Computational and Applied Mathematics (2023) 42:363
https://doi.org/10.1007/s40314-023-02506-4

Entanglement-assisted quantum error-correcting codes from subfield subcodes of projective Reed–Solomon codes

Philippe Gimenez[1] · **Diego Ruano**[1] · **Rodrigo San-José**[1]

Received: 11 April 2023 / Revised: 20 October 2023 / Accepted: 22 October 2023 /
Published online: 25 November 2023

Abstract
We study the subfield subcodes of projective Reed–Solomon codes and their duals: we provide bases for these codes and estimate their parameters. With this knowledge, we can construct symmetric and asymmetric entanglement-assisted quantum error-correcting codes, which in many cases have new or better parameters than the ones available in the literature.

Keywords Asymmetric quantum codes · EAQECC · Evaluation codes · Linear codes · Projective Reed–Solomon codes · Subfield subcodes · Trace

Mathematics Subject Classification 81P70 · 94B05 · 13P25

Communicated by Gaojun Luo.

This work was supported in part by the following grants: Grant TED2021-130358B-I00 funded by MCIN/AEI/10.13039/501100011033 and by the "European Union NextGenerationEU/ PRTR", Grants PID2022-138906NB-C21 and PID2022-137283NB-C22 funded by MCIN/AEI/10.13039/501100011033 and by ERDF "A way of making Europe", FPU20/01311 funded by the Spanish Ministry of Universities, and by QCAYLE project funded by MCIN, the European Union NextGenerationEU (PRTR C17.I1) and Junta de Castilla y León.

✉ Rodrigo San-José
rodrigo.san-jose@uva.es

Philippe Gimenez
pgimenez@uva.es

Diego Ruano
diego.ruano@uva.es

[1] IMUVA-Mathematics Research Institute, Universidad de Valladolid, 47011 Valladolid, Spain

1 Introduction

The subfield subcode of a linear code $C \subset \mathbb{F}_{q^s}^n$, with $s \geq 1$, is the linear code $C \cap \mathbb{F}_q^n$. Considering subfield subcodes is a standard technique for constructing long linear codes over a small finite field. For instance, BCH codes are obtained in this way. They can be regarded as subfield subcodes of Reed–Solomon codes and their duals (Bierbrauer 2002). In this work, we study subfield subcodes of projective Reed–Solomon codes.

Reed–Solomon codes are constructed by evaluating one-variable polynomials at points of the affine line. They have optimal parameters, although they cannot be defined over a small finite field. Projective Reed–Solomon codes are constructed by evaluating two-variable homogeneous polynomials at points of the projective line. When one evaluates at all the points they are commonly called doubly extended Reed–Solomon codes. Subfield subcodes of projective Reed–Solomon codes, when one evaluates at all the points of the projective line, were studied in Bierbrauer and Edel (1997).

In this work, we consider a more general setting: we may evaluate at fewer points to define a projective Reed–Solomon code and then compute its subfield subcode. We provide bases for both the subfield subcodes of projective Reed–Solomon codes and their duals and, thus, a formula for their dimension. For the dual code, we use Delsarte's Theorem 4.1, for which we need to study first the metric structure of the codes we are considering. We also study the vanishing ideal of the points in which we evaluate, which allows us to discuss linear independence between the traces that arise when using Delsarte's Theorem. Moreover, we estimate the minimum distance for both primary and dual codes. For the primary code we simply use the bound given by the projective Reed–Solomon code, and for the dual one we use a BCH-type bound.

Reed–Solomon and BCH codes have been extensively used to construct quantum codes using the CSS construction, see, for instance, (Bierbrauer and Edel 2000; Galindo et al. 2021; La Guardia 2020). It is, therefore, natural to consider subfield subcodes of projective Reed–Solomon for constructing quantum codes.

The construction of quantum computers has important consequences because of their computing capabilities. Despite the fact that quantum mechanical systems are sensitive to disturbances and arbitrary quantum states cannot be replicated, error correction is possible. Quantum error-correcting codes are designed for protecting quantum information from quantum noise and particularly decoherence. An important class of quantum error-correcting codes are stabilizer codes; they can be derived from classical ones using self-orthogonal codes for the symplectic product (Calderbank and Shor 1996). One can also consider the Euclidean and the Hermitian inner product, and we will call the resulting quantum error-correcting codes QECCs. Entanglement-assisted quantum error-correcting codes (EAQECCs) constitute an extension of quantum codes. EAQECCs make use of pre-existing entanglement between transmitter and receiver to correct more errors (Brun et al. 2006; Galindo et al. 2019b). One virtue of this class of codes is that one can get a quantum code from any linear code without any assumption on dual containment. The main additional task for EAQECCs is to give formulae to obtain the optimal number c of maximally entangled pairs of qudits needed.

Moreover, both for QECCs and EAQECCs, one can consider the asymmetric case (Galindo et al. 2020; Ioffe and Mézard 2007; Sarvepalli et al. 2009). Asymmetric quantum codes have a different error-correction capability for phase-shift and qudit-flip errors. These two types of errors are not equally likely, and it is desirable to construct quantum codes with a higher correction capability for phase-shift errors (Ioffe and Mézard 2007).

In this work, we provide EAQECCs with excellent parameters coming from different constructions. In the Euclidean case, we are able to obtain both symmetric and asymmetric EAQECCs with excellent parameters from subfield subcodes of projective Reed–Solomon codes. A key fact for the construction of these codes and the computation of their parameters is the knowledge of the parameters and structure of both the primary and dual codes. We also obtain QECCs, i.e. EAQECCs without entanglement assistance, from subfield subcodes of projective Reed–Solomon codes in some cases. By considering the Hermitian inner product we are also able to obtain codes with excellent parameters. In fact, we produce new parameters according to Grassl (2007). Furthermore, as we are giving several different constructions using subfield subcodes of projective Reed–Solomon codes, this contributes to expanding the known constellation of parameters for EAQECC.

Finally, we consider the codes in Galindo et al. (2019c), Reed–Solomon, and BCH codes obtained by evaluating at the roots of a trace function. We construct the projective version of the codes in Galindo et al. (2019c), that is, the subfield subcodes of projective Reed–Solomon codes evaluating at the roots of a trace function and the point at infinity. This allows us to give classical linear codes which are record in Grassl (2007), and new EAQECCs.

Our results can be summarized as follows.

- We consider projective Reed–Solomon codes over the zero locus of $x^N - x$ (and the point at infinity), where we evaluate an arbitrary set of monomials. We obtain bases for the subfield subcodes of these codes in Theorem 3.4.
- When $p \mid N$, bases for the duals of the subfield subcodes are obtained in Theorem 4.14.
- Considering sets of monomials whose exponents are a union of consecutive cyclotomic sets and the next minimal element, we obtain EAQECCs with entanglement parameter $c \leq 1$ in Theorems 5.5 and 5.15. Some of the resulting codes improve the table for EAQECCs from Grassl (2007).
- Assuming $p \mid N$, by considering the sets of monomials $\{0, 1, \ldots, d_i\}$, for some $1 \leq d_1, d_2 \leq N-1$, we obtain asymmetric EAQECCs with entanglement parameter $c = 1$, which compare favorably with the current literature.
- By evaluating in the zeroes of the trace function, plus the point at infinity, and evaluating monomials whose exponents are a union of consecutive cyclotomic sets and the next minimal element, we obtain linear codes with good parameters in Theorem 6.4, some of which improve the best known parameters in Grassl (2007), see Example 6.5. Moreover, we obtain EAQECCs with good parameters and entanglement parameter $c \leq 1$ in Theorem 6.6.

2 Preliminaries

We consider a finite field $\mathbb{F}_q$ of q elements with characteristic p, and its degree s extension $\mathbb{F}_{q^s}$, with $s \geq 1$. We consider the affine space $\mathbb{A}^1$ over $\mathbb{F}_{q^s}$ and the polynomial ring $R = \mathbb{F}_{q^s}[x]$. We choose a set of elements $Y = \{Q_1, \ldots, Q_n\} \subset \mathbb{A}^1$ and its vanishing ideal $I(Y) = \langle \prod_{i=1}^{n}(x - Q_i) \rangle$, where we are regarding the points of $\mathbb{A}^1$ as elements in $\mathbb{F}_{q^s}$. We define the following evaluation map:

$$\mathrm{ev}_Y : R/I(Y) \to \mathbb{F}_{q^s}^n, \quad f \mapsto (f(Q_1), \ldots, f(Q_n))_{Q_i \in Y}.$$

where we denote a polynomial and its class in the quotient ring $R/I(Y)$ in the same way. Let Δ be a subset of $\{0, 1, \ldots, n-1\}$. Then, the Reed–Solomon code associated to Δ and Y, denoted by $\mathrm{RS}(Y, \Delta)$, is the code generated by

$$\{\mathrm{ev}_Y(x^i) \mid i \in \Delta\}.$$

The usual choices are $\Delta = \{0, 1 \ldots, d\}$ and $Y = \mathbb{F}_{q^s}^* = \mathbb{F}_{q^s} \setminus \{0\}$, which give a Reed–Solomon code with parameters $[q^s - 1, d + 1, q^s - d - 1]$. This code can be extended by evaluating at 0 as well, obtaining a code with parameters $[q^s, d + 1, q^s - d]$.

Let $N > 1$ be such that $N - 1 \mid q^s - 1$. We can consider the set of points $Y_N^* = \{Q_1, \ldots, Q_N\}$ given by the zero locus of $I(Y_N^*) = \langle x^{N-1} - 1 \rangle$. In this case, Y_N^* forms a multiplicative subgroup of $\mathbb{F}_{q^s}^*$ and it is already known how to obtain bases for its subfield subcodes (see, for example, Hattori et al. 1998; Hernando et al. 2010). Moreover, BCH codes can be defined as the duals of the subfield subcodes of Reed–Solomon codes when we evaluate in a subgroup Y_N^* (Bierbrauer 2002). Indeed, let $\alpha \in \mathbb{F}_{q^s}$ be a primitive $(N - 1)$th root of unity. C is a BCH code of designed distance δ if it has as generator polynomial the least common multiple of the minimal polynomials of the $\delta - 1$ consecutive elements $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$, with $b \geq 1$, which implies that C is formed by the vectors over $\mathbb{F}_q^{N-1}$ that are orthogonal to the rows of the matrix:

$$H = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(N-2)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(N-2)(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \cdots & \alpha^{(N-2)(b+\delta-2)} \end{pmatrix}. \tag{1}$$

However, this is precisely the generator matrix of the Reed Solomon code over $\mathbb{F}_{q^s}$ with $\Delta = \{b, b + 1, \ldots, b + \delta - 2\}$ and $Y = Y_N^*$. Furthermore, the vectors in $\mathbb{F}_q^{N-1}$ that are orthogonal to the rows of H are precisely the vectors of the subfield subcode of the dual code of this Reed–Solomon code, which is, therefore, equal to the aforementioned BCH code. In this situation, we say that H is a *pseudo parity check-matrix* for C.

Because of the previous discussion, throughout this work we will focus on evaluating in subgroups of the form Y_N^* unless stated otherwise. As before, we can also include the evaluation of 0, which corresponds to considering instead the set Y_N, the zero locus of $I(Y_N) = \langle x^N - x \rangle$. For the Reed–Solomon codes obtained by evaluating the associated monomials to Δ in Y_N we will use the notation $\mathrm{RS}(N, \Delta)$. The subfield subcode of the code $\mathrm{RS}(N, \Delta)$ over $\mathbb{F}_q$ is denoted by $\mathrm{RS}(N, \Delta)_q := \mathrm{RS}(N, \Delta) \cap \mathbb{F}_q^N$. In this case, for the sake of simplicity, we are also going to denote $R_N := R/I(Y_N)$.

Now, we are going to introduce some necessary definitions to obtain bases for the codes $\mathrm{RS}(N, \Delta)_q$. We define $\mathbb{Z}_N = \{0\} \cup \mathbb{Z}/\langle N - 1 \rangle$, where we represent the classes of $\mathbb{Z}/\langle N - 1 \rangle$ by $\{1, \ldots, N\}$. A subset $\mathfrak{I}$ of $\mathbb{Z}_N$ is called a *cyclotomic set* with respect to q if $q \cdot z \in \mathfrak{I}$ for any $z \in \mathfrak{I}$. $\mathfrak{I}$ is said to be minimal (with respect to q) if it can be expressed as $\mathfrak{I} = \{q^i \cdot z, i = 1, 2, \ldots\}$ for a fixed $z \in \mathfrak{I}$, and in that situation we will write $\mathfrak{I}_z := \mathfrak{I}$ and $n_z = |\mathfrak{I}_z|$. We say z is a *minimal representative* of $\mathfrak{I}_z$ if z is the least element in $\mathfrak{I}_z$, and we will say it is a *maximal representative* of $\mathfrak{I}_z$ if it is the biggest element. We will denote by $\mathcal{A}$ the set of minimal representatives of the minimal cyclotomic cosets, and by $\mathcal{B}$ the set of maximal representatives of the minimal cyclotomic cosets.

Example 2.1 Consider the extension $\mathbb{F}_9 \supset \mathbb{F}_3$. We consider $N = 9$ and we have $\mathbb{Z}_N = \{0\} \cup \mathbb{Z}/\langle 8 \rangle$. We have the following minimal cyclotomic sets:

$$\mathfrak{I}_0 = \{0\}, \mathfrak{I}_1 = \{1, 3\}, \mathfrak{I}_2 = \{2, 6\}, \mathfrak{I}_4 = \{4\}, \mathfrak{I}_5 = \{5, 7\}, \mathfrak{I}_8 = \{8\}.$$

The set of minimal representatives is $\mathcal{A} = \{0, 1, 2, 4, 5, 8\}$, and the set of maximal representatives is $\mathcal{B} = \{0, 3, 4, 6, 7, 8\}$.

The dimension of the subfield subcodes of Reed–Solomon codes is already present in Hattori et al. (1998). For the codes $\mathrm{RS}(N, \Delta)_q$ it is possible to obtain a basis given by the evaluation of some polynomials. For each $a \in \mathcal{A}$, we define the following trace map:

$$\mathcal{T}_a : R_N \to R_N, \quad f \mapsto f + f^q + \cdots + f^{q^{(n_a-1)}},$$

and given $\Delta \subset \{0, 1, \ldots, N-1\}$, we denote $\Delta_{\mathfrak{J}} := \bigcup_{\mathfrak{J}_a \subset \Delta} \mathfrak{J}_a \subset \Delta$. The following result gives a basis for the code $\mathrm{RS}(N, \Delta)_q$ (Galindo et al. 2019a, Thm. 11).

Theorem 2.2 *Let Δ be a subset of $\{0, 1, \ldots, N-1\}$ and set ξ_a a primitive element of the field $\mathbb{F}_{q^{n_a}}$. Then, a basis of the vector space $\mathrm{RS}(N, \Delta)_q$ is given by the images under the map ev_{Y_N} of the set of classes in R_N:*

$$\bigcup_{a \in \mathcal{A} | \mathfrak{J}_a \subset \Delta} \{\mathcal{T}_a(\xi_a^r x^a) \mid 0 \leq r \leq n_a - 1\}.$$

As a consequence, we have that

$$\dim \mathrm{RS}(N, \Delta)_q = \sum_{\mathfrak{J}_z : \mathfrak{J}_z \subset \Delta} n_z = |\Delta_{\mathfrak{J}}|.$$

Having seen the affine setting, we are now going to introduce the codes we are going to use throughout this work. We consider the projective line $\mathbb{P}^1$ over $\mathbb{F}_{q^s}$ and the polynomial ring $S = \mathbb{F}_{q^s}[x_0, x_1]$. Given a degree $d \geq 1$, we denote by S_d the homogeneous polynomials of degree d. We are going to fix representatives for the points of $\mathbb{P}^1$ in the following way: for each point $[P] \in \mathbb{P}^1$, we choose the representative whose first nonzero coordinate is equal to 1. We will denote by P^1 this set of representatives, seen as points in the affine space $\mathbb{A}^2$, and we will call them *standard representatives*. If we also consider a finite set of points $X = \{Q_1, \ldots, Q_n\} \subset P^1$, we can define the following evaluation map:

$$\mathrm{ev}_X : S/I(X) \to \mathbb{F}_{q^s}^n, \quad f \mapsto (f(Q_1), \ldots, f(Q_n))_{Q_i \in X},$$

where, as before, we denote a polynomial in S and its class in $S/I(X)$ in the same way. Given $\Delta \subset \{0, 1, \ldots, n-1\}$, we define $d(\Delta) := \max\{i \mid i \in \Delta\}$. The *projective Reed–Solomon* code associated to Δ and X is the code generated by

$$\{\mathrm{ev}_X(x_0^{d(\Delta)-i} x_1^i) \mid i \in \Delta\},$$

which will be denoted by $\mathrm{PRS}(X, \Delta)$. We note that we are only evaluating monomials of exactly degree $d(\Delta)$, which means that their linear combinations are homogeneous polynomials of degree $d(\Delta)$. If $0 \notin \Delta$, $\mathrm{PRS}(X, \Delta)$ is a degenerate code, because all the previous monomials would evaluate to 0 at the point $[1 : 0]$. Therefore, we are always going to assume in what follows that $0 \in \Delta$. Some authors define these codes over the projective space without fixing representatives, as in Martínez-Bernal et al. (2017), but then they can only define the code up to monomial equivalence. Monomially equivalent codes do not necessarily have monomially equivalent subfield subcodes, for example in Hernando et al. (2013) the authors see that the dimension of the subfield subcode of a generalised Reed–Solomon code depends on the twist vector chosen, and that is why we fix representatives from the beginning.

Given a degree $1 \leq d \leq q^s$, the most standard definition of projective Reed–Solomon code in the literature is the code $\mathrm{PRS}(P^1, \Delta_d)$, where $\Delta_d := \{0, 1, \ldots, d\}$. The code $\mathrm{PRS}(P^1, \Delta_d)$ is also called *doubly extended Reed–Solomon code* and its parameters are $[q^s + 1, d + 1, q^s - d + 1]$.

To obtain bases for the subfield subcodes of the codes $\mathrm{PRS}(X, \Delta)$, we are going to evaluate in subgroups similarly to the affine case. The natural ideal is to add the point at infinity $[0:1]$ to the points that we were considering in the affine case. Therefore, given N, such that $N-1 \mid q^s-1$, we define $\mathbb{X}_N^* = [\{1\} \times Y_N^*] \cup [0:1] \subset \mathbb{P}^1$ and $\mathbb{X}_N = [\{1\} \times Y_N] \cup [0:1] \subset \mathbb{P}^1$, where we recall that Y_N^* and Y_N are the zero locus of $\langle x^{N-1}-1 \rangle$ and $\langle x^N - x \rangle$, respectively. However, it is easy to see that another set of representatives for $\mathbb{X}_N^*$ is $[Y_N \times \{1\}]$. Thus, the codes obtained when evaluating in this set would be monomially equivalent to the ones obtained in the affine case when evaluating in Y_N. As we said before, this does not mean that their subfield subcodes are monomially equivalent. Nevertheless, our experiments show that the parameters that we obtain when evaluating in the set $\mathbb{X}_N^*$ are strictly worse than the ones obtained in the affine case with Y_N. Hence, in what follows we are going to focus on evaluating in the set $\mathbb{X}_N$, although we note that the theory we are going to develop can be adapted for the set $\mathbb{X}_N^*$ as well.

We denote the standard representatives of $\mathbb{X}_N$ by X_N, and we also denote $\mathrm{PRS}(N, \Delta) := \mathrm{PRS}(X_N, \Delta)$. With this notation, doubly extended Reed–Solomon codes are denoted by $\mathrm{PRS}(q^s, \Delta_d)$. Similarly to the case of doubly extended Reed–Solomon codes, given $1 \leq d \leq N$, the parameters of the code $\mathrm{PRS}(N, \Delta_d)$ are $[N+1, d+1, N-d+1]$. In general, for the codes $\mathrm{PRS}(N, \Delta)$ we have the parameters $[N+1, |\Delta|, \geq N - d(\Delta) + 1]$, where the bound for the minimum distance is given by the smallest doubly extended Reed–Solomon code that contains $\mathrm{PRS}(N, \Delta)$.

3 Subfield subcodes of codes over the projective line

Let $\mathbb{F}_{q^s} \supset \mathbb{F}_q$ and N, such that $N-1 \mid q^s-1$. In this section, we want to obtain bases for the subfield subcodes of the codes $\mathrm{PRS}(N, \Delta)$ with respect to this extension, which we will denote by $\mathrm{PRS}(N, \Delta)_q := \mathrm{PRS}(N, \Delta) \cap \mathbb{F}_q$. Given $f \in S$, we say that f evaluates to $\mathbb{F}_q$ in X_N whenever $f(Q) \in \mathbb{F}_q$ for all $Q \in X_N$ (similarly for polynomials in R evaluating in Y_N). The following lemma gives the key idea to obtain bases for $\mathrm{PRS}(N, \Delta)_q$.

Lemma 3.1 *Let $X_N \subset P^1$. Then, $f \in S$ evaluates to $\mathbb{F}_q$ in $X_N \iff f(1, x_1)$ evaluates to $\mathbb{F}_q$ in Y_N and $f(0,1)$ is in $\mathbb{F}_q$.*

We will see now that we can take advantage of the knowledge from the affine case in Theorem 2.2 by homogenizing and using Lemma 3.1. Given a degree d and a polynomial $f(x) \in R$ with $\deg(f) \leq d$, its homogenization up to degree d is the homogeneous polynomial $f^h(x_0, x_1) := x_0^d f(x_1/x_0) \in S_d$. Unless stated otherwise, when we consider the code $\mathrm{PRS}(N, \Delta)$, we are always going to assume that we are homogenizing up to degree $d = d(\Delta)$.

For a polynomial $f \in \mathbb{F}_q[x_1]$, we choose $\mathcal{T}_a(f)$ as the representative of the class in $\mathbb{F}_{q^s}[x_1]/I(Y_N)$ which has the exponents of each monomial reduced modulo q^s-1. Given $d \geq 1$, if the degree of $\mathcal{T}_a(f)$ is lower than d, then we define $\mathcal{T}_a^h(f) := (\mathcal{T}_a(f))^h$, which we call homogenized trace. If we consider one of the traces that appear in Theorem 2.2, its homogenized trace automatically satisfies that, when setting $x_0 = 1$, the resulting polynomial evaluates to $\mathbb{F}_q$ in Y_N, i.e., the first condition from Lemma 3.1 is satisfied. However, the second condition, which means that the coefficient of x_1^d in the homogenized trace must be in $\mathbb{F}_q$, might not be satisfied. Because of this, the projective case is more involved than the affine case, as we will see in the next example.

Example 3.2 We continue with Example 2.1. By Theorem 2.2, the following polynomial associated to $\mathfrak{I}_1$ evaluates to $\mathbb{F}_3$:

$$\mathcal{T}_1(x) = x + x^3.$$

Let $d = 3$ (the degree up to which we homogenize). If we consider the polynomial $f = \mathcal{T}_1^h(x_1) = x_0^2x_1 + x_1^3$, this is a homogeneous polynomial of degree 3, such that $f(1, x_1)$ takes the same values as $\mathcal{T}_1(x_1)$ in $\mathbb{F}_9$, and $f(0, 1) = 1 \in \mathbb{F}_3$. By Lemma 3.1, we know that f evaluates to $\mathbb{F}_3$ when evaluating in P^1.

If ξ is a primitive element in $\mathbb{F}_9$, by Theorem 2.2, the following polynomial also evaluates to $\mathbb{F}_3$:

$$\mathcal{T}_1(\xi x) = \xi x + \xi^3 x^3.$$

However, if we consider $g = \mathcal{T}_1^h(\xi x_1) = \xi x_0^2 x_1 + \xi^3 x_1^3$, we see that $g(0, 1) = \xi^3 \notin \mathbb{F}_3$. Therefore, g does not evaluate to $\mathbb{F}_3$.

Remark 3.3 If we have $f \in S_d$ which evaluates to $\mathbb{F}_q$, then $x_0 f \in S_{d+1}$ also evaluates to $\mathbb{F}_q$. Moreover, if $f(1, x_1)$ evaluates to $\mathbb{F}_q$ in Y_N, then $g = x_0 f \in S_{d+1}$ evaluates to $\mathbb{F}_q$ in X_N, even if f does not, because $g(1, x_1) = f(1, x_1)$, which evaluates to $\mathbb{F}_q$, and $g(0, 1) = 0 \in \mathbb{F}_q$. This already gives a hint about the fact that the sequence of dimensions of the subfield subcodes is going to be non-decreasing.

With Lemma 3.1, we can consider polynomials in one variable that evaluate to $\mathbb{F}_q$ to obtain polynomials in S_d that evaluate to $\mathbb{F}_q$ in X_N in some cases. One could also consider the polynomials in two variables that evaluate to $\mathbb{F}_q$ when evaluating in the points of $\mathbb{A}^2$. All of those polynomials are going to evaluate to $\mathbb{F}_q$ when evaluating in points of P^1. However, there are bivariate polynomials that evaluate to $\mathbb{F}_q$ in P^1, but not in $\mathbb{A}^2$. For example, in Example 3.2 we consider $f = x_0^2x_1 + x_1^3$, which evaluates to $\mathbb{F}_3$ over P^1, but if we consider this polynomial over $\mathbb{A}^2$, then it is clear that it does not evaluate to $\mathbb{F}_3$. For example, if ξ is a primitive element in $\mathbb{F}_9$, $f(0, \xi) = \xi^3 \notin \mathbb{F}_3$.

The following result shows how to use the previous ideas to obtain a basis for $\mathrm{PRS}(N, \Delta)_q$.

Theorem 3.4 *Let Δ be a nonempty subset of $\{0, 1, \ldots, N-1\}$ and let $d = d(\Delta)$. Set ξ_b a primitive element of the field $\mathbb{F}_{q^{n_b}}$. A basis for $\mathrm{PRS}(N, \Delta)_q$ is given by the image by ev_{X_N} of the following polynomials.*

If $\mathfrak{I}_d \subset \Delta$:

$$\bigcup_{b \in \mathcal{B} \mid \mathfrak{I}_b \subset \Delta, b < d} \{\mathcal{T}_b^h(\xi_b^r x_1^b) \mid 0 \leq r \leq n_b - 1\} \cup \{\mathcal{T}_d^h(x_1^d)\}.$$

If $\mathfrak{I}_d \not\subset \Delta$:

$$\bigcup_{b \in \mathcal{B} \mid \mathfrak{I}_b \subset \Delta} \{\mathcal{T}_b^h(\xi_b^r x_1^b) \mid 0 \leq r \leq n_b - 1\}.$$

Proof If we consider

$$\bigcup_{b \in \mathcal{B} \mid \mathfrak{I}_b \subset \Delta, b < d} \{\mathcal{T}_b^h(\xi_b^r x_1^b) \mid 0 \leq r \leq n_b - 1\},$$

these are functions which have linearly independent evaluations, because when evaluating in $[\{1\} \times X_N]$ they are linearly independent by Theorem 2.2. These polynomials do not have the monomial x_1^d in their support. Therefore, by Lemma 3.1, they evaluate to $\mathbb{F}_q$ in X_N.

If $\mathfrak{I}_d \not\subset \Delta$, we are going to see that the evaluation of these polynomials generates the whole subfield subcode. Let $S_{d,\Delta} \subset S_d$ be the linear space generated by $\{x_0^{d-i}x_1^i \mid i \in \Delta\}$, and let $f \in S_{d,\Delta}$ be such that its evaluation is in $\mathrm{PRS}(N, \Delta)_q$. If $f(0, 1) = 0$, then, using Theorem 2.2, we know that we can generate the evaluation of f with these polynomials. On the other hand, we claim that $f(0, 1) \neq 0$ cannot happen in this case, which means that the image by the evaluation map of the stated polynomials generate the whole subfield subcode. If we had $f(0, 1) \neq 0$, that would imply that $f(1, x_1)$ has the monomial x_1^d in its support. However, if $\mathfrak{I}_d \not\subset \Delta$, then we know that there is at least one $a_1 \in \mathfrak{I}_d$ which is not in Δ. Therefore, we cannot obtain the monomial $x_1^{a_1}$ in the support of $f(1, x_1)$, because using Theorem 2.2 in Y_N, once you have x_1^d in the support of $f(1, x_1)$, you should have x_1^a in its support for all $a \in \mathfrak{I}_d$, because $f(1, x_1)$ should be a linear combination of traces. Therefore, $f(0, 1) \neq 0$ is not possible in this case, and the stated polynomials generate the whole subfield subcode.

In the case $\mathfrak{I}_d \subset \Delta$, we have that $d \in \mathcal{B}$, i.e., there is a minimal cyclotomic set whose maximal representative is equal to d. By Lemma 3.1, we have that $\mathcal{T}_d^h(x_1^d)$ evaluates to $\mathbb{F}_q$, and it is linearly independent from the other polynomials that we consider, because it is the only one that takes a nonzero value at $[0 : 1]$.

We are going to show now that the evaluation of the given set of polynomials generates the whole code in this case. Let $f \in S_{d,\Delta}$, such that f evaluates to $\mathbb{F}_q$. By Lemma 3.1, $f(0, 1)$ is in $\mathbb{F}_q$. Hence, we can subtract $\mathcal{T}_d^h(x_1^d)$ multiplied by $f(0, 1) \in \mathbb{F}_q$ and the evaluation would still be in $\mathbb{F}_q$. Therefore, we can assume that f does not have the monomial x_1^d in its support, i.e., $f(0, 1) = 0$. Then, we can use the affine case and argue that if $f(1, x_1)$ evaluates to $\mathbb{F}_q$, by Theorem 2.2 it must be a linear combination of the polynomials in

$$\bigcup_{b\in\mathcal{B}|\mathfrak{I}_b\subset\Delta, b<d} \{\mathcal{T}_b(\xi_b^r x_1^b) \mid 0 \leq r \leq n_b - 1\}.$$

The homogenized polynomials that we consider have the same evaluation as these polynomials in $[\{1\} \times Y_N]$, which completes the proof. □

Remark 3.5 We note that we are obtaining a basis which is the image by the evaluation map of some homogeneous polynomials of degree d, which we already knew that should be possible, because $\mathrm{PRS}(N, \Delta)_q \subset \mathrm{PRS}(N, \Delta)$.

Example 3.6 We continue with Examples 2.1 and 3.2. We consider $N = 9$ and $\Delta = \{0, 1, 2, 3\}$, which means that we have $d(\Delta) = 3$. Looking at the cyclotomic sets from Example 2.1, we see that $\mathfrak{I}_0 \cup \mathfrak{I}_1 \subset \Delta$ (and these are the only complete minimal cyclotomic sets in Δ). By Theorem 3.4, taking into account that in this case we have $\mathfrak{I}_3 = \mathfrak{I}_d \subset \Delta$, we see that the evaluation of the following polynomials is a basis for $\mathrm{PRS}(9, \Delta)_3$:

$$\mathcal{T}_0^h(x_1^0) = x_0^3, \mathcal{T}_3^h(x_1^3) = x_0^2x_1 + x_1^3.$$

We note that the second polynomial is precisely the polynomial f in Example 3.2.

If we take $\Delta = \{0, 1, 2, 3, 4\}$, then we have $d(\Delta) = 4$ and $\mathfrak{I}_0 \cup \mathfrak{I}_1 \cup \mathfrak{I}_4 \subset \Delta$. By Theorem 3.4, the evaluation of the following polynomials is a basis for $\mathrm{PRS}(9, \Delta)_3$:

$$\mathcal{T}_0^h(x_1^0) = x_0^4, \mathcal{T}_3^h(x_1^3) = x_0^3x_1 + x_0x_1^3, \mathcal{T}_3^h(\xi x_1^3) = \xi^3x_0^3x_1 + \xi x_0x_1^3, \mathcal{T}_4^h(x_1^4) = x_1^4.$$

Corollary 3.7 *The dimension of* $\mathrm{PRS}(N, \Delta)_q$ *is the following:*

$$\dim \mathrm{PRS}(N, \Delta)_q = \begin{cases} \sum_{b\in\mathcal{B}:\mathfrak{I}_b\subset\Delta} n_b - (n_d - 1) = \sum_{b\in\mathcal{B}:\mathfrak{I}_b\subset\Delta, b<d} n_b + 1 & \text{if } \mathfrak{I}_d \subset \Delta \\ \sum_{b\in\mathcal{B}:\mathfrak{I}_b\subset\Delta} n_b & \text{otherwise} \end{cases}$$

Remark 3.8 Let $d = d(\Delta)$. If $\mathfrak{I}_d \subset \Delta$, we have dimension 1 more than in the affine case with $\Delta \setminus \{d\}$. On the other hand, if $\mathfrak{I}_d \not\subset \Delta$, we obtain a degenerate code with a 0 at the point $[0 : 1]$. Therefore, the interesting case is when $\mathfrak{I}_d \subset \Delta$, which is the one in which we are going to mainly focus in what follows.

With respect to the minimum distance, if we denote by $\mathrm{wt}(C)$ the minimum distance of a code $C \subset \mathbb{F}_{q^s}^n$, we have $\mathrm{wt}(\mathrm{PRS}(N, \Delta)) \geq N - d(\Delta) + 1$, which implies that $\mathrm{wt}(\mathrm{PRS}(N, \Delta)_q) \geq N - d(\Delta) + 1$, because $\mathrm{PRS}(N, \Delta)_q \subset \mathrm{PRS}(N, \Delta)$. For the case of subfield subcodes of doubly extended Reed–Solomon codes we obtain the following corollary.

Corollary 3.9 *Let $d \in \mathcal{B}$. The parameters of $\mathrm{PRS}(q^s, \Delta_d)_q$ are $[q^s + 1, \sum_{b \in \mathcal{B}: b < d} n_b + 1, \geq q^s - d + 1]$. Moreover, the first nontrivial (dimension higher than 1) subfield subcode is obtained when $d = q^{s-1}$.*

Proof The parameters are a special case of the previous results and discussions. For the last statement, it is clear that $q^s/q = q^{s-1}$ is the lowest possible element in $\mathcal{B}$ (besides 0), and $d = q^{s-1}$ is the first degree, such that $\mathfrak{I}_1 = \{1, q, q^2, \ldots, q^{s-1}\} \subset \Delta_d$. □

The bound used for the minimum distance of the subfield subcodes of doubly extended Reed–Solomon codes is sharp in all cases we have checked with $d \in \mathcal{B}$. The codes obtained in this way have one more length and dimension than in the affine case, with the same minimum distance.

Example 3.10 If we look at the results from Example 3.6, we see that we obtained dimension 2 and 4 for $\mathrm{PRS}(9, \Delta_3)_3$ and $\mathrm{PRS}(9, \Delta_4)_3$. These are the values obtained with Corollary 3.9, because $2 = n_0 + 1$ and $4 = n_0 + n_3 + 1$. We would obtain codes with parameters $[10, 2, 7]$ and $[10, 4, 6]$ over $\mathbb{F}_3$.

4 Dual codes of the previous subfield subcodes

To compute the dual codes of the previous subfield subcodes, we are going to use Delsarte's Theorem (Delsarte 1975).

Theorem 4.1 *Let $C \subset \mathbb{F}_{q^s}^n$ be a linear code:*

$$(C \cap \mathbb{F}_q^n)^\perp = \mathrm{Tr}(C^\perp),$$

where $\mathrm{Tr} : \mathbb{F}_{q^s} \to \mathbb{F}_q$, which maps x to $x + x^q + \cdots + x^{q^{s-1}}$, is applied componentwise to $C^\perp$.

To use this result, we need to compute the dual of the codes $\mathrm{PRS}(N, \Delta)$. It is well known that $\mathrm{PRS}(q^s, \Delta_d)^\perp = \mathrm{PRS}(q^s, \Delta_{q^s-1-d})$ (the dual of a doubly extended Reed–Solomon code is another doubly extended Reed–Solomon code). However, computing the dual of the codes $\mathrm{PRS}(N, \Delta)$ in general can be involved. Nevertheless, we can easily compute the dual in some cases. To do so, we are going to state the metric structure of these codes first. Part of the following result already appears in Galindo et al. (2015, Prop. 1) and López (2021, Lem. 7.1).

Lemma 4.2 *Let γ be a non-negative integer, and N, such that $N-1 \mid q^s-1$. We consider the monomial $x^\gamma \in \mathbb{F}_{q^s}[x]$. We have the following:*

$$\sum_{z\in Y_N} x^\gamma(z) = \begin{cases} N & \text{if } \gamma = 0, \\ 0 & \text{if } \gamma > 0 \text{ and } \gamma \not\equiv 0 \bmod (N-1), \\ N-1 & \text{if } \gamma > 0 \text{ and } \gamma \equiv 0 \bmod (N-1). \end{cases}$$

Proof Let $\xi \in \mathbb{F}_{q^s}$ be an element of order $N-1$, which exists, because $N-1 \mid q^s-1$. Then, $Y_N = \{\xi^0, \xi^1, \ldots, \xi^{N-2}\} \cup \{0\}$. If $\gamma = 0$, $x^\gamma = 1$, and the sum is equal to $|Y_N| = N$. If $\gamma > 0$ and $\gamma \equiv 0 \bmod (N-1)$, then $x^\gamma(z) = 1$ for all $z \in Y_N \backslash \{0\}$, and $\sum_{z\in Y_N} x^\gamma(z) = |Y_N| - 1 = N-1$. Finally, if $\gamma > 0$ and $\gamma \not\equiv 0 \bmod (N-1)$, we have

$$\sum_{z\in Y_N} x^\gamma(z) = \sum_{i=0}^{N-2} (\xi^i)^\gamma = \frac{\xi^{\gamma(N-1)}-1}{\xi^\gamma - 1} = 0.$$

□

Proposition 4.3 *Let $x_0^{\alpha_0}x_1^{\alpha_1}$ and $x_0^{\beta_0}x_1^{\beta_1}$ be two monomials in $\mathbb{F}_{q^s}[x_0, x_1]$ of degree d_α and d_β, respectively. Then, we have the following for the product of the evaluations over X_N. If $\alpha_1 + \beta_1 = 0$:*

$$\mathrm{ev}_{X_N}(x_0^{\alpha_0}x_1^{\alpha_1}) \cdot \mathrm{ev}_{X_N}(x_0^{\beta_0}x_1^{\beta_1}) = \begin{cases} N+1 & \text{if } \alpha_0+\beta_0 = 0, \\ N & \text{if } \alpha_0+\beta_0 > 0. \end{cases}$$

If $\alpha_1 + \beta_1 > 0$:

$$\mathrm{ev}_{X_N}(x_0^{\alpha_0}x_1^{\alpha_1}) \cdot \mathrm{ev}_{X_N}(x_0^{\beta_0}x_1^{\beta_1}) = \begin{cases} N & \text{if } \alpha_1+\beta_1 \equiv 0 \bmod (N-1), \alpha_0+\beta_0 = 0, \\ N-1 & \text{if } \alpha_1+\beta_1 \equiv 0 \bmod (N-1), \alpha_0+\beta_0 > 0, \\ 1 & \text{if } \alpha_1+\beta_1 \not\equiv 0 \bmod (N-1), \alpha_0+\beta_0 = 0, \\ 0 & \text{if } \alpha_1+\beta_1 \not\equiv 0 \bmod (N-1), \alpha_0+\beta_0 > 0. \end{cases}$$

Proof First, we expand the scalar product as a sum over $X_N = \{[1:z] \mid z \in Y_N\} \cup \{[0:1]\} \subset P^1$:

$$\mathrm{ev}_{X_N}(x_0^{\alpha_0}x_1^{\alpha_1}) \cdot \mathrm{ev}_{X_N}(x_0^{\beta_0}x_1^{\beta_1}) = \sum_{P\in X_N} x_0^{\alpha_0+\beta_0}x_1^{\alpha_1+\beta_1}(P) = \sum_{z\in Y_N} z^{\alpha_1+\beta_1} + \epsilon,$$

where ϵ is equal to 1 if $\alpha_0+\beta_0 = 0$ and equal to 0 if $\alpha_0+\beta_0 > 0$ (corresponding to the evaluation at $[0:1]$). The result is obtained using Lemma 4.2. □

If p does not divide N, we have that the evaluation of $x_1^{\alpha_1}$ with $\alpha_1 > 0$ is not orthogonal to the evaluation of $x_1^{\beta_1}$ for any β_1. This means that the dual code $\mathrm{PRS}(N,\Delta)^\perp$ does not have a basis obtained by the evaluation of monomials unless $\mathrm{wt}(\mathrm{PRS}(N,\Delta)) = 1$. This is because if we have $\mathrm{wt}(\mathrm{PRS}(N,\Delta)) > 1$, then $\mathrm{PRS}(N,\Delta)^\perp$ cannot be degenerate. In particular, there must be a vector in $\mathrm{PRS}(N,\Delta)^\perp$, such that the coordinate associated to the point $[0:1]$ is nonzero, which is obtained by evaluating a polynomial with some power of x_1 in its support, but it cannot be just a single power of x_1, because its evaluation would not be orthogonal to the evaluation of x_1^q. Hence, the dual code is not generated by the image by the evaluation map of monomials.

When $p \mid N$, as the next result shows, the previous result gets simplified, and in Proposition 4.10 we will see that in this case the dual code can be generated by the evaluation of monomials.

Corollary 4.4 *If $p \mid N$, then:*

$$\mathrm{ev}_{X_N}(x_0^{\alpha_0}x_1^{\alpha_1}) \cdot \mathrm{ev}_{X_N}(x_0^{\beta_0}x_1^{\beta_1}) = \begin{cases} 1 & \text{if } \alpha_1+\beta_1 = 0, \alpha_0+\beta_0 = 0 \text{ or} \\ & \quad \alpha_1+\beta_1 \not\equiv 0 \mod (N-1), \alpha_0+\beta_0 = 0, \\ -1 & \text{if } \alpha_1+\beta_1 \equiv 0 \mod (N-1), \alpha_i+\beta_i > 0, i = 0,1, \\ 0 & \text{otherwise.} \end{cases}$$

Remark 4.5 One way to have $p \mid N$ is to consider a subfield of $\mathbb{F}_{q^s}$, in which case we are going to obtain a doubly extended Reed–Solomon code over that subfield. However, we may also have $p \mid N$ for different subgroups of $\mathbb{F}_{q^s}^*$. For example, if we consider $q^s = 2^4 = 16$, then 5 divides $q^s - 1$. Therefore, we can take $N = 6$, which is divisible by 2, but Y_6 is not a subfield of $\mathbb{F}_{16}$.

For obtaining a basis for the dual code we will need to work with non-homogeneous polynomials. To understand linear independence in that situation we are going to introduce now a universal Gröbner basis for the vanishing ideal $I(X_N)$. Particular cases of the following result were already present in Nakashima and Matsui (2016).

Proposition 4.6 *A universal Gröbner basis for the ideal $I(X_N)$ is*

$$I(X_N) = \langle x_0^2 - x_0, x_1^N - x_1, (x_0-1)(x_1-1)\rangle.$$

Therefore, $\mathrm{in}(I(X_N)) = \langle x_0^2, x_1^N, x_0x_1\rangle$ *and* $\{1, x_0, x_1, x_1^2, \ldots, x_1^{N-1}\}$ *is a basis for the quotient ring $S/I(X_N)$.*

Proof First, we are going to show that these polynomials generate the vanishing ideal $I(X_N)$. Given any point in X_N, it is clear that it satisfies the equations. Reciprocally, any point satisfying this equations, because of the generator $x_0^2 - x_0$, must have the first coordinate equal to 0 or 1. If the first coordinate is equal to 0, because of the generator $(x_0-1)(x_1-1)$, the last coordinate must be 1, i.e., it must be the point $[0:1] \in X_N$. If the first coordinate is equal to 1, then, because of the generator $x_1^N - x_1$, the second coordinate is in Y_N, which means that the point is in X_N as well.

We have proved that the variety defined by this ideal is X_N. It is clear that the variety defined by this ideal over the algebraic closure $\overline{\mathbb{F}_{q^s}}$ is the same as the variety defined over $\mathbb{F}_{q^s}$. By Seidenberg's Lemma (Kreuzer and Robbiano 2000, Prop. 3.7.15), this ideal is radical. Therefore, by Hilbert's Nullstellensatz applied in the algebraic closure, we have that this ideal is the vanishing ideal of the variety that it defines, i.e., is the vanishing ideal of X_N.

To show that all the S-polynomials of the generators reduce to 0, we just need to use that if the greatest common divisor of the initial monomials of two polynomials is 1, then their S-polynomial reduces to 0 by Cox et al. (2015, Prop. 4, Chapter 2, Section 9). In particular, if two polynomials depend on different variables, their S-polynomial reduces to 0. And if f and g share a common factor w, then $S(f,g) = wS(f/w, g/w)$. Using this, it is easy to see that all the S-polynomials reduce to 0 in this case, for any monomial order. Thus, these generators form a universal Gröbner basis. The initial ideal follows from this fact, and by Macaulay's classical result (Eisenbud 1995, Thm. 15.3) we obtain that the monomials not contained in the initial ideal form a basis for the quotient ring. □

Remark 4.7 Because of the first generator of the previous ideal, any power of x_0 is equivalent to x_0 in the quotient ring. Therefore, we have $x_0^{\alpha_0}x_1^{\alpha_1} \equiv x_0x_1^{\alpha_1} \mod I(X_N)$ if $\alpha_0 > 0$. This is

why we are going to assume $\alpha_0 = 1$ for any monomial divisible by x_0 in what follows, except when we want to remark that we can obtain a code by evaluating homogeneous polynomials of a certain degree.

The following result allows us to express any polynomial in $S/I(X_N)$ in terms of the basis in Proposition 4.6.

Lemma 4.8 *Let a_0, a_1 be integers, with $a_0 > 0$. We have that*

$$x_0^{a_0} x_1^{a_1} \equiv x_0 + x_1^{a_1} - 1 \mod I(X_N).$$

Proof It is easy to check that both polynomials have the same evaluation in X_N, which implies that they are in the same class modulo $I(X_N)$. □

Corollary 4.9 *The following monomials constitute a basis for the quotient $S/I(X_N)$:*

$$\{x_1^N, x_0, x_0x_1, \ldots, x_0x_1^{N-1}\}.$$

Moreover, every set of the form $\{x_1^d, x_0, x_0x_1, \ldots, x_0x_1^{d-1}\}$ with $1 \leq d \leq N$ is linearly independent.

Proof It is easy to check that these monomials are linearly independent by Lemma 4.8 and Proposition 4.6. The fact that for $d = N$ this set is a basis follows from the cardinality of the set and the dimension of the quotient ring. □

Now, we have the tools necessary to deal with the dual as an evaluation code over the projective line. In what follows we are going to assume that $p \mid N$. This is because, by Corollary 4.4, the metric structure is going to be similar to the one of doubly extended Reed–Solomon codes, and in this case the dual code will be generated by the evaluation of monomials. For the following result it will be useful to introduce the definition $\Delta^\perp = \{\alpha \in \{0, 1, \ldots, N-1\} \mid \alpha \neq N - 1 - h, h \in \Delta\}$.

Proposition 4.10 *Let N be a non-negative integer, such that $N - 1 \mid q^s - 1$ and $p \mid N$. Let $\Delta \subset \{0, 1, \ldots, N-1\}$ and let $d = d(\Delta)$. Then, $\mathrm{PRS}(N, \Delta)^\perp$ has a basis obtained by taking the image by ev_{X_N} of the following monomials:*

$$\{x_0x_1^\alpha \mid \alpha \in \Delta^\perp\} \cup \{x_1^{N-1-d}\}. \tag{2}$$

Moreover, if $N - 1 \notin \Delta$, we can also obtain the same basis by taking the image by ev_{X_N} of the following monomials of degree $2(N-1) - d$ (which allows us to get the dual code as an evaluation code of homogeneous polynomials):

$$\{x_0^{2(N-1)-d-\alpha} x_1^\alpha \mid \alpha \in \Delta^\perp\} \cup \{x_1^{2(N-1)-d}\}. \tag{3}$$

If $N - 1 \in \Delta$, then the following set of homogeneous polynomials of degree $2N - 1$ give the same image as the set in item (2):

$$\{x_0^{2N-1-\alpha} x_1^\alpha \mid \alpha \in \Delta^\perp\} \cup \{x_1^{2N-1} + x_0^{2N-1} - x_0^{N-1}x_1^N\}. \tag{4}$$

Proof Using Corollary 4.4 it is easy to see that the evaluation of the monomials in (2) is orthogonal to the vectors in $\mathrm{PRS}(N, \Delta)$. When $N - 1 \notin \Delta$, using Lemma 4.8 it is easy to see that the evaluation of these monomials is linearly independent, and the dimension of this subspace is the same as the dimension of the dual code. If $N - 1 \in \Delta$, then $x_1^{N-1-d} = 1$, and it is easy to see that the monomials that we obtain are linearly independent and generate

the dual code. When $N-1 \notin \Delta$, the evaluation of the set (3) is clearly the same. Finally, if $N-1 \in \Delta$, we have that

$$x_1^{2N-1} + x_0^{2N-1} - x_0^{N-1}x_1^N \equiv x_1 + x_0 - x_0x_1 \equiv 1 \mod I(P^1).$$

Therefore, the evaluation of the set (4) is the same as the one obtained with (2). □

We have the next result for the case when $p \mid N$, which generalizes what we know about the duality in the case of doubly extended Reed–Solomon codes. We note that, as we are evaluating all the monomials of degree d in the next result, and the set of evaluation points is a complete intersection, the theory from Duursma et al. (2001) and González-Sarabia and Rentería (2004) could also be used to study the codes $\mathrm{PRS}(N, \Delta_d)$ and their duals.

Corollary 4.11 *Let $\Delta_d = \{0, 1, \ldots, d\}$ and $\Delta_{N-1-d} = \{0, 1, \ldots, N-1-d\}$. If $p \mid N$, then we have that $\mathrm{PRS}(N, \Delta_d)^\perp = \mathrm{PRS}(N, \Delta_{N-1-d})$.*

Proof We can consider the monomials in (2), homogenizing up to degree $N-1-d$ with the variable x_0. Taking into account that in this case $\Delta^\perp \cup \{N-1-d\} = \Delta_{N-1-d}$ we obtain the result. □

With the evaluation map ev_{X_N}, if we consider the trace function $T : S \to S$, defined by $f \to f + f^q + \cdots + f^{q^{s-1}}$, then it is easy to verify that $\mathrm{ev}_{X_N} \circ T = \mathrm{Tr} \circ \mathrm{ev}_{X_N}$ (Tr was defined in Theorem 4.1). Then, we see that if $\mathrm{PRS}(N, \Delta)^\perp = \mathrm{ev}_{X_N}(\langle\{f_1, f_2, \ldots, f_l\}\rangle)$, using Theorem 4.1 and the previous observation we get that

$$\begin{aligned}(\mathrm{PRS}(N, \Delta)_q)^\perp &:= (\mathrm{PRS}(N, \Delta)_q)^\perp = \mathrm{Tr}(\mathrm{ev}_{X_N}(\langle\{f_1, f_2, \ldots, f_l\}\rangle)) \\ &= \mathrm{ev}_{X_N}(T(\langle\{f_1, f_2, \ldots, f_l\}\rangle)).\end{aligned}$$

Remark 4.12 Taking into account that T is linear, then it is clear that in this situation $(\mathrm{PRS}(N, \Delta)_q)^\perp$ is spanned by the image by the evaluation of the polynomials $T(\gamma f_i)$, $\gamma \in \mathbb{F}_{q^s}$, $i = 1, \ldots, l$.

Even if f_i, for $i = 1, \ldots, l$, are monomials, the dual code will be generated by traces of those monomials by Remark 4.12, which in general are going to be non-homogeneous polynomials. We have introduced the vanishing ideal from Proposition 4.6 precisely to understand linear independence of sets of monomials of different degree over X_N. In order to state a basis for $(\mathrm{PRS}(N, \Delta)_q)^\perp$ we will need the following lemma.

Lemma 4.13 *Let $\Delta \subset \{0, 1, \ldots, N-1\}$ and $0 < a \neq N-1$. Then, we have that $\mathfrak{I}_a \subset \Delta \iff |\mathfrak{I}_{N-1-a} \cap \Delta^\perp| = 0$.*

Proof It is clear that we have a bijection between $\mathfrak{I}_a$ and $\mathfrak{I}_{-a}$, given by $h \mapsto -h$. In $\mathbb{Z}_N$ we have that $-h \equiv N-1-h \mod N-1$ if $h \neq 0$. Hence, we get a bijection between $\mathfrak{I}_a$ and $\mathfrak{I}_{N-1-a}$ given by $h \mapsto N-1-h$. Because of the definition of $\Delta^\perp$, we see that if $h \in \Delta$, then $N-1-h \notin \Delta^\perp$. Thus, it is clear that if $\mathfrak{I}_a \subset \Delta$, then $|\mathfrak{I}_{N-1-a} \cap \Delta^\perp| = 0$, and vice versa. □

Theorem 4.14 *Let Δ be a nonempty subset of $\{0, 1, \ldots, N-1\}$ and let $d = d(\Delta)$. Set ξ_a a primitive element of the field $\mathbb{F}_{q^{na}}$ with $\mathcal{T}_a(\xi_a) \neq 0$ (this can always be done Cohen 1990). A basis for $(\mathrm{PRS}(N, \Delta)_q)^\perp$ is given by the image by ev_{X_N} of the following polynomials.*

If $\mathfrak{I}_d \subset \Delta$*:*

$$\bigcup_{a\in\mathcal{A}|\mathfrak{I}_a\cap\Delta^\perp\neq\emptyset} \{\mathcal{T}_a(\xi_a^r x_0 x_1^a) \mid 0 \le r \le n_a - 1\} \cup$$
$$\{\mathcal{T}_{N-1-d}(\xi_{N-1-d}^r x_1^{N-1-d}) \mid 0 \le r \le n_{N-1-d} - 1\}.$$

If $\mathfrak{I}_d \not\subset \Delta$*:*

$$\bigcup_{a\in\mathcal{A}|\mathfrak{I}_a\cap\Delta^\perp\neq\emptyset} \{\mathcal{T}_a(\xi_a^r x_0 x_1^a) \mid 0 \le r \le n_a - 1\} \cup \{\mathcal{T}_{N-1-d}(\xi_{N-1-d} x_1^{N-1-d})\}.$$

Proof In Remark 4.12 we saw that it is enough to consider the traces of multiples of the monomials whose images span $\mathrm{PRS}(N, \Delta)^\perp$. Therefore, we have that the traces of multiples of the monomials in (2) span $\mathrm{Tr}(\mathrm{PRS}(N, \Delta)^\perp) = (\mathrm{PRS}(N, \Delta)_q)^\perp$. Moreover, it is enough to consider the following traces for $\mathfrak{I}_a$ with $\mathfrak{I}_a \cap \Delta^\perp \neq \emptyset$

$$\{\mathcal{T}_a(\xi_a^r x_0 x_1^a), 0 \le r \le n_a - 1\}$$

because they are linearly independent (a dependence relation would give a polynomial relation on ξ_a of degree less than n_a) and there are n_a of them, which is the maximum dimension that we can get with n_a monomials. The same reasoning shows that it is enough to consider the following traces for the monomial x_1^{N-1-d}:

$$\{\mathcal{T}_{N-1-d}(\xi_{N-1-d}^r x_1^{N-1-d}), 0 \le r \le n_{N-1-d} - 1\}, \tag{5}$$

which are linearly independent between them as well.

If $\mathfrak{I}_d \subset \Delta$, by Lemma 4.13 we have that $|\mathfrak{I}_{N-1-d} \cap \Delta^\perp| = \emptyset$. Hence, when we consider all of these sets of polynomials together, they are independent, because between sets corresponding to different cyclotomic sets $\mathfrak{I}_a$, we have polynomials with disjoint support (the monomials that we are considering are linearly independent in $S/I(X_N)$ by Corollary 4.9).

On the other hand, when $\mathfrak{I}_d \not\subset \Delta$, by Lemma 4.13 we know that there is at least one element $h \in \mathfrak{I}_{N-1-d} \cap \Delta^\perp$. The argument for the previous case works in this case, except when considering the traces of polynomials associated to $\mathfrak{I}_{N-1-d}$ and the polynomials in (5), because by Lemma 4.8, we will have the same powers of x_1. However, if from the later set of polynomials we only consider $\mathcal{T}_{N-1-d}(\xi_{N-1-d} x_1^{N-1-d})$, then the linear independence is clear, because this polynomial is equal to $\mathcal{T}_{N-1-d}(\xi_{N-1-d}) \neq 0$ at $[0 : 1]$ (because of the choice of the primitive elements), while the rest of polynomials that we are considering are 0 at $[0 : 1]$. Moreover, with these polynomials we can generate the rest of the polynomials in (5) taking into account Lemma 4.8:

$$\begin{aligned}\mathcal{T}_a(\xi_a^r x_0 x_1^a) &= \xi_a^r(x_0 + x_1^a - 1) + \xi_a^{qr}(x_0 + x_1^{qa} - 1) + \cdots + \xi_a^{q^{n_a-1}r}(x_0 + x_1^{q^{n_a-1}a} - 1)\\ &= \mathcal{T}_a(\xi_a^r)(x_0 - 1) + \mathcal{T}_a(\xi_a^r x_1^a).\end{aligned}$$

With $r = 1$ we see that we can generate $(x_0 - 1)$ with the polynomials we are considering, and with $(x_0 - 1)$ we can generate the rest of polynomials in (5), because $\mathcal{T}_a(\xi_a^r) \in \mathbb{F}_q$. □

In the case $\mathfrak{I}_{d(\Delta)} \not\subset \Delta$ of the previous result, we have seen that we can generate $(x_0 - 1)$. The evaluation of this polynomial on P^1 gives a codeword with Hamming weight 1, which means that $(\mathrm{PRS}(N, \Delta)_q)^\perp$ has minimum distance 1. This is equivalent to having that $\mathrm{PRS}(N, \Delta)_q$ is a degenerate code (it has a common zero in the coordinate associated to the point $[0 : 1]$). Once again, we see that the interesting case for us is when $\mathfrak{I}_{d(\Delta)} \subset \Delta$.

Example 4.15 We continue with Example 3.2. Let $\Delta_4 = \{0, 1, 2, 3, 4\}$, which implies $d(\Delta_4) = 4$. We are going to obtain a set of polynomials, such that its image by the evaluation map is a basis for $(\mathrm{PRS}(9, \Delta_4)_3)^\perp$. We have that $\Delta_4^\perp = \{0, 1, 2, 3\}$. The minimal cyclotomic sets $\mathcal{I}_a$ with $\mathcal{I}_a \cap \Delta^\perp \neq \emptyset$ are $\mathcal{I}_0$, $\mathcal{I}_1$ and $\mathcal{I}_2$. As in the previous examples, if ξ is a primitive element of $\mathbb{F}_9$, by Theorem 4.14, we obtain the following set of polynomials:

$$\mathcal{T}_0(x_0) = x_0, \mathcal{T}_1(x_0x_1) = x_0x_1 + x_0^3x_1^3, \mathcal{T}_1(\xi x_0x_1) = \xi x_0x_1 + \xi x_0^3x_1^3$$
$$\mathcal{T}_2(x_0x_1^2) = x_0x_1^2 + x_0^3x_1^6, \mathcal{T}_2(\xi x_0x_1^2) = \xi x_0x_1^2 + \xi^3x_0^3x_1^6, \mathcal{T}_4(x_1^4) = x_1^4.$$

In all the previous expressions, we can reduce the exponent of x_0 to 1 and the evaluation would not change.

As a consequence of Theorem 4.14, we obtain directly an explicit formula for the dimension of $(\mathrm{PRS}(N, \Delta)_q)^\perp$ without using the dimension of the primary codes from Corollary 3.7.

Corollary 4.16 *Let $\Delta \subset \{0, 1, \ldots, N-1\}$ and let $d = d(\Delta)$. The dimension of $(\mathrm{PRS}(N, \Delta)_q)^\perp$ is equal to*

$$\dim (\mathrm{PRS}(N, \Delta)_q)^\perp = \begin{cases} \sum_{a \in \mathcal{A} | \mathcal{I}_a \cap \Delta^\perp \neq \emptyset} n_a + n_d & \text{if } \mathcal{I}_d \subset \Delta \\ \sum_{a \in \mathcal{A} | \mathcal{I}_a \cap \Delta^\perp \neq \emptyset} n_a + 1 & \text{if } \mathcal{I}_d \not\subset \Delta \end{cases}$$

Now, we are going to turn our attention to the minimum distance of the dual code $(\mathrm{PRS}(N, \Delta)_q)^\perp$. In the affine case, a BCH-type bound has been used frequently for the minimum distance of the duals of the subfield subcodes of Reed–Solomon codes. If one considers the code $\mathrm{RS}(N, \Delta)$ with $\Delta = \mathcal{I}_{a_0} \cup \mathcal{I}_{a_1} \cup \cdots \cup \mathcal{I}_{a_l}$ a union of cyclotomic sets, then this code is Galois invariant in the sense of Bierbrauer (2002), i.e., $\mathrm{RS}(N, \Delta) = (\mathrm{RS}(N, \Delta))^q$. By Bierbrauer (2002, Thm. 4), we have that $\mathrm{Tr}(\mathrm{RS}(N, \Delta)) = \mathrm{RS}(N, \Delta)_q$. We can write Theorem 4.1 in the following way: $C^\perp \cap \mathbb{F}_q^n = \mathrm{Tr}(C)^\perp$. Therefore, we have that $\left(\mathrm{RS}(N, \Delta)_q\right)^\perp = \left(\mathrm{RS}(N, \Delta)^\perp\right)_q$. For $(\mathrm{RS}(N, \Delta)^\perp)_q$, it is easy to see that we have a BCH-type bound, because we can consider the generator matrix of $\mathrm{RS}(N, \Delta)$ as a pseudo-parity check matrix for the code $(\mathrm{RS}(N, \Delta)^\perp)_q$ (as we did with the matrix in (1) for BCH codes). If we have t consecutive exponents in Δ, we have a Vandermonde matrix as a submatrix of the generator matrix for $\mathrm{RS}(N, \Delta)$ and we get that $\mathrm{wt}\left((\mathrm{RS}(N, \Delta)_q)^\perp\right) \geq t + 1$.

In the projective case, arguing in a similar way, we get that, if we have t consecutive exponents in Δ, we have the BCH-type bound $\mathrm{wt}\left((\mathrm{PRS}(N, \Delta)^\perp)_q\right) \geq t + 1$. However, even if Δ is a union of cyclotomic sets, we will see in Remark 4.23 and Example 4.24 that in the projective case we do not have in general that $\mathrm{PRS}(N, \Delta)$ is Galois invariant, and thus we do not have the equality between $(\mathrm{PRS}(N, \Delta)^\perp)_q$ and $(\mathrm{PRS}(N, \Delta)_q)^\perp$ in general. Nevertheless, we can still use the affine case to get a bound for the minimum distance. If we have a code $C \subset \mathbb{F}_q^n$, we are going to denote by $(C, 0) := \{(u_1, \ldots, u_n, 0) \in \mathbb{F}_q^{n+1} \mid u = (u_1, \ldots, u_n) \in C\}$. In what follows, we are going to assume that the coordinate associated to the point $[0 : 1]$ is the last one. We recall that $\mathcal{A}$ (resp. $\mathcal{B}$) is the set of minimal representatives (resp. maximal representatives) of the minimal cyclotomic sets. We are going to denote $\Delta' := \Delta \backslash \{d\}$, and $(\Delta')_\mathcal{I} = \bigcup_{b \in \mathcal{B}, b < d | \mathcal{I}_b \subset \Delta} \mathcal{I}_b \subset \Delta'$ as before.

Proposition 4.17 *Let $\Delta \subset \{0, 1, \ldots, N-1\}$. We assume that $d(\Delta) \in \mathcal{B}$ with $\mathcal{I}_{d(\Delta)} \subset \Delta$. If t is the number of consecutive exponents in $(\Delta')_\mathcal{I}$, then we have that* $\mathrm{wt}\left((\mathrm{PRS}(N, \Delta)_q)^\perp\right) \geq t + 1$.

Proof We assume that the point $[0 : 1]$ corresponds to the last coordinate. We have $\mathrm{PRS}(N, \Delta)_q \supset (\mathrm{RS}(N, \Delta')_q, 0)$, which implies

$$(\mathrm{PRS}(N, \Delta)_q)^\perp \subset (\mathrm{RS}(N, \Delta')_q, 0)^\perp = ((\mathrm{RS}(N, \Delta')_q)^\perp, 0) + \langle (0, \ldots, 0, 1) \rangle.$$

We know that $(0, \ldots, 0, 1) \notin (\mathrm{PRS}(N, \Delta)_q)^\perp$, because that would imply that $\mathrm{PRS}(N, \Delta)_q$ is degenerate, and that is not the case because of the assumptions that we have made. Thus, any vector in $(\mathrm{PRS}(N, \Delta)_q)^\perp$ must belong to $(\mathrm{RS}(N, \Delta')_q)^\perp$ after puncturing the last coordinate, and therefore, the weight of any vector in $(\mathrm{PRS}(N, \Delta)_q)^\perp$ must be at least $t + 1$ because of the BCH-type bound for $(\mathrm{RS}(N, \Delta')_q)^\perp$. □

As a corollary, we have the following result about the duals of the subfield subcodes of doubly extended Reed–Solomon codes.

Corollary 4.18 *Let $\Delta_d = \{0, 1, \ldots, d\}$ with $d \in \mathcal{B}$. If t is the number of consecutive exponents in $(\Delta'_d)_\mathfrak{I}$, the parameters of $(\mathrm{PRS}(q^s, \Delta_d)_q)^\perp$ are $[q^s + 1, \sum_{a \in \mathcal{A} | \mathfrak{I}_a \cap \Delta^\perp \neq \emptyset} n_a, \geq t + 1]$.*

This estimate would give codes with length 1 more than in the affine case, but same dimension and same bound for the minimum distance. However, the bound for the minimum distance is not sharp in general and we are able to improve upon the affine case in many examples. For instance, in the next result we show that when $|\mathfrak{I}_d| = 1$ we have a better estimate for the minimum distance.

Proposition 4.19 *Let $\Delta \subset \{0, 1, \ldots, N - 1\}$, such that $|\mathfrak{I}_{d(\Delta)}| = 1$. Then, $\mathrm{PRS}(N, \Delta_\mathfrak{I})$ is Galois invariant, we have that $(\mathrm{PRS}(N, \Delta_\mathfrak{I})^\perp)_q = (\mathrm{PRS}(N, \Delta_\mathfrak{I})_q)^\perp = (\mathrm{PRS}(N, \Delta)_q)^\perp$, and, if there are t consecutive exponents in $\Delta_\mathfrak{I}$, the parameters of $(\mathrm{PRS}(N, \Delta)_q)^\perp$ are $[N + 1, \sum_{a \in \mathcal{A} | \mathfrak{I}_a \cap \Delta^\perp_\mathfrak{I} \neq \emptyset} n_a + 1, \geq t + 1]$.*

Proof Let $d = d(\Delta)$. We have that $\mathrm{PRS}(N, \Delta_\mathfrak{I})$ is generated by the evaluation of monomials. Because of the fact that $\Delta_\mathfrak{I}$ is a union of cyclotomic sets, we can divide the monomials into sets corresponding to different minimal cyclotomic sets. For $a \neq d$ we have the monomials

$$\{x_0 x_1^\alpha \mid \alpha \in \mathfrak{I}_a \subset \Delta\}.$$

If we consider these monomials to the power of q, the set remains invariant in $S/I(P^1)$, because the exponents of x_1 are in a cyclotomic set, and the exponent of x_0 does not change the evaluation. For $\mathfrak{I}_d$ we have that $x_1^{q(N-1-d)} \equiv x_1^{N-1-d} \mod I(P^1)$, because $|\mathfrak{I}_d| = 1$. Therefore, the set of monomials is invariant under taking powers of q, which implies that $\mathrm{PRS}(N, \Delta_\mathfrak{I}) = (\mathrm{PRS}(N, \Delta_\mathfrak{I}))^q$. Because of the previous discussion, we have that being Galois invariant implies in this case that $(\mathrm{PRS}(N, \Delta_\mathfrak{I})^\perp)_q = (\mathrm{PRS}(N, \Delta_\mathfrak{I})_q)^\perp$. Taking into account that $\mathrm{PRS}(N, \Delta_\mathfrak{I})_q = \mathrm{PRS}(N, \Delta)_q$ because of Theorem 3.4, the parameters are clear from Theorem 4.14 and the BCH-type bound. □

In many situations, the previous result gives codes with higher length and dimension than in the affine case. Assuming the hypotheses of the previous result, the affine code with $(\mathrm{RS}(N, \Delta)_q)^\perp$ would have parameters $[N, \sum_{a \in \mathcal{A} | \mathfrak{I}_a \cap \Delta^\perp_\mathfrak{I} \neq \emptyset} n_a, \geq t + 1]$, meanwhile the projective code $(\mathrm{PRS}(N, \Delta)_q)^\perp$ would have parameters $[N + 1, \sum_{a \in \mathcal{A} | \mathfrak{I}_a \cap \Delta^\perp_\mathfrak{I} \neq \emptyset} n_a + 1, \geq t + 1]$.

These codes can also be compared to $(\mathrm{RS}(N, \Delta')_q)^\perp$, with $\Delta' = \Delta \setminus \{d(\Delta)\}$. Taking into account that $|\mathfrak{I}_d| = 1$, this code has parameters $[N, \sum_{a \in \mathcal{A} | \mathfrak{I}_a \cap \Delta^\perp_\mathfrak{I} \neq \emptyset} n_a + 1, \geq t' + 1]$, where t' is the number of consecutive exponents in Δ'. We see that this code has the same

dimension as $(\mathrm{PRS}(N, \Delta)_q)^\perp$. However, the bound for the minimum distance is worse than the one for $(\mathrm{PRS}(N, \Delta)_q)^\perp$.

The following result shows many situations in which we can use Proposition 4.19 besides the obvious case with $\Delta = \{0\}$.

Lemma 4.20 *Let $q > 2$. If $d_\lambda := \lambda(N-1)/(q-1) \in \mathbb{N}$, for some λ, $1 \leq \lambda \leq q-1$, then $|I_{d_\lambda}| = 1$.*

Proof We only have to observe that

$$\lambda \frac{N-1}{q-1} q - \lambda \frac{N-1}{q-1} = \lambda(N-1) \equiv 0 \mod N-1.$$

□

Remark 4.21 If $q-1 \mid N-1$, then with the previous result we obtain $q-1$ cyclotomic sets with cardinality one besides $\mathfrak{I}_0$. For example, if $N = q^s$, then we directly have $q-1 \mid N-1$. However, that is not the only case. For example we can consider $q^s = 3^8$ and $N = 83$. In that situation it can be checked that $q-1 = 2 \mid 82 = N-1$, and we have that $|I_{41}| = 1$. In this situation, when we have $q-1 \mid N-1$, the previous result is actually a characterization of when we have $|I_d| = 1$:

$$|I_d| = 1 \iff dq \equiv d \mod N-1 \iff d(q-1) = \lambda(N-1) = \lambda(q-1)\frac{N-1}{q-1}$$
$$\iff d = \lambda \frac{N-1}{q-1}, \text{ for some } 1 \leq \lambda < q-1.$$

Example 4.22 We consider the field extension $\mathbb{F}_{16} \supset \mathbb{F}_4$, which gives the following minimal cyclotomic sets:

$$\mathfrak{I}_0 = \{0\}, \mathfrak{I}_1 = \{1, 4\}, \qquad \mathfrak{I}_2 = \{2, 8\}, \mathfrak{I}_3 = \{3, 12\}, \mathfrak{I}_5 = \{5\},$$
$$\mathfrak{I}_6 = \{6, 9\}, \mathfrak{I}_7 = \{7, 13\}, \quad \mathfrak{I}_{10} = \{10\}, \mathfrak{I}_{11} = \{11, 14\}, \mathfrak{I}_{15} = \{15\}.$$

We see that we have $|\mathfrak{I}_{10}| = 1$. If we take $\Delta = \{0, 1, 4, 10\} = \mathfrak{I}_0 \cup \mathfrak{I}_1 \cup \mathfrak{I}_{10}$, then $\Delta^\perp = \{0, 1, \ldots, N-1\} \backslash \{\mathfrak{I}_{15} \cup \mathfrak{I}_{11} \cup \mathfrak{I}_5\}$ and we can use Corollary 4.16 to compute the dimension. All the cyclotomic sets, besides $\mathfrak{I}_5$, $\mathfrak{I}_{11}$ and $\mathfrak{I}_{15}$, have nonzero intersection with $\Delta^\perp$, and we have $\mathfrak{I}_{d(\Delta)} = \mathfrak{I}_{10} \subset \Delta$. Hence, by Corollary 4.16, $\dim(\mathrm{PRS}(N, \Delta)_q)^\perp = (n_0 + n_1 + n_2 + n_3 + n_6 + n_7 + n_{10}) + n_{10} = 13$. For the minimum distance, we have $t = 2$ consecutive elements in $\Delta_{\mathfrak{I}} = \Delta$, which gives the following parameters for $(\mathrm{PRS}(N, \Delta)_q)^\perp$: $[17, 13, \geq 3]$.

We can do the same for $\Delta = \{0, 1, 2, 4, 8, 10\} = \mathfrak{I}_0 \cup \mathfrak{I}_1 \cup \mathfrak{I}_2 \cup \mathfrak{I}_{10}$, and we obtain the parameters $[17, 11, \geq 4]$. The true parameters are $[17, 13, 3]$ and $[17, 11, 4]$, which lengthen the parameters of the affine case $[16, 12, 3]$ and $[16, 10, 4]$. We see that the bound for the minimum distance coincides with the real minimum distance in this case.

Remark 4.23 If we do not assume in Proposition 4.19 that $|\mathfrak{I}_d| = 1$, then, if $d = d(\Delta) \in \mathcal{B}$ and $\mathfrak{I}_d \subset \Delta$ (which is the interesting case in the projective setting), we will have the evaluation of the monomial x_1^d in $\mathrm{PRS}(N, \Delta)$, and also the evaluation of at least one monomial $x_0^{d-a} x_1^a$ with $a \in \mathfrak{I}_d \backslash \{d\}$. We know that $d \equiv q^r a \mod N-1$ for some $r > 0$. Thus, we have the image of $x_0^{d-q^{r-1}a} x_1^{q^{r-1}a}$ in $\mathrm{PRS}(N, \Delta)$, but if we take this monomial to the power of q, we get $x_0^{q(d-q^{r-1}a)} x_1^d \not\equiv x_1^d \mod I(P^1)$. It is not hard to check that we do not have the image of this monomial in $\mathrm{PRS}(N, \Delta)$, which implies that $\mathrm{PRS}(N, \Delta)$ is not Galois invariant. In the following example we show how this affects the bound for the minimum distance.

Example 4.24 We continue with Example 4.22. We can consider $\Delta = \{0, 1, 2, 3, 4\}$, which gives $\Delta_{\mathfrak{I}} = \mathfrak{I}_0 \cup \mathfrak{I}_1$. However, we do not have $|\mathfrak{I}_4| = 1$ and Proposition 4.19 does not hold in this case. For instance, there are $t = 2$ consecutive elements in Δ, but the parameters of $(\mathrm{PRS}(N, \Delta)_q)^{\perp}$ are $[17, 15, 2]$, and $2 < t + 1 = 3$. On the other hand, we have that $(\Delta')_{\mathfrak{I}} = \mathfrak{I}_0$, which only has $t = 1$ consecutive elements, and Proposition 4.17 would give the parameters $[17, 15, \geq 2]$.

5 Applications to EAQECCs

This section is devoted to providing quantum codes from the linear codes developed in the previous section. Namely, we will construct EAQECCs using the CSS construction (Galindo et al. 2019b, Thm. 4) and the Hermitian construction (Galindo et al. 2019b, Thm. 3), as well as asymmetric EAQECCs (Galindo et al. 2020).

5.1 Euclidean EAQECCs

In this section, we will be interested in obtaining EAQECCs using the CSS construction (Galindo et al. 2019b, Thm. 4). Given a nonempty set $U \subset \mathbb{F}_q^n$, we denote by $\mathrm{wt}(U)$ the number $\min\{\mathrm{wt}(v) \mid v \in U \setminus \{0\}\}$, extending the notation that we have been using only for linear codes until now.

Theorem 5.1 (CSS Construction) *Let $C_i \subset \mathbb{F}_q^n$ be linear codes of dimension k_i, for $i = 1, 2$. Then, there is an EAQECC with parameters $[[n, \kappa, \delta; c]]_q$, where*

$$c = k_1 - \dim(C_1 \cap C_2^{\perp}), \ \kappa = n - (k_1 + k_2) + c, \ \textit{and}$$
$$\delta = \min\left\{\mathrm{wt}\left(C_1^{\perp} \setminus \left(C_1^{\perp} \cap C_2\right)\right), \mathrm{wt}\left(C_2^{\perp} \setminus \left(C_2^{\perp} \cap C_1\right)\right)\right\}.$$

We are going to introduce some new notation for the codes we are going to use. In what follows, we are assuming that $p \mid N$.

Definition 5.2 Let $\mathcal{A} = \{a_0 = 0 < a_1 < \cdots < a_j\}$, the set of minimal representatives of the minimal cyclotomic sets. We are going to consider a set $\Delta = \bigcup_{i=0}^{t-1} \mathfrak{I}_{a_i} \cup \{a_t\}$, i.e., the union of consecutive minimal cyclotomic sets with minimal representatives $a_0, \ldots, a_{t-1}$, and the minimal element a_t. For such a set Δ, we are going to consider the code $\mathcal{D}(N, \Delta)$ defined as the linear code generated by $\{\mathrm{ev}_{X_N}(x_0 x_1^{\alpha}) \mid \alpha \in \Delta \setminus \{a_t\}\} \cup \{\mathrm{ev}_{X_N}(x_1^{a_t})\}$.

Remark 5.3 If we look at the basis for the dual codes from Proposition 4.10, we see that $\mathcal{D}(N, \Delta) = \mathrm{PRS}(N, \Delta^*)^{\perp}$, with $\Delta^* = \{0, 1, \ldots, N-1\} \setminus \bigcup_{i=0}^{t-1} \mathfrak{I}_{N-1-a_i}$. In particular, the codes we are considering are not degenerate.

Although the previous remark shows that we can use the notation $\mathrm{PRS}(N, \Delta^*)^{\perp}$ instead of $\mathcal{D}(N, \Delta)$, in what follows we are going to use $\mathcal{D}(N, \Delta)$, because this will be the appropriate notation for Sect. 6. This allows us to make reference to the following proofs directly from Sect. 6, which helps to avoid repetition.

Remark 5.4 By the definitions, it is clear that $\mathcal{D}(N, \Delta) = (\mathrm{RS}(N, \Delta'), 0) + \langle \mathrm{ev}_{X_N}(x_1^{a_t}) \rangle$, where $\Delta' = \Delta \setminus \{a_t\}$. This means that $\dim \mathcal{D}(N, \Delta) = \dim \mathrm{RS}(N, \Delta') + 1 = \dim \mathrm{RS}(N, \Delta)$.

We also have that $\dim(\mathcal{D}(N,\Delta)^{\perp})_q = \dim \mathrm{PRS}(N,\Delta^*)_q = N+1-\sum_{i=0}^{t} n_{a_i}$ from Corollary 3.7. If $G_{N,\Delta}$ is a generator matrix of $\mathrm{RS}(N,\Delta)$, then we have that

$$\left(\begin{array}{c|c} G_{N,\Delta} & \begin{matrix}0\\ \vdots \\ 0\end{matrix} \\ \hline \mathrm{ev}_{Y_N}(x^{a_t}) & 1 \end{array}\right)$$

is a generator matrix of $\mathcal{D}(N,\Delta)$. We see that this does not correspond to any standard lengthening technique for linear codes. On the other hand, the BCH-type bound gives $\mathrm{wt}((\mathcal{D}(N,\Delta)^{\perp})_q) \geq \mathrm{wt}(\mathcal{D}(N,\Delta)^{\perp}) \geq a_t + 2$.

Theorem 5.5 *Let $\mathcal{A} = \{a_0 = 0 < a_1 < a_2 < \cdots < a_z\}$ be the set of minimal representatives of the cyclotomic sets $\mathfrak{I}_{a_i}$, $0 \leq i \leq z$, of $\{0,1,\ldots,N-1\}$ with respect to q. Let $\Delta = \bigcup_{i=0}^{t-1} \mathfrak{I}_{a_i} \cup \{a_t\}$, such that $\mathrm{RS}(N,\Delta'') \subset \mathrm{RS}(N,\Delta'')^{\perp}$, where $\Delta'' = \bigcup_{i=0}^{t} \mathfrak{I}_{a_i}$. Then, we can construct an EAQECC with parameters $[[n,\kappa,\geq \delta; c]]_q$, where $n = N+1$, $\kappa = N+1-2\left(\sum_{i=0}^{t} n_{a_i}\right)+c$, $\delta = a_t+2$, and $c \leq 1$.*

Proof We are going to consider the code $C_1 = C_2 = ((\mathcal{D}(N,\Delta)^{\perp})_q)^{\perp}$ for the CSS Construction 5.1. We have $\dim((\mathcal{D}(N,\Delta)^{\perp})_q)^{\perp} = N+1-\dim(\mathcal{D}(N,\Delta)^{\perp})_q = N+1-\dim \mathrm{PRS}(N,\Delta^*)_q = \sum_{i=0}^{t} n_{a_i}$ by Remark 5.4. Remark 5.4 also gives $\mathrm{wt}((\mathcal{D}(N,\Delta)^{\perp})_q) \geq a_t+2$.

For the parameter c, we claim that $\dim\left((\mathcal{D}(N,\Delta)^{\perp})_q \cap ((\mathcal{D}(N,\Delta)^{\perp})_q)^{\perp}\right) \geq \dim(\mathrm{RS}(N,\Delta'')_q,0) - 1 = \sum_{i=0}^{t} n_{a_i} - 1$, which gives $c \leq 1$. Let $\Delta' = \Delta\backslash\{a_t\}$. By Remark 5.4 we have $\mathcal{D}(N,\Delta) = (\mathrm{RS}(N,\Delta'),0) + \langle \mathrm{ev}_{X_N}(x_1^{a_t})\rangle$.

We consider $v \in (\mathrm{RS}(N,\Delta)^{\perp},0)$. Then, v is orthogonal to $(\mathrm{RS}(N,\Delta'),0)$ (taking into account that $\mathrm{RS}(N,\Delta') \subset \mathrm{RS}(N,\Delta)$), and it is also orthogonal to $\mathrm{ev}_{X_N}(x_1^{a_t})$, because the last coordinate of v is 0, which means that $v \cdot \mathrm{ev}_{X_N}(x_1^{a_t}) = v \cdot \mathrm{ev}_{X_N}(x_0 x_1^{a_t})$, and $\mathrm{ev}_{X_N}(x_0 x_1^{a_t}) \in (\mathrm{RS}(N,\Delta),0)$. Therefore, $v \in \mathcal{D}(N,\Delta)^{\perp}$. Taking into account the dimension and the fact that the codes $\mathcal{D}(N,\Delta)^{\perp}$ are not degenerate, we can write $\mathcal{D}(N,\Delta)^{\perp} = (\mathrm{RS}(N,\Delta)^{\perp},0) + \langle w\rangle$, where w is a vector with a nonzero last entry.

We consider a basis for $(\mathcal{D}(N,\Delta)^{\perp})_q$ now, and we can also assume that all the vectors in the basis, besides one vector w', have 0 as their last coordinate. Taking into account that $(\mathcal{D}(N,\Delta)^{\perp})_q$ is not degenerate, this means that we have $(\mathcal{D}(N,\Delta)^{\perp})_q = ((\mathrm{RS}(N,\Delta)^{\perp})_q,0) + \langle w'\rangle$ for some vector w' with nonzero last coordinate. In this case we have $(\mathrm{RS}(N,\Delta)^{\perp})_q = (\mathrm{RS}(N,\Delta'')^{\perp})_q$, because $\Delta^{\perp}$ and $\Delta''^{\perp}$ contain the same complete minimal cyclotomic sets (which is what matters to compute the subfield subcode of the dual, this can be seen using Theorem 2.2 and Galindo and Hernando 2015, Prop. 3). Moreover, we have that $\mathrm{RS}(N,\Delta'')_q \subset (\mathrm{RS}(N,\Delta'')^{\perp})_q = (\mathrm{RS}(N,\Delta'')_q)^{\perp}$, because this code is Galois invariant by the reasoning after Corollary 4.16.

Thus, we have seen that $(\mathcal{D}(N,\Delta)^{\perp})_q \supset ((\mathrm{RS}(N,\Delta'')^{\perp})_q,0) \supset (\mathrm{RS}(N,\Delta'')_q,0)$. On the other hand, we have

$$((\mathcal{D}(N,\Delta)^{\perp})_q)^{\perp} = \left((\mathrm{PRS}(N,\Delta'')_q,0) + \langle(0,0,\ldots,0,1)\rangle\right) \cap \langle w'\rangle^{\perp}.$$

Note that $(0,0,\ldots,0,1) \notin \langle w'\rangle^{\perp}$, because w' has a nonzero last coordinate. Hence, we can consider a basis for $((\mathcal{D}(N,\Delta)^{\perp})_q)^{\perp}$ formed by $(\dim \mathrm{RS}(N,\Delta'')_q - 1)$ vectors $u_i \in (\mathrm{RS}(N,\Delta'')_q,0)$, and a vector w'', such that its last coordinate is nonzero. Note that not all vectors can have the last coordinate equal to 0 because that would mean that we have the vector $(0,0,\ldots,0,1) \in (\mathcal{D}(N,\Delta)^{\perp})_q$, contradicting the bound given for the minimum

distance. Therefore, all the vectors u_i are in $(\mathcal{D}(N, \Delta)^{\perp})_q \cap ((\mathcal{D}(N, \Delta)^{\perp})_q)^{\perp}$, which gives $c \leq 1$. □

Remark 5.6 In Galindo et al. (2015), there are conditions to have $\mathrm{RS}(N, \Delta'') \subset \mathrm{RS}(N, \Delta'')^{\perp}$. For example, for the type of set Δ'' that we are considering in Theorem 5.5, if, for every cyclotomic set $\mathfrak{I}_a \subset \Delta''$, we have $\mathfrak{I}_{N-1-a} \not\subset \Delta''$, then $\mathrm{RS}(N, \Delta'') \subset \mathrm{RS}(N, \Delta'')^{\perp}$.

For the code $\mathrm{RS}(N, \Delta'')^{\perp}$ we have the bound $\mathrm{wt}(\mathrm{RS}(N, \Delta'')^{\perp}) \geq a_{t+1} + 1$. However, we have $a_{t+1} + 1 = a_t + 2$ in many cases (this happens if and only if $a_t + 1 \notin \Delta''$, because in that case $a_{t+1} = a_t + 1$). In that situation, we have the same bound for the minimum distance for $\mathrm{RS}(N, \Delta'')^{\perp}$ and for the corresponding EAQECC from Theorem 5.5. In the following discussion we will assume that $a_{t+1} + 1 = a_t + 2$.

If we get a QECC with parameters $[[n, \kappa, \delta; 0]]_q$ from the affine case using $\mathrm{RS}(N, \Delta'')_q$, then we would get an EAQECC with parameters $[[n + 1, \kappa + 1 + c, \delta; c]]_q$ in the projective case using Theorem 5.5, where $c \leq 1$. If we take into account the rate $\rho := \kappa/n$ and the net rate $\overline{\rho} := (\kappa - c)/n$, we see that the code obtained with Theorem 5.5 has better rate and net rate than the one obtained in the affine case. Moreover, it can be checked that the codes we obtain are not directly obtainable from the affine case using the propagation rules from Luo et al. (2022), which can be adapted for EAQECCs arising from Theorem 5.1 (for example, see Anderson et al. 2022).

In the constructions from Theorems 5.15 and 6.6, the same argument shows that, as long as $a_{t+1} + 1 = a_t + 2$, we can obtain codes with better rates than the ones from the affine case, which cannot be deduced from the propagation rules from Luo et al. (2022).

Example 5.7 We consider $N = q^s = 3^4 = 81$, with $q = 3^2$ ($s = 2$). The first minimal cyclotomic sets, ordered by their minimal element, are

$$\mathfrak{I}_0 = \{0\},\ \mathfrak{I}_1 = \{1, 9\},\ \mathfrak{I}_2 = \{2, 18\},\ \mathfrak{I}_3 = \{3, 27\},\ \mathfrak{I}_4 = \{4, 36\},\ \mathfrak{I}_5 = \{5, 45\}.$$

With the notation that we have been using, we consider the minimal elements a_i, for $i = 0, \ldots, 5$, and $\Delta = \bigcup_{i=0}^{4} \mathfrak{I}_{a_i} \cup \{5\}$ ($t = 5$ with the previous notation). We have $\sum_{i=0}^{5} n_{a_i} = 11$, and we have $a_t + 2 = 7$. It is easy to check that $\mathfrak{I}_{N-1-a_i} \not\subset \Delta$ for $i = 0, \ldots, 5$. By Remark 5.6 we have $\mathrm{RS}(N, \Delta'') \subset \mathrm{RS}(N, \Delta'')^{\perp}$ and we can apply Theorem 5.5 to obtain a quantum code with parameters $[[82, 61, 7; 1]]_9$. If we had used the affine code $\mathrm{RS}(N, \Delta'')$ with $\Delta'' = \bigcup_{i=0}^{5} \mathfrak{I}_{a_i}$, the bound for the minimum distance would have been the same, because $a_t + 1 = 8 \notin \Delta''$, and we would have obtained the code $[[81, 59, 7; 0]]_9$.

We can also get QECCs (EAQECCs with $c = 0$) directly under some assumptions, as the following result shows.

Proposition 5.8 *Assume that $p > 2$. Let N be an odd integer, such that $N - 1 \mid q^s - 1$ and $p \mid N$. We consider a union of cyclotomic sets $\Delta \subset \{0, 1, \ldots, N - 1\}$, such that $d = d(\Delta) = (N - 1)/2$. If t is the number of consecutive exponents in Δ, then we can construct a QECC with parameters $[[n, \kappa, \geq \delta; 0]]_q$, where $n = N + 1$, $\kappa = N + 1 - 2|\Delta|$, and $\delta = t + 1$.*

Proof By Proposition 4.19, Lemma 4.20 and Remark 5.3, we have that $\mathrm{PRS}(N, \Delta)$ is Galois invariant, and we have $\mathrm{wt}((\mathrm{PRS}(N, \Delta)_q)^{\perp}) \geq t + 1$. By Corollary 4.11, if we consider $\Delta_d = \{0, 1, \ldots, (N - 1)/2\}$, we have that

$$\mathrm{PRS}(N, \Delta) \subset \mathrm{PRS}(N, \Delta_d) = \mathrm{PRS}(N, \Delta_d)^{\perp} \subset \mathrm{PRS}(N, \Delta)^{\perp}.$$

Therefore, considering the intersection with $\mathbb{F}_q^n$ we obtain that $\mathrm{PRS}(N,\Delta)_q \subset (\mathrm{PRS}(N,\Delta)_q)^{\perp}$. If we consider $C_1 = C_2 = \mathrm{PRS}(N,\Delta)_q$ in the CSS Construction 5.1, we have already obtained the length, the bound for the minimum distance, and $c = 0$, for the parameters of the corresponding quantum error-correcting code. For the dimension, we have $\dim \mathrm{PRS}(N,\Delta)_q = |\Delta|$ by Corollary 3.7, taking into account that $|\mathfrak{I}_d| = 1$ in this case by Lemma 4.20. □

Example 5.9 We consider $q^s = 3^3, q = 3$ and $N = 3^3 = 27$. Let $\Delta = \mathfrak{I}_0 \cup \mathfrak{I}_1 \cup \mathfrak{I}_4 \cup \mathfrak{I}_{13}$ (note that $13 = (N-1)/2$). We are not considering consecutive cyclotomic sets, which means that the BCH-type bound for the minimum distance might not be accurate. Hence, we have computed it directly with Magma (Bosma et al. 1997). The code $(\mathrm{PRS}(N,\Delta)_q)^{\perp}$ has parameters [28, 20, 6], which gives a QECC with parameters $[[28, 12, 6; 0]]_3$ by Proposition 5.8, which are the best known parameters for a quantum code over $\mathbb{F}_3$ with that length and dimension according to Grassl (2007). With $\mathrm{RS}(N,\Delta)$ and $\mathrm{RS}(N,\Delta')$ (where $\Delta' = \Delta \setminus \{(N-1)/2\}$), we obtain the parameters [27, 19, 6] and [27, 20, 5] for the dual codes of their subfield subcodes, respectively. These codes would give QECCs with parameters $[[27, 11, 6; 0]]_3$ and $[[27, 13, 5; 0]]_3$, respectively, applying the CSS Construction 5.1.

5.2 Asymmetric EAQECCs

As we said in the introduction, phase-shift and qudit-flip errors are not equally likely to occur. It is, therefore, desirable to obtain EAQECCs with different error correction capabilities for each of these types of errors. To construct asymmetric EAQECCs, we can use the following result from Galindo et al. (2020).

Theorem 5.10 *Let $C_i \subset \mathbb{F}_q^n$ be linear codes of dimension k_i, for $i = 1, 2$. Then, there is an asymmetric EAQECC with parameters $[[n, \kappa, \delta_z/\delta_x; c]]_q$, where*

$$c = k_1 - \dim(C_1 \cap C_2^{\perp}),\ \kappa = n - (k_1 + k_2) + c,$$
$$\delta_z = \mathrm{wt}\left(C_1^{\perp} \setminus \left(C_1^{\perp} \cap C_2\right)\right) \text{ and } \delta_x = \mathrm{wt}\left(C_2^{\perp} \setminus \left(C_2^{\perp} \cap C_1\right)\right).$$

The two minimum distances δ_z and δ_x give the error correction capability of the corresponding asymmetric EAQECC, which can correct up to $\lfloor(\delta_z - 1)/2\rfloor$ phase-shift errors and $\lfloor(\delta_x - 1)/2\rfloor$ qudit-flip errors.

In Sects. 3 and 4, we obtained bases for both the primary codes $\mathrm{PRS}(N,\Delta)_q$ and their duals $(\mathrm{PRS}(N,\Delta)_q)^{\perp}$. This is the key for the proof of the following result, which allows us to construct asymmetric EAQECCs from subfield subcodes of projective Reed–Solomon codes. We recall that, for $\Delta \subset \{0, 1, \ldots, N-1\}$, we denote $\Delta_{\mathfrak{I}} = \bigcup_{\mathfrak{I}_a \subset \Delta} \mathfrak{I}_a$, and we also recall that $\mathcal{B}$ is the set of maximal representatives of the minimal cyclotomic sets.

Theorem 5.11 *Let $1 \le d_1, d_2 \le N-1$, such that $d_i \in \mathcal{B}$, for $i = 1, 2$, and $p \mid N$. We consider $\Delta_{d_i} = \{0, 1, \ldots, d_i\}$ and we denote $\Delta'_{d_i} := \Delta_{d_i} \setminus \{d_i\}$, for $i = 1, 2$. If $((\Delta'_{d_1})_{\mathfrak{I}})^{\perp} \subset (\Delta'_{d_2})_{\mathfrak{I}}$, then we can construct an asymmetric EAQECC with parameters*

$$\left[\left[N+1, \sum_{b\in\mathcal{B}, b<d_1} n_b + \sum_{b\in\mathcal{B}, b<d_2} n_b + 2 - N, \delta_z/\delta_x; 1\right]\right]_q,$$

where $\delta_z \ge N - d_1 + 1$, $\delta_x \ge N - d_2 + 1$.

Proof We are going to consider $C_i = (\mathrm{PRS}(N, \Delta_{d_i})_q)^\perp$, for $i = 1, 2$, and we are going to use Theorem 5.10. The bounds for δ_z and δ_x are clear, and we obtain the dimension using Corollary 3.7 if we assume $c = 1$. For the parameter $c = \dim(\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp - \dim((\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp \cap \mathrm{PRS}(N, \Delta_{d_2})_q)$, we are going to study $\dim((\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp \cap \mathrm{PRS}(N, \Delta_{d_2})_q)$. For $(\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp$ we have the basis given by the evaluation of the following set from Theorem 4.14:

$$\bigcup_{a \in \mathcal{A} \mid \mathfrak{I}_a \cap \Delta_{d_1}^\perp \neq \emptyset} \{\mathcal{T}_a(\xi_a^r x_0 x_1^a) \mid 0 \leq r \leq n_a - 1\} \cup$$
$$\{\mathcal{T}_{N-1-d_1}(\xi_{N-1-d_1}^r x_1^{N-1-d_1}) \mid 0 \leq r \leq n_{d_1} - 1\}. \tag{6}$$

From Theorem 3.4 it is easy to obtain that the evaluation of the following set gives a basis for $\mathrm{PRS}(N, \Delta_{d_2})_q$:

$$\bigcup_{a \in \mathcal{A} \mid \mathfrak{I}_a \subset \Delta'_{d_2}} \{\mathcal{T}_a(\xi_a^r x_0 x_1^a) \mid 0 \leq r \leq n_a - 1\} \cup \{\mathcal{T}_{d_2}^h(x_1^{d_2})\}. \tag{7}$$

It is also clear that the $a \in \mathcal{A}$, such that $\mathfrak{I}_a \cap \Delta_{d_1}^\perp \neq \emptyset$ are precisely the $a \in \mathcal{A}$, such that $\mathfrak{I}_a \subset ((\Delta_{d_1})_\mathfrak{I})^\perp$. We also have that $((\Delta'_{d_1})_\mathfrak{I})^\perp = ((\Delta_{d_1})_\mathfrak{I})^\perp \cup \mathfrak{I}_{N-1-d_1}$. Therefore, taking into account the assumption $((\Delta'_{d_1})_\mathfrak{I})^\perp \subset (\Delta'_{d_2})_\mathfrak{I} \subset \Delta'_{d_2}$, we have that all the traces of monomials of the type $x_0 x_1^a$, with $a \in \mathcal{A}$, in the set from (6), are contained in the set from (7). This implies that the evaluation of the set

$$\bigcup_{a \in \mathcal{A} \mid \mathfrak{I}_a \cap \Delta_{d_1}^\perp \neq \emptyset} \{\mathcal{T}_a(\xi_a^r x_0 x_1^a) \mid 0 \leq r \leq n_a - 1\} \tag{8}$$

is in $(\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp \cap \mathrm{PRS}(N, \Delta_{d_2})_q$.

Now we are going to study which polynomials from the set generated by

$$\{\mathcal{T}_{N-1-d_1}(\xi_{N-1-d_1}^r x_1^{N-1-d_1}) \mid 0 \leq r \leq n_{d_1} - 1\}$$

have their evaluation in $(\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp \cap \mathrm{PRS}(N, \Delta_{d_2})_q$. As in Theorem 4.14, we assume that ξ_{N-1-d_1} is a primitive element of $\mathbb{F}_{q^{n_{d_1}}}$ (note that $n_{d_1} = n_{N-1-d_1}$), such that $\mathcal{T}_{N-1-d_1}(\xi_{N-1-d_1}) \neq 0$. For ease of notation, we are going to denote now $d'_1 = N - 1 - d_1$. For $0 \leq r \leq n_{d_1} - 1$, $r \neq 1$, we have

$$\begin{aligned} &\mathcal{T}_{d'_1}(\xi_{d'_1})\mathcal{T}_{d'_1}(\xi_{d'_1}^r x_0 x_1^{d'_1}) - \mathcal{T}_{d'_1}(\xi_{d'_1}^r)\mathcal{T}_{d'_1}(\xi_{d'_1} x_0 x_1^{d'_1}) \\ &\quad \equiv \mathcal{T}_{d'_1}(\xi_{d'_1})\mathcal{T}_{d'_1}(\xi_{d'_1}^r x_1^{d'_1}) - \mathcal{T}_{d'_1}(\xi_{d'_1}^r)\mathcal{T}_{d'_1}(\xi_{d'_1} x_1^{d'_1}) \bmod I(X_N). \end{aligned} \tag{9}$$

This is easy to see, because when we set $x_0 = 1$, we obtain the same polynomials at each side, which means that they have the same evaluation in $[\{1\} \times Y_N]$, and both polynomials evaluate to 0 in $[0 : 1]$. Therefore, they have the same evaluation in X_N. Because of the assumption $((\Delta'_{d_1})_\mathfrak{I})^\perp = ((\Delta_{d_1})_\mathfrak{I})^\perp \cup \mathfrak{I}_{d'_1} \subset (\Delta'_{d_2})_\mathfrak{I}$, we obtain $\mathfrak{I}_{d'_1} \subset \Delta'_{d_2}$ and it is clear that we have the evaluation of the polynomial in the left-hand side of (9) in $\mathrm{PRS}(N, \Delta_{d_2})_q$ if we consider the basis from (7). The evaluation of the polynomial in the right-hand side is clearly in $(\mathrm{PRS}(N, \Delta_{d_1})_q)^\perp$ (see (6)). Thus, we have proved that the image by the evaluation map of the polynomials in the set

$$\{\mathcal{T}_{d'_1}(\xi_{d'_1})\mathcal{T}_{d'_1}(\xi_{d'_1}^r x_0 x_1^{d'_1}) - \mathcal{T}_{d'_1}(\xi_{d'_1}^r)\mathcal{T}_{d'_1}(\xi_{d'_1} x_0 x_1^{d'_1}) \mid 0 \leq r \leq n_{d_1} - 1, r \neq 1\} \tag{10}$$

is in $(\mathrm{PRS}(N, \Delta_{d_1})_q)^{\perp} \cap \mathrm{PRS}(N, \Delta_{d_2})_q$.

Hence, the evaluation of the union of the sets from (8) and (10) is in $(\mathrm{PRS}(N, \Delta_{d_1})_q)^{\perp} \cap \mathrm{PRS}(N, \Delta_{d_2})_q$, and it is easy to see that the evaluation of this union is linearly independent. Taking into account the basis from (6), we obtain that $\dim((\mathrm{PRS}(N, \Delta_{d_1})_q)^{\perp} \cap \mathrm{PRS}(N, \Delta_{d_2})_q) \geq \dim((\mathrm{PRS}(N, \Delta_{d_1})_q)^{\perp}) - 1$, i.e., $c \leq 1$.

On the other hand, having $c = 0$ means that $(\mathrm{PRS}(N, \Delta_{d_1})_q)^{\perp} \subset \mathrm{PRS}(N, \Delta_{d_2})_q$. This implies that the evaluation of all the traces appearing in (9) are in $\mathrm{PRS}(N, \Delta_{d_2})_q$. However, the evaluations of $\mathcal{T}_{d_1'}(\xi_{d_1'} x_0 x_1^{d_1'})$ and $\mathcal{T}_{d_1'}(\xi_{d_1'} x_1^{d_1'})$ differ only at the coordinate associated to the point $[0 : 1]$. This would imply that the minimum distance of $\mathrm{PRS}(N, \Delta_{d_2})_q$ is 1, a contradiction. Therefore, $c = 1$. □

Remark 5.12 We note that in the previous result we have that $(\Delta_d')_{\mathfrak{I}} = \bigcup_{b \in \mathcal{B} | b < d} \mathfrak{I}_b$.

As we said in the introduction, it is desirable to obtain asymmetric quantum codes with higher error-correction capability for phase-shift errors, i.e. with $\delta_z > \delta_x$. For the codes obtained using Theorem 5.11, this corresponds to choosing $d_1 < d_2$.

In the next example we show that we are able to obtain codes which are better than the ones available in the current literature.

Example 5.13 We consider the extension $\mathbb{F}_{16} \supset \mathbb{F}_4$, which is the setting from Example 4.22. We choose $d_1 = 14$, $d_2 = 15$, and apply Theorem 5.11, which gives the parameters $[[17, 14, 3/2; 1]]_4$. In Galindo et al. (2020), we can find a code with parameters $[[15, 12, 3/2; 1]]_4$ using BCH codes. We see that the code we have obtained has better rate κ/n, and also better net rate $(\kappa - c)/n$.

If we consider the extension $\mathbb{F}_{25} \supset \mathbb{F}_5$ instead, and choose $d_1 = 22$, $d_2 = 23$, we obtain a code with parameters $[[26, 19, 4/3; 1]]_5$ using Theorem 5.11. It is possible to adapt the propagation rules from Luo et al. (2022) to asymmetric EAQECCs arising from Theorem 5.10. For example, we can reduce the length by using extra entanglement, provided that $c \leq n - \kappa - 2$:

$$[[n, \kappa, \delta_z/\delta_x; c]]_q \to [[n-1, \kappa, \delta_z/\delta_x; c+1]]_q. \tag{11}$$

In Galindo et al. (2020) a code with parameters $[[24, 19, 4/3; 3]]_5$ is presented, which can be obtained from our code with parameters $[[26, 19, 4/3; 1]]_5$ by applying (11) two times. In this sense, we can say that the parameters $[[24, 19, 4/3; 3]]_5$ appearing in Galindo et al. (2020) are a consequence of the parameters $[[26, 19, 4/3; 1]]_5$ that we obtain with Theorem 5.11.

Finally, if we consider the extension $\mathbb{F}_{64} \supset \mathbb{F}_8$, for $d_1 = 60$ and $d_2 = 63$, we obtain the parameters $[[65, 58, 5/2; 1]]_8$, which give a better rate and net rate than the code with parameters $[[63, 56, 5/2; 1]]_8$ from Galindo et al. (2020). If we choose $d_1 = 58$ and $d_2 = 62$ instead, we obtain the parameters $[[65, 52, 7/3; 1]]_8$, which, after using the propagation rule (11) as before, give the parameters $[[63, 52, 7/3; 3]]_8$ that appear in Galindo et al. (2020).

If we do not assume $((\Delta_{d_1}')_{\mathfrak{I}})^{\perp} \subset (\Delta_{d_2}')_{\mathfrak{I}}$ in Theorem 5.11, then we would obtain instead the parameters $[[N+1, \sum_{b \in \mathcal{B}, b < d_1} n_b + \sum_{b \in \mathcal{B}, b < d_2} n_b + 1 + c - N, \delta_z/\delta_x; c]]_q$, for $c = \dim(\mathrm{PRS}(N, \Delta_{d_1})_q)^{\perp} - \dim((\mathrm{PRS}(N, \Delta_{d_1})_q)^{\perp} \cap \mathrm{PRS}(N, \Delta_{d_2})_q)$.

5.3 Hermitian EAQECCs

In the Hermitian case, we have to work with three different fields. Hence, we are going to change the notation from the previous sections. We consider the field extension $\mathbb{F}_{q^{2\ell}} \supset \mathbb{F}_{q^2}$,

where $q^{2\ell} = p^{2r}, q = p^s$, for some $r, s > 0$, and $r = \ell s$. Thus, in what follows we are going to obtain codes of length $n = N + 1$, where $N > 1$ is an integer, such that $N - 1 \mid q^{2\ell} - 1$.

As before, we are going to consider the set $\mathbb{Z}_N = \{0\} \cup \{1, 2, \ldots, N-1\}$, where $\{1, 2, \ldots, N-1\}$ is regarded as the set of representatives of the ring $\mathbb{Z}/(N-1)\mathbb{Z}$. We consider the cyclotomic sets with respect to q^2 over $\{0, 1, \ldots, N-1\}$. We call $\mathcal{A}$ the set of minimal elements of the different cyclotomic sets. We introduce now the Hermitian construction (Galindo et al. 2019b, Thm. 3) that we are going to use.

Theorem 5.14 (Hermitian construction) *Let $C \subset \mathbb{F}_{q^2}^n$ be a linear code of dimension k and $C^{\perp_h}$ its Hermitian dual. Then, there is an EAQECC with parameters $[[n, \kappa, \delta; c]]_q$, where*

$$c = k - \dim(C \cap C^{\perp_h}), \ \kappa = n - 2k + c, \ \text{and} \ \delta = \mathrm{wt}(C^{\perp_h} \setminus (C \cap C^{\perp_h})).$$

We are only going to consider the Hermitian product over $\mathbb{F}_{q^2}$. Therefore, for $a, b \in \mathbb{F}_{q^2}^n$ we have

$$a \cdot_h b := \sum_{i=0}^{n} a_i b_i^q.$$

In what follows, when considering a power of a code or a vector, we will be considering the component-wise power, i.e., $C^q := \{c^q := (c_1^q, \ldots, c_n^q) \mid c = (c_1, \ldots, c_n) \in C\}$. It is easy to check that, for codes over $\mathbb{F}_{q^2}$, we have that $C^\perp = (C^{\perp_h})^q$, where $C^{\perp_h}$ denotes the Hermitian dual.

Theorem 5.15 *Let $\mathcal{A} = \{a_0 = 0 < a_1 < a_2 < \cdots < a_z\}$ be the set of minimal representatives of the cyclotomic sets $\mathfrak{I}_{a_i}$, $0 \le i \le z$, of $\{0, 1, \ldots, N-1\}$ with respect to q^2. Let $\Delta = \bigcup_{i=0}^{t-1} \mathfrak{I}_{a_i} \cup \{a_t\}$, such that $\mathrm{RS}(N, \Delta'')_{q^2} \subset (\mathrm{RS}(N, \Delta'')_{q^2})^{\perp_h}$, where $\Delta'' = \bigcup_{i=0}^{t} \mathfrak{I}_{a_i}$. Then, we can construct an EAQECC with parameters $[[n, \kappa, \geq \delta; c]]_q$, where $n = N + 1$, $\kappa = N + 1 - 2\left(\sum_{i=0}^{t} n_{a_i}\right) + c$, $\delta = a_t + 2$ and $c \le 1$.*

Proof We are going to consider the code $C = ((\mathcal{D}(N, \Delta)^\perp)_{q^2})^{\perp_h}$ for the Hermitian construction 5.14. Using what we obtained in Theorem 5.5, the only thing left to prove is the statement about the parameter c.

Following the proof of Theorem 5.5, we have $(\mathcal{D}(N, \Delta)^\perp)_{q^2} = ((\mathrm{RS}(N, \Delta'')^\perp)_{q^2}, 0) + \langle w' \rangle$ for some vector w' with nonzero last coordinate. Therefore, we see that $\dim((\mathcal{D}(N, \Delta)^\perp)_{q^2})^{\perp_h} = \dim \mathrm{RS}(N, \Delta'')_{q^2} = \dim((\mathrm{RS}(N, \Delta'')^\perp)_{q^2})^{\perp_h}$. Moreover, we have

$$\begin{aligned}((\mathrm{RS}(N, \Delta'')^\perp)_{q^2})^{\perp_h} &= ((\mathrm{RS}(N, \Delta'')_{q^2})^\perp)^{\perp_h} = (((\mathrm{RS}(N, \Delta'')_{q^2})^\perp)^\perp)^q \\ &= \left(\mathrm{RS}(N, \Delta'')_{q^2}\right)^q.\end{aligned}$$

Thus, we obtain

$$((\mathcal{D}(N, \Delta)^\perp)_{q^2})^{\perp_h} = (((\mathrm{PRS}(N, \Delta'')_{q^2})^q, 0) + \langle (0, 0, \ldots, 0, 1) \rangle) \cap \langle (w') \rangle^{\perp_h}.$$

Note that $(0, 0, \ldots, 0, 1) \notin \langle (w') \rangle^{\perp_h}$, because w' has a nonzero last coordinate. We can consider a basis for $((\mathcal{D}(N, \Delta)^\perp)_{q^2})^{\perp_h}$ formed by $(\dim \mathrm{RS}(N, \Delta'')_{q^2} - 1)$ vectors $u_i \in ((\mathrm{RS}(N, \Delta'')_{q^2})^q, 0)$, and a vector w, such that its last coordinate is nonzero (not all vectors can have the last coordinate equal to 0 because that would mean that we have the vector $(0, 0, \ldots, 0, 1) \in (\mathcal{D}(N, \Delta)^\perp)_{q^2}$, contradicting the bound given for the minimum distance).

By our hypothesis, we have $\mathrm{RS}(N,\Delta'')_{q^2} \subset (\mathrm{RS}(N,\Delta'')_{q^2})^{\perp_h}$. This implies that $\big(\mathrm{RS}(N,\Delta'')_{q^2}\big)^q \subset \big((\mathrm{RS}(N,\Delta'')_{q^2})^{\perp_h}\big)^q = (\mathrm{RS}(N,\Delta'')_{q^2})^{\perp} = (\mathrm{RS}(N,\Delta'')^{\perp})_{q^2}$. Taking into account that $(\mathcal{D}(N,\Delta)^{\perp})_{q^2} \supset ((\mathrm{RS}(N,\Delta'')^{\perp})_{q^2},0) \supset ((\mathrm{RS}(N,\Delta'')_{q^2})^q,0)$, we see that the vectors u_i are in $(\mathcal{D}(N,\Delta)^{\perp})_{q^2}$ as well, and we obtain the desired inequality for the dimension of the intersection. □

Remark 5.16 From Galindo et al. (2015, Prop. 3) we can obtain conditions to have $\mathrm{RS}(N,\Delta'')_{q^2} \subset (\mathrm{RS}(N,\Delta'')_{q^2})^{\perp_h}$, like the one we show next. Let $\Delta'' = \bigcup_{i=0}^{t} \mathfrak{I}_{a_i}$, and we denote by a_i' the minimal element in $\mathcal{A}$, such that $\mathfrak{I}_{a_i'} = \mathfrak{I}_{-qa_i}$. Assuming $d(\Delta) < N-1$, if $\Delta'' \subset (\Delta'')^{\perp_h} := \{0,1,\ldots,N-1\} \setminus \bigcup_{i=0}^{t} \mathfrak{I}_{a_i'}$, then we have $\mathrm{RS}(N,\Delta'')_{q^2} \subset (\mathrm{RS}(N,\Delta'')_{q^2})^{\perp_h}$.

Example 5.17 We continue with the setting from Example 5.7. It is easy to check that the set Δ in Example 5.7 satisfies $\Delta \subset \Delta^{\perp_h}$, and by Remark 5.16 and Theorem 5.15 we obtain a quantum code with parameters $[[82, 67, 7; 1]]_3$.

With the construction from Theorem 5.15 we can obtain several quantum codes over $\mathbb{F}_2$ whose parameters do not appear in the table of EAQECCs from Grassl (2007), and therefore, we improve the table. With the extension $\mathbb{F}_{2^4} \supset \mathbb{F}_{2^2}$, we can obtain a code with parameters $[[17, 12, 3; 1]]_2$, which is not in the table from Grassl (2007). We can consider now the following propagation rule from Luo et al. (2022): let C be an EAQECC with parameters $[[n,\kappa,\delta;c]]_q$ obtained from Theorem 5.14 (for example, the codes from Theorem 5.15). If $c \leq n-\kappa-2$, then we can reduce the length using extra entanglement:

$$[[n,\kappa,\delta;c]]_q \to [[n-1,\kappa,\delta;c+1]]_q. \tag{12}$$

Iterating this rule, it is easy to check that, from an EAQECC with parameters $[[n,\kappa,\delta;c]]_q$, one can obtain EAQECCs with parameters $[[n-s,\kappa,\delta;c+s]]_q$, $s=1,\ldots,(n-\kappa-c)/2$. Note that the maximum value for c is $k = \dim C$, where C is the classical code used for Theorem 5.14, and for the maximum value of s that we have stated we have precisely that $c+s=k$:

$$c+s = c+\frac{n-\kappa-c}{2} = c+\frac{2k-2c}{2} = k.$$

Applying the propagation rule (12) to the parameters $[[17, 12, 3; 1]]_2$, we obtain $[[16, 12, 3; 2]]_2$ and $[[15, 12, 3; 3]]_2$, which are also missing in the table (Grassl 2007).

For the extension $\mathbb{F}_{2^6} \supset \mathbb{F}_{2^2}$, we obtain codes with length 65, which is greater than the current maximum length in Grassl (2007) for EAQECCs over $\mathbb{F}_2$. Nevertheless, we can reduce the length with the propagation rule (12) and check if the corresponding parameters are in the table. A code with parameters $[[64, 58, 3; 2]]_2$, whose parameters are missing in Grassl (2007), is obtained from the code with parameters $[[65, 58, 3; 1]]_2$ derived from Theorem 5.15 using (12). Moreover, by applying the propagation rule (12) to the code with parameters $[[65, 40, 7; 1]]_2$ deduced from Theorem 5.15, we obtain codes with parameters $[[65-i, 40, 7; 1+i]]_2$, for $i = 1, 2, \ldots, 12$, whose parameters are also missing in Grassl (2007).

In total, we obtain in this way 16 EAQECCs over $\mathbb{F}_2$ whose parameters are missing in Grassl (2007).

The table of EAQECCs from Grassl (2007) also covers codes over $\mathbb{F}_3$. However, the smaller length that we can achieve with Theorem 5.15 over $\mathbb{F}_3$ would be $3^4+1 = 82$, much higher than the current maximum length in the table from Grassl (2007) for this case. For

example, we obtain codes with parameters $[[82, 77, 3; 1]]_3$, $[[82, 73, 4; 1]]_3$, $[[82, 69, 5; 1]]_3$ and $[[82, 65, 6; 1]]_3$.

6 Evaluating at the trace roots

In this section, following the ideas from Galindo et al. (2019c), we are going to consider evaluation codes over the roots of a suitable trace polynomial. In Galindo et al. (2019c), the authors considered the trace polynomial over $\mathbb{F}_{q^{2\ell}}$ with respect to $\mathbb{F}_q$ defined as

$$\mathrm{Tr}_\ell(x) = x + x^q + x^{q^2} + \cdots + x^{q^{2\ell-1}}.$$

Let $Y_{\mathrm{Tr}_\ell} = \{\alpha \in \mathbb{F}_{q^{2\ell}} \mid \mathrm{Tr}_\ell(\alpha) = 0\}$. It is well known that $|Y_{\mathrm{Tr}_\ell}| = q^{2\ell-1}$. In Galindo et al. (2019c), evaluation codes over the roots of the trace are defined, obtaining codes with length $q^{2\ell-1}$, and bounds for the dimension and minimum distance of these codes are found. In this section, we are going to do a similar thing over the projective space, obtaining codes of length $q^{2\ell-1} + 1$.

First, we need to define the finite set of projective points in which we are going to evaluate. To do this, we are simply going to add the point at infinity to the set of roots of the trace, i.e., we are going to consider the following set of points:

$$\mathbb{X}_{\mathrm{Tr}_\ell} = \{[1 : \alpha] \mid \mathrm{Tr}_\ell(\alpha) = 0\} \cup \{[0 : 1]\}.$$

It is clear from the definition that $|\mathbb{X}_{\mathrm{Tr}_\ell}| = q^{2\ell-1} + 1$. Moreover, we can give this set as the zeroes of a square-free homogeneous polynomial. In the rest of this section, when we consider the homogenization f^h of a polynomial f, we are considering the standard homogenization (up to degree $\deg(f)$).

Proposition 6.1 *The vanishing ideal of* $\mathbb{X}_{\mathrm{Tr}_\ell}$ *is* $I(\mathbb{X}_{\mathrm{Tr}_\ell}) = \langle x_0(\mathrm{Tr}_\ell(x_1))^h \rangle$.

Proof The generator of the ideal is a homogeneous polynomial. Therefore, we can just look at the set of representatives P^1 to check the zeroes of the ideal. It is clear that $[0 : 1] \in V(\langle x_0(\mathrm{Tr}_\ell(x_1))^h \rangle)$. And it is also clear that if $[1 : \alpha]$ is a zero of $x_0(\mathrm{Tr}_\ell(x_1))^h$, then α must be a root of $\mathrm{Tr}_\ell(x)$. Thus, we have that $V(\langle x_0(\mathrm{Tr}_\ell(x_1))^h \rangle) = \mathbb{X}_{\mathrm{Tr}_\ell}$.

On the other hand, we have the decomposition

$$\mathrm{Tr}_\ell(x) = \prod_{\alpha \in \mathbb{F}_{q^{2\ell}} | \mathrm{Tr}_\ell(\alpha)=0} (x - \alpha).$$

Homogenizing and multiplying by x_0 we get

$$x_0(\mathrm{Tr}_\ell(x_1))^h = x_0 \prod_{\alpha \in \mathbb{F}_{q^{2\ell}} | \mathrm{Tr}_\ell(\alpha)=0} (x_1 - \alpha x_0).$$

Therefore, $x_0(\mathrm{Tr}_\ell(x_1))^h$ is a square-free polynomial and $\langle x_0(\mathrm{Tr}_\ell(x_1))^h \rangle$ is a radical ideal by Cox et al. (2015, Prop. 9, Chapter 4, Section 2), which means that it is equal to $I(\mathbb{X}_{\mathrm{Tr}_\ell})$. □

If we consider the set of standard representatives X_{Tr_ℓ} of $\mathbb{X}_{\mathrm{Tr}_\ell}$, we obtain the following vanishing ideal.

Proposition 6.2 *The vanishing ideal of* X_{Tr_ℓ} *is*

$$I(X_{\mathrm{Tr}_\ell}) = \langle x_0^2 - x_0, x_1^{q^{2\ell}} - x_1, (x_0 - 1)(x_1 - 1), x_0 \,\mathrm{Tr}(x_1) \rangle.$$

Proof It is clear that any point of X_{Tr_ℓ} satisfies the equations. On the other hand, any point that satisfies this equations must have the first coordinate equal to 0 or 1 because of the first equation. If it is 0, then by the equation $(x_0 - 1)(x_1 - 1) \equiv 0 \bmod I(X_{\mathrm{Tr}_\ell})$ we have that the last coordinate is equal to 1. If the first coordinate is 1, then the last equation implies that the last coordinate must be a zero of $\mathrm{Tr}(x)$. Therefore, $V(I(X_{\mathrm{Tr}_\ell})) = X_{\mathrm{Tr}_\ell}$. We obtain the result applying Seidenberg's Lemma (Kreuzer and Robbiano 2000, Prop. 3.7.15) and Hilbert's Nullstellensatz over the algebraic closure of $\mathbb{F}_{q^{2\ell}}$. □

We are going to define the evaluation map that we are going to use to construct these new codes (we have $n = q^{2\ell-1} + 1$):

$$\mathrm{ev}_{\mathrm{Tr}_\ell} : \mathbb{F}_{q^{2\ell}}[x_0, x_1]/I(X_{\mathrm{Tr}_\ell}) \to \mathbb{F}_{q^{2\ell}}^n, \quad f \mapsto (f(P_1), \ldots, f(P_n))_{P_i \in X_{\mathrm{Tr}_\ell}}.$$

Definition 6.3 Let $\mathcal{A} = \{a_0 = 0 < a_1 < \cdots < a_z\}$. We are going to consider a set $\Delta = \bigcup_{i=0}^{t-1} \mathfrak{I}_{a_i} \cup \{a_t\}$ as before. For such a set Δ, we consider the code $\mathcal{D}(\mathrm{Tr}_\ell, \Delta)$ defined as the linear code generated by $\{\mathrm{ev}_{\mathrm{Tr}_\ell}(x_0 x_1^\alpha) \mid \alpha \in \Delta \backslash \{a_t\}\} \cup \{\mathrm{ev}_{\mathrm{Tr}_\ell}(x_1^{a_t})\}$.

In what follows we are going to need to use the codes $\mathrm{RS}(\mathrm{Tr}_\ell, \Delta) := \mathrm{RS}(Y_{\mathrm{Tr}_\ell}, \Delta)$ that appear in Galindo et al. (2019c), which are the puncturing of the codes $\mathcal{D}(\mathrm{Tr}_\ell, \Delta)$ at the coordinate associated to the point $[0 : 1]$. When Δ is a union of consecutive cyclotomic sets, we have that $(\mathrm{RS}(\mathrm{Tr}_\ell, \Delta)_{q^2})^\perp = (\mathrm{RS}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}$. We are going to be interested in the code $(\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}$, for which we have the following result.

Theorem 6.4 *Let $a_0 = 0 < a_1 < a_2 < \cdots < a_{t-1} < a_t < q^{2\ell} - 1$ be a sequence of consecutive elements of $\mathcal{A}$. Let $\Delta = \bigcup_{i=0}^{t-1} \mathfrak{I}_{a_i} \cup \{a_t\}$ and let $\Delta'' = \Delta \cup \mathfrak{I}_{a_t}$. Assuming that $(\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}$ is not degenerate, we have the following inequalities:*

$$\dim\,(\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2} = \dim(\mathrm{RS}(\mathrm{Tr}_\ell, \Delta'')^\perp)_{q^2} + 1 \geq n - \sum_{i=0}^{t} n_{a_i},$$

$$\mathrm{wt}((\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}) \geq a_t + 2.$$

Proof By the definitions, it is clear that $\mathcal{D}(\mathrm{Tr}_\ell, \Delta) = (\mathrm{RS}(\mathrm{Tr}_\ell, \Delta'), 0) + \langle \mathrm{ev}_{\mathrm{Tr}_\ell}(x_1^{a_t}) \rangle$, where $\Delta' = \Delta \setminus \{a_t\}$. This means that $\dim \mathcal{D}(\mathrm{Tr}_\ell, \Delta) = \dim \mathrm{RS}(\mathrm{Tr}_\ell, \Delta') + 1 = \dim \mathrm{RS}(\mathrm{Tr}_\ell, \Delta)$, because if we have $\dim \mathrm{RS}(\mathrm{Tr}_\ell, \Delta') = \dim \mathrm{RS}(\mathrm{Tr}_\ell, \Delta)$, this means that $\mathrm{ev}_{\mathrm{Tr}_\ell}(x_0 x_1^{a_t})$ is in $(\mathrm{RS}(\mathrm{Tr}_\ell, \Delta'), 0)$, which implies that $\mathrm{ev}_{\mathrm{Tr}_\ell}(x_0 x_1^{a_t} - x_1^{a_t})$ is in $\mathcal{D}(\mathrm{Tr}_\ell, \Delta)$, but this is a vector of weight 1, which is a contradiction, because $(\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}$ (and $\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp$) is not degenerate. Therefore, we have that $\dim \mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp = \dim \mathrm{RS}(\mathrm{Tr}_\ell, \Delta)^\perp + 1$.

Arguing as in the proof of Theorem 5.5, we have $\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp = (\mathrm{RS}(\mathrm{Tr}_\ell, \Delta)^\perp, 0) + \langle w \rangle$, where w is a vector with a nonzero last entry, and we also obtain $(\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2} = ((\mathrm{RS}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}, 0) + \langle w' \rangle$ for some vector w' with nonzero last coordinate. Moreover, a basis for $((\mathrm{RS}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}, 0)$ would give us $\dim(\mathrm{RS}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}$ linearly independent vectors with last coordinate equal to 0, which means that $\dim\,(\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2} = \dim(\mathrm{RS}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2} + 1$.

We obtain $\dim\,(\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2} = \dim(\mathrm{RS}(\mathrm{Tr}_\ell, \Delta'')^\perp)_{q^2} + 1$, because $(\mathrm{RS}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2} = (\mathrm{RS}(\mathrm{Tr}_\ell, \Delta'')^\perp)_{q^2}$, which is what we are going to see next. When evaluating in all the points of $\mathbb{F}_{q^{2\ell}}$, we have $(\mathrm{RS}(q^{2\ell}, \Delta)^\perp)_{q^2} = (\mathrm{RS}(q^{2\ell}, \Delta'')^\perp)_{q^2}$. The code $\mathrm{RS}(\mathrm{Tr}_\ell, \Delta)$ (resp. $\mathrm{RS}(\mathrm{Tr}_\ell, \Delta'')$) corresponds to a puncturing of $\mathrm{RS}(q^{2\ell}, \Delta)$ (resp. $\mathrm{RS}(q^{2\ell}, \Delta'')$), because we

only evaluate in the zeroes of $\mathrm{Tr}_\ell(x)$. The dual of a punctured code is equal to the shortening of the dual code at the same positions (Pellikaan et al. 2018, Prop. 2.1.17). Given a code C, if we denote by S the positions where we are puncturing (resp. shortening), by C_S the punctured code and by C^S the shortened code, we obtain

$$((C_S)^\perp)_{q^2} = ((C^\perp)^S)_{q^2} = ((C^\perp)_{q^2})^S,$$

because shortening a code commutes with considering its subfield subcode. Let S be the positions where we puncture to obtain $\mathrm{RS}(\mathrm{Tr}_\ell, \Delta)$ from $\mathrm{RS}(q^{2\ell}, \Delta)$. Using the previous expression and the fact that $(\mathrm{RS}(q^{2\ell}, \Delta)^\perp)_{q^2} = (\mathrm{RS}(q^{2\ell}, \Delta'')^\perp)_{q^2}$ we get

$$\begin{aligned}(\mathrm{RS}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2} &= ((\mathrm{RS}(q^{2\ell}, \Delta)_S)^\perp)_{q^2} = ((\mathrm{RS}(q^{2\ell}, \Delta)^\perp)_{q^2})^S = ((\mathrm{RS}(q^{2\ell}, \Delta'')^\perp)_{q^2})^S \\ &= ((\mathrm{RS}(q^{2\ell}, \Delta'')_S)^\perp)_{q^2} = (\mathrm{RS}(\mathrm{Tr}_\ell, \Delta'')^\perp)_{q^2}.\end{aligned}$$

The bound for the dimension given in the statement is obtained by using Galindo et al. (2019c, Thm. 13).

On the other hand, for the minimum distance, we have the BCH-type bound for $\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp$, which gives $\mathrm{wt}(\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp) \geq a_t + 2$, and it is inherited by $(\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}$. □

The previous result shows that, if $a_{t+1} + 1 = a_t + 2$, then the code $(\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}$ has 1 more length and dimension than the code $(\mathrm{RS}(\mathrm{Tr}_\ell, \Delta'')^\perp)_{q^2}$. In the next example we obtain some codes $(\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}$ with record parameters according to Grassl (2007).

Example 6.5 We consider the field extension $\mathbb{F}_{2^8} \supset \mathbb{F}_{2^2}$, i.e., we have $q = 2$ and $\ell = 4$. Therefore, we will get codes with length $N = 129$. Let $\Delta = \mathfrak{I}_0 \cup \mathfrak{I}_1 \cup \cdots \mathfrak{I}_{a_{t-1}} \cup \{a_t\}$. Hence, we have $\mathrm{wt}\left((\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}\right) \geq a_t + 2$. The dimension of these codes can be easily computed using Magma (Bosma et al. 1997). In this case, we obtain a lot of codes whose parameters achieve the best known values in Grassl (2007), and in many cases we are obtaining codes with higher length and dimension, but same minimum distance as in the affine case. Moreover, we obtain the parameters $[129, 90, 15]_4$, $[129, 86, 16]_4$ and $[129, 41, 44]_4$, for a_t equal to 13, 14 and 42, respectively. In Grassl (2007), a construction of a code with parameters $[129, 86, 16]_4$ is currently missing, and we are able to obtain one. The codes with parameters $[129, 90, 15]_4$ and $[129, 41, 44]_4$ exceed the best known values in Grassl (2007). Furthermore, by shortening and puncturing these codes we are able to obtain more codes with record parameters or missing constructions in Grassl (2007). For instance, from the code with parameters $[129, 41, 44]_4$, we obtain the parameters $[129-i-j, 41-i, 44-j]_4$, for $0 \leq i \leq 4$, $0 \leq j \leq 3$, which are either records or the construction of a code with those parameters is missing in Grassl (2007).

The next result shows that we can construct quantum codes over $\mathbb{F}_q$ using Theorem 6.4 together with the Hermitian construction 5.14.

Theorem 6.6 *Let $\mathcal{A} = \{a_0 = 0 < a_1 < a_2 < \cdots < a_z\}$ be the set of minimal representatives of the cyclotomic sets $\mathfrak{I}_{a_i}$, $0 \leq i \leq z$, of $\{0, 1, \ldots, q^{2\ell} - 1\}$ with respect to q^2. Let $t \leq z$ be an index, such that*

$$a_t \leq q^\ell - \left\lfloor \frac{(q-1)}{2} \right\rfloor q^{\ell-1} - \cdots - \left\lfloor \frac{(q-1)}{2} \right\rfloor q - 1.$$

Then, for $\Delta = \bigcup_{i=0}^{t-1} \mathfrak{I}_{a_i} \cup \{a_t\}$ as before, assuming that $(\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}$ is not degenerate, we have that:

$$\dim\left(((\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2})^{\perp_h} \cap (\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}\right) \geq \dim\left((\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2})^{\perp_h} - 1.\right.$$

As a consequence, we can construct an EAQECC with parameters

$$\left[\left[n, \geq n - 2\sum_{i=0}^{t} n_{a_i} + c, \geq a_t + 2; c\right]\right]_q,$$

where $n = q^{2\ell-1} + 1$ *and* $c \leq 1$.

Proof Similarly to the proof of Theorem 5.15, we are going to consider the code $C = ((\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2})^{\perp_h}$ for the Hermitian construction 5.14. By Theorem 6.4 we obtain the bound for the minimum distance, and we also obtain that $\dim((\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2})^{\perp_h} \leq \sum_{i=0}^{t} n_{a_i}$, which explains the dimension of the quantum code. The only thing left to prove is the claim about the intersection of $(\mathcal{D}(\mathrm{Tr}_\ell, \Delta)^\perp)_{q^2}$ with its hermitian dual.

Under our assumptions, in Galindo et al. (2019c, Thm. 15) it is proved that we have $\mathrm{RS}(\mathrm{Tr}_\ell, \Delta'')_{q^2} \subset (\mathrm{RS}(\mathrm{Tr}_\ell, \Delta'')_{q^2})^{\perp_h}$ for $\Delta'' = \bigcup_{i=0}^{t} \mathfrak{I}_{a_i}$. The reasoning from the proof of Theorem 5.15 finishes the proof. □

Example 6.7 We continue with Example 6.5. For $a_t = 10$, we have $a_t + 2 = 12$, and, computing the dimension with Magma (Bosma et al. 1997), we obtain a quantum code with parameters $[[129, 67, 12; 1]]_2$ using Theorem 6.6. In the affine case from Galindo et al. (2019c), the parameters $[[128, 65, 12; 0]]_2$ are obtained. Therefore, we have increased the length by 1 and the dimension by 2, at the expense of increasing the parameter c by 1. Moreover, the codes $[[129, 73, 11; 1]]_2$, $[[129, 67, 12; 1]]_2$ and $[[129, 59, 13; 1]]_2$ that we can obtain in this way (by changing a_t) cannot be deduced using the propagation rules from Luo et al. (2022) with the codes in the table of QECCs from Grassl (2007).

In Galindo et al. (2019c), the authors consider what they call *complementary codes*, which are obtained in an analogous way, but evaluating in precisely all the points in $\mathbb{F}_{q^{2\ell}}$ besides the zeroes of $\mathrm{Tr}_\ell(x)$. For the projective case, it is easy to see that including the point at infinity in this set corresponds to considering the zero set of

$$\frac{x_0 x_1^{q^{2\ell}} - x_0^{q^{2\ell}} x_1}{\mathrm{Tr}_\ell(x_1)^h}.$$

All the results we have given in this section apply to these types of codes as well, but with length $q^{2\ell} - q^{2\ell-1} + 1$ (instead of $q^{2\ell-1} + 1$).

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

Anderson SE, Camps-Moreno E, López HH, Matthews GL, Ruano D, Soprunov I (2022) Relative hulls and quantum codes. ArXiv:2212.14521

Bierbrauer J (2002) The theory of cyclic codes and a generalization to additive codes. Des Codes Cryptogr 25(2):189–206

Bierbrauer J, Edel Y (1997) New code parameters from Reed–Solomon subfield codes. IEEE Trans Inf Theory 43(3):953–968

Bierbrauer J, Edel Y (2000) Quantum twisted codes. J Comb Des 8(3):174–188

Bosma W, Cannon J, Playoust C (1997) The Magma algebra system. I. The user language. J Symb Comput 24(3–4):235–265

Brun T, Devetak I, Hsieh M-H (2006) Correcting quantum errors with entanglement. Science 314(5798):436–439

Calderbank AR, Shor PW (1996) Good quantum error-correcting codes exist. Phys Rev A 54:1098–1105

Cohen SD (1990) Primitive elements and polynomials with arbitrary trace. Discrete Math 83(1):1–7

Cox DA, Little J, O'Shea D (2015) Ideals, varieties, and algorithms. Undergraduate Texts in Mathematics, 4th edn. Springer, Cham, An introduction to computational algebraic geometry and commutative algebra

Delsarte P (1975) On subfield subcodes of modified Reed-Solomon codes. IEEE Trans Inf Theory IT–21(5):575–576

Duursma IM, Rentería C, Tapia-Recillas H (2001) Reed-Muller codes on complete intersections. Appl Algebra Eng Commun Comput 11(6):455–462

Eisenbud D (1995) Commutative algebra with a view toward algebraic geometry, graduate texts in mathematics, vol 150. Springer, New York

Galindo C, Hernando F (2015) Quantum codes from affine variety codes and their subfield-subcodes. Des Codes Cryptogr 76(1):89–100

Galindo C, Hernando F, Ruano D (2015) Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement. Quantum Inf Process 14(9):3211–3231

Galindo C, Geil O, Hernando F, Ruano D (2019a) New binary and ternary LCD codes. IEEE Trans Inf Theory 65(2):1008–1016

Galindo C, Hernando F, Matsumoto R, Ruano D (2019b) Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. Quantum Inf Process 18(4):116, 18

Galindo C, Hernando F, Ruano D (2019c) Classical and quantum evaluation codes at the trace roots. IEEE Trans Inf Theory 65(4):2593–2602

Galindo C, Hernando F, Matsumoto R, Ruano D (2020) Asymmetric entanglement-assisted quantum error-correcting codes and BCH codes. IEEE Access 8:18571–18579

Galindo C, Hernando F, Ruano D (2021) Entanglement-assisted quantum error-correcting codes from RS codes and BCH codes with extension degree 2. Quantum Inf Process 20(5):158, 26

González-Sarabia M, Rentería C (2004) The dual code of some Reed–Muller type codes. Appl Algebra Eng Commun Comput 14(5):329–333

Grassl M (2007) Bounds on the minimum distance of linear codes and quantum codes. http://www.codetables.de. Accessed on 4 Apr 2023

Hattori M, McEliece RJ, Solomon G (1998) Subspace subcodes of Reed–Solomon codes. IEEE Trans Inf Theory 44(5):1861–1880

Hernando F, O'Sullivan ME, Popovici E, Srivastava S (2010) Subfield-subcodes of generalized toric codes. In: 2010 IEEE international symposium on information theory, pp 1125–1129

Hernando F, Marshall K, O'Sullivan ME (2013) The dimension of subcode-subfields of shortened generalized Reed–Solomon codes. Des Codes Cryptogr 69(1):131–142

Ioffe L, Mézard M (2007) Asymmetric quantum error-correcting codes. Phys Rev A 75:032345

Kreuzer M, Robbiano L (2000) Computational commutative algebra. 1. Springer, Berlin

La Guardia GG (2020) Quantum error correction–symmetric, asymmetric, synchronizable, and convolutional codes. Quantum science and technology. Springer, Cham

López HH, Soprunov I, Villarreal RH (2021) The dual of an evaluation code. Des Codes Cryptogr 89(7):1367–1403

Luo G, Ezerman MF, Grassl M, Ling S (2022) How much entanglement does a quantum code need? ArXiv:2207.05647

Martínez-Bernal J, Pitones Y, Villarreal RH (2017) Minimum distance functions of graded ideals and Reed–Muller-type codes. J Pure Appl Algebra 221(2):251–275

Nakashima N, Matsui H (2016) Decoding of projective reed-muller codes by dividing a projective space into affine spaces. IEICE Trans Fund Electron Commun Comput Sci E99.A(3):733–741

Pellikaan R, Wu X-W, Bulygin S, Jurrius R (2018) Codes, cryptology and curves with computer algebra. Cambridge University Press, Cambridge

Sarvepalli PK, Klappenecker A, Rötteler M (2009) Asymmetric quantum codes: constructions, bounds and performance. Proc R Soc Lond Ser A Math Phys Eng Sci 465(2105):1645–1672