory* 56.8 (2010), pp. 4080–4084. DOI: 10.1109/TIT.2010.2050828.
- [21] H. H. López, G. L. Matthews and I. Soprunov. “Monomial-Cartesian codes and their duals, with applications to LCD codes, quantum codes, and locally recoverable codes”. In: *CoRR* abs/1907.11812 (2019). arXiv: 1907.11812. URL: <http://arxiv.org/abs/1907.11812>.
- [22] J. Lv, R. Li and J. Wang. “New Binary Quantum Codes Derived From One-Generator Quasi-Cyclic Codes”. In: *IEEE Access* 7 (2019), pp. 85782–85785. DOI: 10.1109/ACCESS.2019.2923800.
- [23] C. Munuera, W. Tenório and F. Torres. “Quantum error-correcting codes from algebraic geometry codes of Castle type”. In: *Quantum Inf. Process.* 15.10 (2016), pp. 4071–4088. ISSN: 1573-1332. DOI: 10.1007/s11128-016-1378-9.

- [24] E. M. Rains. “Nonbinary quantum codes”. In: *IEEE Transactions on Information Theory* 45.6 (1999), pp. 1827–1832. ISSN: 0018-9448. DOI: 10.1109/18.782103.
- [25] X. Shi, Q. Yue and Y. Wu. “New quantum MDS codes with large minimum distance and short length from generalized Reed–Solomon codes”. In: *Discrete Mathematics* 342.7 (2019), pp. 1989 –2001. ISSN: 0012-365X. DOI: <https://doi.org/10.1016/j.disc.2019.03.019>.
- [26] P. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*. Los Alamitos, CA, USA: IEEE Computer Society, 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.
- [27] P. W. Shor. “Scheme for reducing decoherence in quantum computer memory”. In: *Phys. Rev. A* 52 (4 1995), R2493–R2496. DOI: 10.1103/PhysRevA.52.R2493.
- [28] D. Simon. “On the power of quantum computation”. In: *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*. Los Alamitos, CA, USA: IEEE Computer Society, 1994, pp. 116–123. DOI: 10.1109/SFCS.1994.365701.
- [29] A. Steane. “Multiple-Particle Interference and Quantum Error Correction”. In: *Proc. R. Soc. Lond. Ser. A: Math. Phys. Eng. Sci.* 452.1954 (1996), pp. 2551–2577. ISSN: 13645021.
- [30] A. M. Steane. “Enlargement of Calderbank-Shor-Steane quantum codes”. In: *IEEE Trans. Inf. Theory* 45.7 (1999), pp. 2492–2495. DOI: 10.1109/18.796388.
- [31] F. Tian and S. Zhu. “Some new quantum MDS codes from generalized Reed–Solomon codes”. In: *Discrete Mathematics* 342.12 (2019), p. 111593. ISSN: 0012-365X. DOI: <https://doi.org/10.1016/j.disc.2019.07.009>.