Universidad de Valladolid

PROGRAMA DE DOCTORADO EN MATEMÁTICAS

TESIS DOCTORAL:

Commutative Algebra and Coding Theory, with Applications to Quantum Error-Correction

Presentada por Rodrigo San José Rubio para optar al grado de
Doctor/a por la Universidad de Valladolid

Dirigida por:
Philippe Gimenez
Diego Ruano

Abstract

Modern digital communication systems often face the challenge of data corruption due to noise, leading to discrepancies between transmitted and received symbols. Error-correcting codes guarantee reliable and fast transmission of information in such systems by adding redundant symbols. Algebraic Coding Theory plays an important role not only in many different aspects of communication but also in cryptography and quantum computing. This is because the additional algebraic structure of algebraic codes allows us to derive further properties of them. Since these properties characterize the performance of the code for certain applications, we can consider or design codes that are suitable for each setting. In particular, in this thesis we are interested in using tools from Commutative Algebra to derive properties of linear codes. We focus mainly on evaluation codes, since they have a natural connection to Commutative Algebra, but we also consider other types of codes such as cyclic codes (which can be viewed as subfield subcodes of evaluation codes) or matrix-product codes.

Many aspects of evaluation codes can be understood by means of the vanishing ideal of the set of points considered. A natural question that arises is how to compute this vanishing ideal. When one considers the evaluation points over the affine space, this computation is straightforward. However, in the projective setting one usually has to compute the radical of an ideal. In Paper A, we give an alternative and more efficient way of computing the vanishing ideal by using the saturation with respect to the homogeneous maximal ideal. Another option to study evaluation codes over the projective space is to consider a set of fixed representatives of the points, regarded as a subset of the affine space, and its vanishing ideal. In Papers B and C, we give a universal Gröbner basis for this vanishing ideal when the set of points corresponds to certain subsets of the projective line, or to the whole projective space.

Obtaining long codes with good parameters over a small finite field, which is desirable for applications, is a complicated problem in general. One approach to achieve this is to take codes with good parameters over a large field (e.g., Reed-Solomon codes), and then consider their subfield subcodes. The resulting code usually has lower dimension than the original code, and obtaining bases for the subfield subcodes (which give the dimension) is one of the main problems to study when working with subfield subcodes. By using the aforementioned Gröbner bases, in Papers B and C we obtain bases for the subfield subcodes of projective Reed-Solomon codes and projective Reed-Muller codes in many cases. An alternative approach for this problem is also given in Paper D, using a recursive construction for projective Reed-Muller codes.

The interest of the generalized Hamming weights of a linear code originates from the fact that they determine its performance on the wire-tap channel of type II. Since they

were introduced by Wei, many more applications have been found for them, such as list decoding or secret sharing schemes (considering relative generalized Hamming weights). In Paper D, we provide lower and upper bounds for the generalized Hamming weights of projective Reed-Muller codes, determining the true values in many cases. Inspired by the approach from Paper D, in Paper H we also provide bounds for the generalized Hamming weights of matrix-product codes. As a sample of our results, we obtain the exact value of the generalized Hamming weights of matrix-product codes obtained with two Reed-Solomon codes.

The development of reliable quantum computing and communication requires error-correction to deal with noise and decoherence. To perform error-correction, we can consider stabilizer quantum codes. The CSS construction provides a way to construct such codes using self-orthogonal classical linear codes. Furthermore, we consider two additional aspects specific to quantum codes: we can assume entanglement between the encoder and the decoder, giving rise to entanglement-assisted quantum error-correcting codes; and we can also consider two different types of errors, qudit-flip and phase-shift errors, leading to asymmetric quantum codes. The CSS construction can be generalized to cover these cases by considering a pair of classical linear codes, and their minimum distances. The dimension of their relative hull gives the parameter c, which is the minimum number required of maximally entangled pairs. Therefore, in this more general setting we do not require any self-orthogonality condition, but we have an additional parameter to compute. In Paper B, we have used the subfield subcodes of projective Reed-Solomon codes to construct both symmetric and asymmetric entanglement-assisted quantum error-correcting codes.

Since we have seen that the dimension of the hull determines the parameter c of the corresponding quantum code, the study of the hulls of projective Reed-Muller codes over the projective plane carried out in Paper E determines all the parameters of the corresponding quantum codes. Entanglement assistance can improve the rate of the corresponding quantum code, but maintaining entanglement over time can be costly. Therefore, this trade-off must be analyzed for each application, and this also motivates obtaining codes with different requirements of entanglement assistance. In Paper F, we study how to change the dimension of the hull of projective Reed-Muller codes by considering monomially equivalent codes, giving rise to families of codes with a flexible amount of entanglement.

One of the main problems for quantum computing is the fault-tolerant implementation of non-Clifford gates. In Paper G, we study CSS-T codes, which are quantum codes derived from the CSS construction that support the transversal T gate. We give a new characterization of CSS-T codes, and we use it to determine which CSS-T codes can be constructed from cyclic codes. Moreover, we also obtain a propagation rule for nondegenerate CSS-T codes, and we use it to obtain CSS-T codes with better parameters than those available in the literature.

Resumen

Los sistemas modernos de comunicación digital a menudo sufren de corrupción de datos debido al ruido, dando lugar a discrepancias entre los símbolos enviados y recibidos. Los códigos correctores de errores garantizan una transmisión fiable y rápida de la información en tales sistemas al agregar símbolos redundantes. La Teoría Algebraica de Códigos juega un papel importante en muchos aspectos diferentes de la comunicación, así como en la criptografía y la computación cuántica. Esto se debe a que la estructura algebraica adicional de los códigos algebraicos nos permite derivar propiedades adicionales de los mismos. Dado que estas propiedades caracterizan el rendimiento del código para ciertas aplicaciones, podemos considerar o diseñar códigos que sean adecuados para cada contexto. En particular, en esta tesis estamos interesados en usar herramientas de Álgebra Conmutativa para derivar propiedades de códigos lineales. Nos centramos principalmente en códigos de evaluación, ya que tienen una conexión natural con el Álgebra Conmutativa, pero también consideramos otros tipos de códigos como los códigos cíclicos (que pueden verse como subcódigos subcuerpo de los códigos de evaluación) o los códigos producto de matrices.

Muchos aspectos de los códigos de evaluación pueden entenderse mediante el ideal de anulación del conjunto de puntos considerado. Una pregunta natural que surge es cómo calcular este ideal de anulación. Cuando se consideran los puntos de evaluación sobre el espacio afín, este cálculo es sencillo. Sin embargo, en el caso proyectivo, generalmente se tiene que calcular el radical de un ideal. En el Artículo A, damos una forma alternativa y más eficiente de calcular el ideal de anulación utilizando la saturación con respecto al ideal homogéneo maximal. Otra opción para estudiar los códigos de evaluación sobre el espacio proyectivo es considerar un conjunto de representantes fijados de los puntos, considerados como un subconjunto del espacio afín, y su ideal de anulación. En los Artículos B y C, obtenemos una base de Gröbner universal para este ideal de anulación cuando el conjunto de puntos corresponde a ciertos subconjuntos de la recta proyectiva o a todo el espacio proyectivo.

Obtener códigos largos con buenos parámetros sobre un cuerpo finito pequeño, lo cual es deseable para aplicaciones, es un problema complicado en general. Una manera de lograr esto es considerar códigos con buenos parámetros sobre un cuerpo grande (por ejemplo, códigos Reed-Solomon), y luego considerar sus subcódigos subcuerpo. El código resultante generalmente tiene menor dimensión que el código original, y obtener bases para los subcódigos subcuerpo (lo cual también determina la dimensión) es uno de los principales problemas a estudiar cuando se trabaja con subcódigos subcuerpo. Utilizando las bases de Gröbner mencionadas anteriormente, en los Artículos B y C obtenemos bases para los subcódigos subcuerpo de los códigos Reed-Solomon proyectivos y los códigos Reed-Muller proyectivos en muchos casos. Un enfoque alternativo para este problema también

se presenta en el Artículo D, utilizando una construcción recursiva para los códigos Reed-Muller proyectivos.

El interés por los pesos de Hamming generalizados de un código lineal surge del hecho de que determinan su rendimiento en el canal *wire-tap* de tipo II. Desde que fueron introducidos por Wei, se han encontrado muchas más aplicaciones para ellos, como la decodificación en lista o los esquemas de compartición de secretos. En el Artículo D, proporcionamos cotas inferiores y superiores para los pesos de Hamming generalizados de los códigos Reed-Muller proyectivos, determinando los valores verdaderos en muchos casos. Generalizando las ideas del Artículo D, en el Artículo H también proporcionamos cotas para los pesos de Hamming generalizados de los códigos producto de matrices. Como muestra de nuestros resultados, obtenemos el valor exacto de los pesos de Hamming generalizados de los códigos producto de matrices obtenidos a partir dos códigos Reed-Solomon.

El desarrollo de la computación cuántica y la comunicación cuántica fiable requiere corrección de errores para lidiar con el ruido y la decoherencia. Para realizar la corrección de errores, podemos considerar códigos cuánticos estabilizadores. La construcción CSS proporciona una forma de construir dichos códigos utilizando códigos lineales clásicos auto-ortogonales. Además, consideramos dos aspectos adicionales específicos de los códigos cuánticos: podemos asumir entrelazamiento previo entre el codificador y el decodificador, dando lugar a códigos cuánticos de corrección de errores asistidos por entrelazamiento; y también podemos considerar dos tipos diferentes de errores, errores de *qudit-flip* y errores de *phase-shift*, lo que da lugar a los códigos cuánticos asimétricos. La construcción CSS se puede generalizar para cubrir estos casos considerando un par de códigos lineales clásicos y sus distancias mínimas. La dimensión de su *hull* relativo da el parámetro c, que es el número mínimo requerido de pares entrelazados maximalmente. Por lo tanto, en esta situación más general no requerimos ninguna condición de auto-ortogonalidad, pero tenemos un parámetro adicional que calcular. En el Artículo B, hemos utilizado los subcódigos subcuerpo de los códigos Reed-Solomon proyectivos para construir códigos cuánticos de corrección de errores asistidos por entrelazamiento tanto simétricos como asimétricos.

Dado que hemos visto que la dimensión del *hull* determina el parámetro c del código cuántico correspondiente, el estudio de los *hulls* de los códigos Reed-Muller proyectivos sobre el plano proyectivo realizado en el Artículo E determina todos los parámetros de los códigos cuánticos correspondientes. El entrelazamiento puede mejorar la tasa de transmisión del código cuántico correspondiente, pero mantenerlo a lo largo del tiempo puede ser costoso. Por lo tanto, este compromiso debe ser analizado para cada aplicación, y esto también motiva la obtención de códigos con diferentes requisitos de asistencia por entrelazamiento. En el Artículo F, estudiamos cómo cambiar la dimensión del *hull* de los códigos Reed-Muller proyectivos considerando códigos monomialmente equivalentes, dando lugar a familias de códigos cuánticos con requisitos flexibles de entrelazamiento.

Uno de los principales problemas para la computación cuántica es la implementación tolerante a fallos de puertas *non-Clifford*. En el Artículo G, estudiamos los códigos CSS-T, que son códigos cuánticos derivados de la construcción CSS que soportan la puerta transversal T. Damos una nueva caracterización de los códigos CSS-T, y la usamos para determinar qué códigos CSS-T pueden construirse a partir de códigos cíclicos. Además, obtenemos una regla de propagación para los códigos CSS-T no degenerados, y la usamos para obtener códigos CSS-T con mejores parámetros que los disponibles en la literatura.

Agradecimientos

En primer lugar, me gustaría expresar mi más profundo agradecimiento a mis directores de tesis, Philippe y Diego, cuya dedicación y compromiso han sido fundamentales para la culminación exitosa de esta tesis. Ellos me introdujeron a este tema de investigación, que encaja perfectamente dentro de mis intereses y conocimientos de álgebra y códigos (incluso de física). Su orientación no se ha limitado únicamente a proporcionarme los conocimientos necesarios, si no que ha cubierto otros aspectos esenciales, como la parte personal o incluso la gestión administrativa. También agradezco las oportunidades que me han brindado para realizar las distintas actividades que he llevado a cabo durante el doctorado.

I would also like to thank the members of the Applied Algebra Research Group at Virginia Tech for their hospitality during my stay(s). In particular, I would like to thank Gretchen, Hiram and Eduardo for our fruitful and pleasant discussions.

I am also grateful to Jade for inviting me to the Institute of Mathematics of Rennes and for revealing discussions.

Me gustaría dar las gracias a mi familia por su apoyo incondicional, y a mis amigos y compañeros de Valladolid. En particular, estoy agradecido a Jesús, cuyas conversaciones han sido una fuente inagotable de inspiración y reflexión durante el desarrollo de nuestras tesis.

Finalmente, también me gustaría agradecer el apoyo del Ministerio de Universidades por las becas FPU20/01311 y EST23/00777, que han financiado mis estudios de doctorado y mi estancia de investigación en Virginia Tech, y también quería agradecer el apoyo para financiar la asistencia a congresos, escuelas y talleres que me han dado los siguientes proyectos (a los cuales he tenido acceso gracias a mis directores): PID2019-104844GB-I00, PGC2018-096446-B-C21, TED2021-130358B-I00, PID2022-138906NB-C21, PID2022-137283NB-C22 y QCAYLE.

Rodrigo San José Rubio
Universidad de Valladolid, Julio de 2024

Contents

Part I

Introduction

Introduction

Linear codes, which were originally considered for reliable communication protocols, have found many different applications during the last few decades: secret sharing, post-quantum cryptography, quantum error-correction and quantum fault-tolerant computation, secure multiparty computation, etc. For each particular application, one needs to consider different aspects beyond the basic parameters of the codes involved. Two examples of these aspects of linear codes which are relevant to this thesis are the *generalized Hamming weights* and the *hulls* (for both the Euclidean and Hermitian inner products). One can impose additional structure on the codes considered to gain insight into these additional properties. A flexible framework for this purpose is provided by evaluation codes, which are obtained by evaluating functions at certain sets of points. Depending on the choice of functions and points, it is possible to use techniques from Algebraic Geometry and Commutative Algebra to study the properties of the codes involved.

In this thesis, we further explore the connections between *Commutative Algebra* and *Coding Theory*, with a particular focus on applications to quantum codes. This introduction provides an overview of the main results obtained during the development of the thesis, and it is organized according to several transversal topics which link the publications associated to this thesis together.

In Section 1, we introduce the main tools from Commutative Algebra that we use for the rest of the sections, which can be found in Papers A and C. In Section 2, we use the aforementioned tools to obtain bases for the subfield subcodes of projective Reed-Solomon codes and projective Reed-Muller codes. In Section 3, we obtain bounds for the generalized Hamming weights of projective Reed-Muller codes (Subsection 3.1) and matrix-product codes (Subsection 3.2). Finally, in Section 4, we derive quantum error-correcting codes appropriate for both quantum communication (Subsection 4.1) and fault-tolerant quantum computing (Subsection 4.2), using the results from Sections 1 and 2 (mainly for the case of quantum communication).

Since in Section 2 we consider several fields, mainly $\mathbb{F}_{q^s}$ and $\mathbb{F}_q$, we note now that all the codes are considered to be over $\mathbb{F}_q$, except in Section 2, where the original codes are considered over $\mathbb{F}_{q^s}$ and their subfield subcodes over $\mathbb{F}_q$. All the references from this chapter correspond to the global bibliography at the end of this thesis, which collects all the references mentioned in this introduction and in the publications.

1 Vanishing ideals and Coding Theory

We start this section by introducing evaluation codes, which are one of the main objects of study of this work. Let $\mathbb{F}_q$ be a finite field, let $R = \mathbb{F}_q[x_1, \ldots, x_m]$, and let $I \subset R$ be

an ideal. We denote by $\mathcal{X} = V_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\} \subset \mathbb{A}^m$ the finite set of rational points in which all the polynomials of I vanish. We denote its vanishing ideal by $I(\mathcal{X})$, and we define the evaluation map

$$\mathrm{ev}_{\mathcal{X}} : R/I(\mathcal{X}) \to \mathbb{F}_q^n, \;\; f + I(X) \mapsto (f(P_1), \ldots, f(P_n)) \,.$$

This evaluation map provides an isomorphism of $\mathbb{F}_q$-vector spaces $R/I(\mathcal{X}) \cong \mathbb{F}_q^n$. We can consider L a vector subspace of $R/I(\mathcal{X})$ and define the *affine variety code* $C(I, L)$ as the image of L under the evaluation map $\mathrm{ev}_{\mathcal{X}}$. That is:

$$C(I, L) := \mathrm{ev}_{\mathcal{X}}(L) = \{\mathrm{ev}_{\mathcal{X}}(f + I(\mathcal{X})) \mid f + I(\mathcal{X}) \in L\}.$$

One of the key aspects of evaluation codes is that, since $\mathrm{ev}_{\mathcal{X}}$ is an isomorphism, we can identify the codewords of $C(I, L)$ with (classes of) polynomials. Thus, we can use polynomial-related techniques to gain information about the code $C(I, L)$.

Following a similar idea, one can consider evaluation codes over the projective space $\mathbb{P}^m$. Let $I \subset S = \mathbb{F}_q[x_0, \ldots, x_m]$ be a homogeneous ideal, and let $\mathbb{X} = V_{\mathbb{P}^m}(I) = \{[P_1], \ldots, [P_n]\} \subset \mathbb{P}^m$ be the finite set of projective points defined by I with representatives P_i. As before, if we denote the vanishing ideal of $\mathbb{X}$ by $I(\mathbb{X})$, we can define the following $\mathbb{F}_q$-linear map for each degree d:

$$\mathrm{ev}_d : S_d \to \mathbb{F}_q^n, \;\; f \mapsto \left(\frac{f(P_1)}{f_1(P_1)}, \ldots, \frac{f(P_n)}{f_n(P_n)} \right),$$

where $f_i \in S_d$ are fixed homogeneous polynomials verifying $f_i(P_i) \neq 0$. The image of S_d under ev_d, denoted by $C_{\mathbb{X}}(d)$, is called a *projective Reed-Muller type code* of degree d on $\mathbb{X}$. By definition, $I(\mathbb{X})_d = \ker \mathrm{ev}_d$. Thus, $S_d/I(\mathbb{X})_d \cong C_{\mathbb{X}}(d)$. It can easily be checked that the basic parameters of the code (length, dimension and minimum distance) do not depend on the choice of the polynomials f_i. These codes have been studied in various contexts [27,28, 125] and they provide a nice connection between Coding Theory and Commutative Algebra [33, 60, 96, 131]. For example, the length of these codes is given by $n = \deg(S/I(\mathbb{X}))$, and the dimension is given by $k = H_{\mathbb{X}}(d) = \dim(S_d/I(\mathbb{X})_d)$. Furthermore, the minimum distance of $C_{\mathbb{X}}(d)$, and, more generally, its generalized Hamming weights (which we will introduce in later section), can also be expressed in terms of invariants of the ideal [33,96].

Therefore, the vanishing ideal $I(\mathbb{X})$ plays a crucial role in studying this family of codes. In many cases, the set of points $\mathbb{X}$ is usually given as the projective variety defined by a homogeneous ideal, and one may wonder how to compute $I(\mathbb{X})$ from this ideal. If we consider first an affine variety $\mathcal{X}$ defined by an ideal $I \subset R$ instead, the answer is straightforward. The ideal $I_q = I_q + I(\mathbb{A}^m) = I + \langle x_1^q - x_1, \ldots, x_m^q - x_m \rangle$ satisfies

$$V_{\overline{\mathbb{F}_q}}(I_q) = V_{\mathbb{F}_q}(I_q) = V_{\mathbb{F}_q}(I) = V_{\mathbb{F}_q}(I(X)) = \mathcal{X}.$$

By Seidenberg's Lemma [85, Prop. 3.7.15], I_q is radical. Hence, in this case $I_q = I(\mathcal{X})$ by Hilbert's Nullstellensatz (also see [55]).

We can replicate this idea in the projective case and consider, for a homogeneous ideal $I \subset S$, the ideal $I_q = I + I(\mathbb{P}^m)$, where

$$I(\mathbb{P}^m) = \langle \{x_i^q x_j - x_i x_j^q, 0 \leq i < j \leq m\} \rangle$$

was obtained in [99]. However, I_q is not radical in general. In fact, we have observed that this ideal is radical only in very specific cases. Since the computation of the radical of an ideal may be computationally intensive, this raises the question of finding easier ways to compute $I(\mathbb{X})$. In Paper A, we obtain the following result.

Theorem 1.1 [Thm. A.2.10]**.** *Let I be an homogeneous ideal such that $(I(\mathbb{P}^m) : I) \neq I(\mathbb{P}^m)$. Let $\mathbb{X} = V_{\mathbb{P}^m}(I)$ and $\mathfrak{m} = (x_0, \ldots, x_m)$ the homogeneous maximal ideal. Then*

$$I(\mathbb{X}) = (I + I(\mathbb{P}^m)) : \mathfrak{m}^\infty.$$

The condition $(I(\mathbb{P}^m) : I) \neq I(\mathbb{P}^m)$ is equivalent to having $\mathbb{X} \neq \emptyset$, which is the case we are interested in for Coding Theory. Thus, this result provides a more efficient way of computing $I(\mathbb{X})$ by using the saturation with respect to the homogeneous maximal ideal instead of computing the radical, since the saturation is regarded as a less computationally intensive operation than obtaining the radical.

Another approach to study Reed-Muller type codes is to fix the representatives of the points of $\mathbb{P}^m$. Indeed, we can fix the *standard representatives*, that is, for each point in $\mathbb{P}^m$, we consider the representative with the leftmost nonzero coordinate equal to 1. In this way, we obtain a set of representatives, denoted P^m, which can be regarded as a subset of $\mathbb{A}^{m+1}$. Analogously, from $\mathbb{X} \subset \mathbb{P}^m$ we obtain its set of standard representatives $X \subset P^m \subset \mathbb{A}^{m+1}$. We can extend the definition of ev_X to S, and then we can consider the code $\mathrm{ev}_X(S_d)$, which is monomially equivalent to $C_{\mathbb{X}}(d)$. This gives the isomorphism

$$\mathrm{ev}_X(S_d) \cong S_d/(I(X) \cap S_d) \cong (S_d + I(X))/I(X),$$

and we can also study the properties of the code $\mathrm{ev}_X(S_d)$ (or $C_{\mathbb{X}}(d)$) by studying the ideal $I(X)$. To compute $I(X)$, first we consider $I(P^m)$, for which we have the following result from Paper C.

Theorem 1.2 [Thm. C.4.1]**.** *The vanishing ideal of P^m is generated by:*

$$\begin{aligned} I(P^m) =& \langle x_0^2 - x_0, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m, (x_0 - 1)(x_1^2 - x_1), \\ & (x_0 - 1)(x_1 - 1)(x_2^2 - x_2), \ldots, (x_0 - 1) \cdots (x_{m-1}^2 - x_{m-1}), (x_0 - 1) \cdots (x_m - 1) \rangle. \end{aligned}$$

Moreover, these generators form a universal Gröbner basis of the ideal $I(P^m)$, and we have that

$$\mathrm{in}(I(P^m)) = \langle x_0^2, x_1^q, x_2^q, \ldots, x_m^q, x_0 x_1^2, x_0 x_1 x_2^2, \ldots, x_0 x_1 \cdots x_{m-1}^2, x_0 x_1 \cdots x_m \rangle.$$

With this result, we can argue as before and, if we consider a homogeneous ideal I such that $V_{\mathbb{F}_q}(I) = \mathbb{X}$, then $I_q = I + I(P^{m-1})$ is radical by Seidenberg's Lemma [85, Prop. 3.7.15], and $I_q = I(X)$ (again, also see [55]).

The most well known family of projective Reed-Muller type codes are obtained when one considers $X = P^m$. In that case, the code $\mathrm{ev}_X(S_d)$ is called a *projective Reed-Muller code* of degree d, and is denoted by $\mathrm{PRM}_d(q, m)$, or by $\mathrm{PRM}_d(m)$ if there is no confusion about the field. This family of codes was introduced in [88], and their basic parameters were studied in [125]. In particular, from [125] we have the following results (for the minimum distance, also see [56, 126]).

Theorem 1.3. *The projective Reed-Muller code* $\mathrm{PRM}_d(q,m)$, $1 \leq d \leq m(q-1)$, *is an* $[n,k]$*-code with*

$$n = \frac{q^{m+1}-1}{q-1},$$
$$k = \sum_{t \equiv d \bmod q-1, 0<t\leq d} \left(\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{t-jq+m}{t-jq} \right).$$

For the minimum distance, we have

$$\mathrm{wt}(\mathrm{PRM}_d(q,m)) = (q-\ell)q^{m-r-1}, \text{ where } d-1 = r(q-1)+\ell,\ 0 \leq \ell < q-1.$$

Theorem 1.4. *Let* $1 \leq d \leq m(q-1)$ *and let* $d^\perp = m(q-1)-d$. *Then*

$$\mathrm{PRM}_d^\perp(q,m) = \mathrm{PRM}_{d^\perp}(q,m) \qquad \text{if } d \not\equiv 0 \bmod q-1,$$
$$\mathrm{PRM}_d^\perp(q,m) = \mathrm{PRM}_{d^\perp}(q,m) + \langle (1,\ldots,1) \rangle \qquad \text{if } d \equiv 0 \bmod q-1.$$

In [89], it is shown that the parameters of projective Reed-Muller codes can outperform those of affine Reed-Muller codes. However, projective Reed-Muller codes have received much less attention than their affine counterpart, and a substantial part of this thesis is devoted to filling this gap.

To study $\mathrm{PRM}_d(m)$, we study first how to work over the quotient ring $S/I(P^m)$, which contains $(S_d + I(P^m))/I(P^m) \cong \mathrm{PRM}_d(m)$. From Macaulay's classical result [42, Thm. 15.3], the monomials not contained in $\mathrm{in}(P^m)$ (sometimes called the *footprint*) form a basis for $S/I(P^m)$. Therefore, using Theorem 1.5, in Paper C we obtain the following basis.

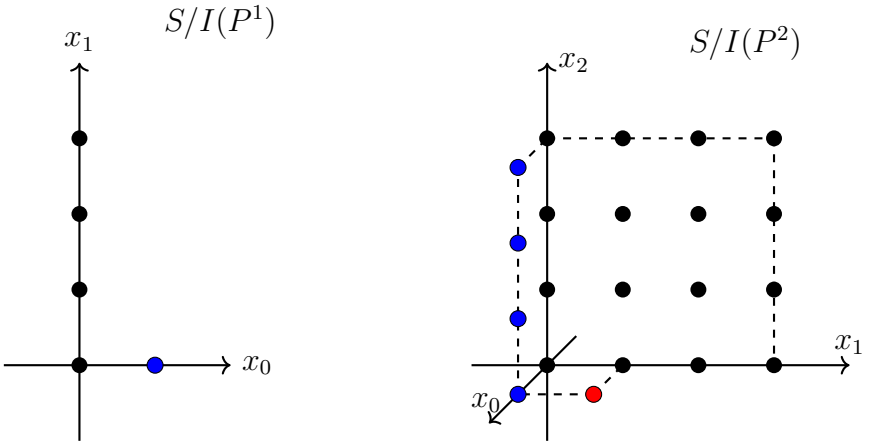
Lemma 1.5 [Lem. C.4.3]**.** *The set given by the classes of the following monomials*

$$\{x_1^{a_1} \cdots x_m^{a_m}, x_0 x_2^{a_2} \cdots x_m^{a_m}, \ldots, x_0 x_1 \cdots x_{m-2} x_m^{a_m}, x_0 \cdots x_{m-1} \mid 0 \leq a_i \leq q-1, 1 \leq i \leq m\}$$

is a basis for $S/I(P^m)$.

One can check that there are exactly $q^m + q^{m-1} + \cdots + q + 1 = (q^{m+1}-1)/(q-1) = |P^m|$ monomials in the basis.

Example 1.6. We have $\mathrm{in}(I(P^1)) = \langle x_1^2, x_2^q, x_1 x_2 \rangle$ and $\mathrm{in}(I(P^2)) = \langle x_1^2, x_2^q, x_3^q, x_1 x_2^2, x_1 x_2 x_3 \rangle$. For $q = 4$, we have the following footprints:



We have used different colors to show the correspondence between the number of monomials in the footprint and $|P^m|$. For $m = 2$ and $q = 4$, we obtain $4^2 = 16$ monomials in black, which is the number of points of $\mathbb{A}^2$, and $4 + 1 = 5$ monomials in blue or red, corresponding to the line at infinity, which can be regarded as an affine line (monomials in blue) and a point at infinity (monomial in red).

Additionally, in Theorem C.4.4, we prove how to reduce any monomial with respect to the Gröbner basis from Theorem 1.2, thus obtaining its expression in terms of the basis from Lemma 1.5. These are the main tools we use to study projective Reed-Muller codes and to obtain applications in the following sections.

2 Subfield subcodes

Given a code $C \subset \mathbb{F}_{q^s}^n$, its subfield subcode is the linear code $C \cap \mathbb{F}_q^n$, which we denote C_q (it can be denoted by C^σ as well). Considering subfield subcodes is a standard technique for constructing long linear codes over a small finite field. For instance, BCH codes can be seen as subfield subcodes of Reed-Solomon codes [13]. In the multivariate case, the subfield subcodes of J-affine variety codes are well known [47] (in particular, the subfield subcodes of Reed-Muller codes) and have been used for several applications [46, 52]. The main problem that arises when working with subfield subcodes is the computation of a basis for the code, which also gives the dimension. In this section, we study the subfield subcodes of projective Reed-Solomon codes, which can be regarded as doubly extended BCH codes, and projective Reed-Muller codes. Throughout this section, the polynomial rings are understood to have coefficients in $\mathbb{F}_{q^s}$, and the codes are understood to be over $\mathbb{F}_{q^s}$ except when considering subfield subcodes, which are assumed to be over $\mathbb{F}_q$.

We introduce first projective Reed-Solomon codes. We consider $X \subset P^1$ (over $\mathbb{F}_{q^s}$), and the polynomial ring $S = \mathbb{F}_{q^s}[x_0, x_1]$. Given $\Delta \subset \{0, 1, \dots, n-1\}$, 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 $\mathrm{PRS}(X, \Delta)$. 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 $\Delta_d := \{0, 1, \dots, d\}$. The code $\mathrm{PRS}(P^1, \Delta_d)$ is also called *doubly extended Reed-Solomon code* and its parameters are $[q^s + 1, d + 1, q^s - d + 1]$. This code can be regarded as a projective Reed-Muller code in 1 variable.

For the evaluation points X, we are going to consider a subgroup of the multiplicative group $\mathbb{F}_{q^s}^*$, plus zero and the point at infinity. Indeed, given N such that $N - 1 \mid q^s - 1$, we define Y_N to be the zero locus of $\langle x^N - x \rangle$, that is, a multiplicative subgroup of $\mathbb{F}_{q^s}^*$ plus zero, and $X_N = (\{1\} \times Y_n) \cup \{(0, 1)\} \subset P^1$. For convenience, we will denote $\mathrm{PRS}(N, \Delta) := \mathrm{PRS}(X_N, \Delta)$. With this notation, doubly extended Reed-Solomon codes are denoted by $\mathrm{PRS}(q^s, \Delta_d)$. In general, for the codes $\mathrm{PRS}(N, \Delta)$ we have the parameters $[N + 1, |\Delta|, \geq N - d(\Delta) + 1]$.

We will say that a polynomial evaluates to $\mathbb{F}_q$ in X if $\mathrm{ev}_X(f) \in \mathbb{F}_q^n$. The following result, which partially appears in Papers B and C, is crucial for relating the subfield subcodes of codes over the affine space and the projective space.

Lemma 2.1 [Lem. B.3.1 and Lem. C.2.6]. *Let $X_N \subset P^1$. Then $f \in \mathbb{F}_{q^s}[x_0, x_1]$ 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 $\mathbb{F}_q$. For the case $m \geq 2$, one has that $f \in \mathbb{F}_{q^s}[x_0, \ldots, x_m]$ evaluates to $\mathbb{F}_q$ in P^m if and only if $f(1, x_1, \ldots, x_m)$, $f(0, 1, x_2, \ldots, x_m)$, $f(0, 0, 1, x_3, \ldots, x_m)$,..., and $f(0, 0, \ldots, 0, 1, x_m)$ evaluate to $\mathbb{F}_q$ in $\mathbb{A}^m, \mathbb{A}^{m-1}, \mathbb{A}^{m-2}, \ldots, \mathbb{A}$, respectively, and $f(0, \ldots, 0, 1) \in \mathbb{F}_q$.*

Since bases for subfield subcodes of Reed-Solomon codes and the subfield subcodes of affine Reed-Muller codes are known [47], by homogenizing those polynomials we get candidates for polynomials that evaluate to $\mathbb{F}_q$ in the projective space, because the homogenization will automatically satisfy that, when setting $x_0 = 1$, the resulting polynomial evaluates to $\mathbb{F}_q$ (the first condition in Lemma 2.1 for both P^1 and P^m). For simplicity, we show next how to use this Lemma to obtain bases for the subfield subcodes of projective Reed-Solomon codes only. The details for the case of projective Reed-Muller codes are in Paper C. First, we need to introduce the notation of cyclotomic sets and trace functions.

For N such that $N - 1 \mid q^s - 1$, 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.

Given a degree d and a polynomial $f(x_1) \in \mathbb{F}_{q^s}[x_1]$ with $\deg(f) \leq d$, its homogenization up to degree d is the homogeneous polynomial $f^h(x_0, x_1) := x_0^d f(x_1/x_0) \in \mathbb{F}_{q^s}[x_0, x_1]_d$. For each $a \in \mathcal{A}$, we define the following trace map:

$$\mathcal{T}_a : \mathbb{F}_{q^s}[x_1]/I(Y_N) \to \mathbb{F}_{q^s}[x_1]/I(Y_N), \;\; f \mapsto f + f^q + \cdots + f^{q^{(n_a-1)}},$$

and given $\Delta \subset \{0, 1, \ldots, N - 1\}$, we denote $\Delta_{\mathfrak{I}} := \bigcup_{\mathfrak{I}_a \subset \Delta} \mathfrak{I}_a \subset \Delta$.

Consider $f \in \mathbb{F}_q[x_1]$. We choose for $\mathcal{T}_a(f)$ 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 or equal to d, then we define $\mathcal{T}_a^h(f) := (\mathcal{T}_a(f))^h$. With this notation, in Paper B we obtain the following basis for $\mathrm{PRS}(N, \Delta)_q$.

Theorem 2.2 [Thm. B.3.4]. *Let $N \mid q^s - 1$, 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 $\mathfrak{I}_d \subset \Delta$:

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

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

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

As a corollary, one can deduce a formula for the dimension of these subfield subcodes.

Corollary 2.3 [Cor. B.3.7]. *The dimension of* $\mathrm{PRS}(N,\Delta)_q$ *is the following:*

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

For the minimum distance, since $\mathrm{PRS}(N,\Delta)_q \subset \mathrm{PRS}(N,\Delta)$, we always have

$$\mathrm{wt}(\mathrm{PRS}(N,\Delta)_q) \geq N - d(\Delta) + 1.$$

For some applications (e.g., for quantum codes) it is useful to also have a basis for the dual of the code. The following result is due to Delsarte [38] and is often used to study the dual of subfield subcodes.

Theorem 2.4. *Let* $C \subset \mathbb{F}_{q^s}^n$ *be a linear code.*

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

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

The dual of $\mathrm{PRS}(N,\Delta)$ is studied in Paper B. We show that $\mathrm{PRS}(N,\Delta)^\perp$ is not generated by the evaluation of some monomials unless $p \mid N$ (where p is the characteristic of $\mathbb{F}_{q^s}$) or $\mathrm{wt}(\mathrm{PRS}(N,\Delta)) = 1$. For the case $p \mid N$, we obtain a basis for $\mathrm{PRS}(N,\Delta)^\perp$ in Proposition B.4.10. This result, together with Delsarte's theorem, allows us to obtain a basis for $(\mathrm{PRS}(N,\Delta)_q)^\perp$ in Theorem B.4.14.

Following the ideas from [53], we can evaluate at the zeroes of a trace (plus the point at infinity). In that case, instead of having a formula for the dimension, we only have a lower bound, which gives room for improvements in some cases. Indeed, by doing this, in Paper B, we obtain codes with parameters $[129, 90, 15]_4$, $[129, 86, 16]_4$ and $[129, 41, 44]_4$. In [64], a construction for a code with parameters $[129, 86, 16]_4$ is missing, and the parameters $[129, 90, 15]_4$ and $[129, 41, 44]_4$ exceed the best known values. By shortening and puncturing, we obtain 22 new codes in total, whose parameters improve the ones in the table or whose construction was missing.

For the case of projective Reed-Muller codes, for $m = 2$ we obtain explicit bases for their subfield subcodes and for the duals thereof in Paper C. To understand the linear independence of the evaluation of the polynomials involved, the crucial tool is considering the normal form of these polynomials with respect to the Gröbner basis from Theorem 1.2. When increasing m, the computations get increasingly involved. We give now a complementary approach, using the recursive construction from Paper D, which allows us to obtain bases for the subfield subcodes of projective Reed-Muller codes for any m for some particular degrees. We start with the aforementioned recursive construction. We denote by $\mathrm{RM}_d(m)$ the affine Reed-Muller code of degree obtained by evaluating the polynomials of degree $\leq d$ in m variables.

Theorem 2.5 [Thm. D.3.1]. *Let* $1 \leq d \leq m(q^s - 1)$ *and let* ξ *be a primitive element in* $\mathbb{F}_{q^s}$. *We have the following recursive construction:*

$$\mathrm{PRM}_d(m) = \{(u + v_{\xi,d}, v) \mid u \in \mathrm{RM}_{d-1}(m), v \in \mathrm{PRM}_d(m-1)\},$$

where $v_{\xi,d} := v \times \xi^d v \times \cdots \times \xi^{(q^s-2)d} v \times \{0\} = (v, \xi^d v, \xi^{2d} v, \ldots, \xi^{(q^s-2)d} v, 0)$.

This is reminiscent of what happens with binary Reed-Muller codes, which can be constructed recursively using the $(u, u+v)$ construction. Also note that, more generally, q-ary Reed-Muller codes can be constructed recursively using a matrix-product code construction [16]. For some particular degrees, this construction translates for the subfield subcodes.

Corollary 2.6 [Cor. D.4.2]**.** *Let $\xi \in \mathbb{F}_{q^s}$ be a primitive element. Let $m > 1$ and let $d_\lambda = \lambda\frac{q^s-1}{q-1}$ for some $\lambda \in \{1, 2, \ldots, m(q-1)\}$. Then we have*

$$(\mathrm{PRM}_{d_\lambda}(m))_q = \{(u + v_{\xi,d_\lambda}, v), u \in (\mathrm{RM}_{d_\lambda-1}(m))_q, v \in (\mathrm{PRM}_{d_\lambda}(m-1))_q\}.$$

As a consequence, we obtain:

$$\dim((\mathrm{PRM}_{d_\lambda}(m))_q) = \dim((\mathrm{RM}_{d_\lambda-1}(m))_q) + \dim((\mathrm{PRM}_{d_\lambda}(m-1))_q).$$

We see that, for those particular degrees, we obtain the dimension of the subfield subcode in a recursive manner. The dimension of the subfield subcodes of affine Reed-Muller codes is known, and the formula can be applied recursively until it depends on the projective Reed-Muller codes over $\mathbb{P}^2$ or $\mathbb{P}^1$, for which we know the dimension of their subfield subcodes by Papers B and C. In a similar recursive way, it is also possible to derive a basis for $(\mathrm{PRM}_{d_\lambda}(m))_q$ from bases of subfield subcodes of affine Reed-Muller codes (which are known [47]) and subfield subcodes of projective Reed-Muller codes in less variables.

In Table 1 we show the parameters of some subfield subcodes of projective Reed-Muller codes. All codes presented in Table 1 exceed the Gilbert-Varshamov bound, and some of them have the best known parameters according to [64]. More examples can be found in Papers C and D.

Table 1: Parameters of some subfield subcodes of projective Reed-Muller codes arising from the recursive construction.

q	s	m	λ	n	k	$\mathrm{wt}(C) \geq$
2	2	2	1	21	9	8
2	2	3	1	85	16	32
2	2	3	2	85	60	8
3	9	2	1	91	9	54
4	2	2	1	273	9	192
5	2	2	1	651	9	500
7	2	2	1	2451	9	2058

3 Generalized Hamming weights

The generalized Hamming weights (GHWs) of a code, introduced in [132], are a set of parameters that generalizes the minimum distance of a code. As such, they give finer information about the code, and, in terms of applications, they characterize the performance of the code on the wire-tap channel of type II and as a t-resilient function [132], and they also have applications to list decoding [62, 69]. Moreover, for certain families of codes, they are interesting by themselves, e.g., for projective Reed-Muller codes, they

give the maximum number of solutions of a system of homogeneous polynomial equations in the projective space over a finite field. In this thesis, we have studied the GHWs of projective Reed-Muller codes and matrix-product codes (which we will define later).

To introduce the GHWs of a code, we first start with the notion of support. Let $C \subset \mathbb{F}_q^n$, and let $D \subset C$ be a subcode. The support of D, denoted by $\mathrm{supp}(D)$, is defined as

$$\mathrm{supp}(D) := \{i \mid \exists\ u = (u_1, \ldots, u_n) \in D,\ u_i \neq 0\}.$$

The r-th *generalized Hamming weight* of C, denoted by $d_r(C)$, is defined as

$$d_r(C) := \min\{|\mathrm{supp}(D)| \mid D \text{ is a subcode of } C \text{ with } \dim D = r\}.$$

Remark 3.1. Note that we use the notation $d_r(C)$ for the r-th generalized Hamming weight, and d_i for some particular degree (depending on i) in some results. There is no confusion between the two notations since $d_r(C)$ always makes reference to the code C.

For ease of notation, throughout this thesis we will denote $d_0(C) = 0$, and $d_r(C) = \infty$ if $r > \dim C$. The GHWs satisfy the following general properties for any linear code C, as shown in [132].

Theorem 3.2 (Monotonicity)**.** *For an $[n, k]$ linear code C with $k > 0$ we have*

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n.$$

Corollary 3.3 (Generalized Singleton Bound)**.** *For an $[n, k]$ linear code C we have*

$$d_r(C) \leq n - k + r,\ 1 \leq r \leq k.$$

Remark 3.4. As a consequence of the previous results, for an MDS code C we have

$$d_r(C) = n - k + r,$$

for all $1 \leq r \leq k$.

In the following subsections, we show the results we have obtained in Papers D and H regarding the GHWs of projective Reed-Muller codes and matrix-product codes.

3.1 GHWs of projective Reed-Muller codes

The GHWs of affine Reed-Muller codes were completely determined more than 20 years ago in [72]. However, the computation of the GHWs of projective Reed-Muller codes in general remains an open problem and only partial results are known [9, 17, 36]. In [11], many of the previous results and hypotheses are collected, and the authors obtain the GHWs of projective Reed-Muller codes in some cases for degree $d < q$. In Paper D, we use the recursive construction from Theorem 2.5 to give a recursive lower bound for the GHWs of a projective Reed-Muller code of any degree, which we show next (note that we use q instead of q^s, which is what we used in Section 2 since we were considering subfield subcodes).

Theorem 3.5 [Thm. D.5.7]. *Let $1 \leq d \leq m(q-1)$ and $2 \leq r \leq \dim(\mathrm{PRM}_d(m))$. We consider*

$$Y = \left\{ (\alpha, \gamma) : \begin{array}{c} \max\{r - \dim \mathrm{RM}_{d-1}(m), 0\} \leq \alpha \leq \min\{\dim \mathrm{PRM}_d(m-1), r\} \\ \max\{r - \dim \mathrm{RM}_d(m), 0\} \leq \gamma \leq \min\{\dim \mathrm{PRM}_{d-(q-1)}(m-1), \alpha\} \end{array} \right\}.$$

Then we have

$$d_r(\mathrm{PRM}_d(m)) \geq \min_{(\alpha,\gamma)\in Y} B_{\alpha,\gamma},$$

where $B_{\alpha,\gamma}$ is defined as

$$\begin{aligned} B_{\alpha,\gamma} := &\max(d_{r-\gamma}(\mathrm{RM}_d(m)), d_{r-\alpha}(\mathrm{RM}_{d-1}(m))) \\ &+ \max(d_\alpha(\mathrm{PRM}_d(m-1)), d_\gamma(\mathrm{PRM}_{d-(q-1)}(m-1))). \end{aligned}$$

We say that the bound is recursive because it bounds the GHWs of $\mathrm{PRM}_d(m)$ using the GHWs of affine Reed-Muller codes (which are known [72]), and the GHWs of projective Reed-Muller codes in less variables. For $m = 1$, projective Reed-Muller codes are doubly extended Reed-Solomon codes, which are MDS and, thus, we know their GHWs by Remark 3.4. With the GHWs of doubly extended Reed-Solomon codes, we can bound the GHWs of projective Reed-Muller codes over $\mathbb{P}^2$, which can be used to bound the GHWs for $\mathbb{P}^3$, etc. There is another bound for the GHWs of projective Reed-Muller codes, the projective footprint bound, which is a generalization of the well known footprint bound to the projective case [10, 96]. In all the cases we have checked, the bound from Theorem 3.5 is greater than or equal to the projective footprint bound, and in many cases it is strictly greater. Moreover, the bound from Theorem 3.5 has proven to be much less computationally intensive to compute in our experiments than the projective footprint bound.

Since this result mainly depends on the recursive construction from Theorem 2.5, in Paper D we also use Theorem 2.6 to obtain a recursive bound for the GHWs of the subfield subcodes of projective Reed-Muller codes for some degrees.

To complement the lower bound from Theorem 3.5, we obtain the following upper bound.

Lemma 3.6 [Lem. D.5.8]. *Let $2 \leq r \leq \max\{\dim \mathrm{RM}_{d-1}(m), \dim \mathrm{PRM}_d(m-1)\}$ and $1 \leq d \leq m(q-1)$. Then*

$$d_r(\mathrm{PRM}_d(m)) \leq \min\{d_r(\mathrm{RM}_{d-1}(m)), q \cdot d_r(\mathrm{PRM}_d(m-1))\}.$$

Note that the previous result only gives a nontrivial bound if $r \leq \dim \mathrm{RM}_{d-1}(m)$ or $r \leq \dim \mathrm{PRM}_d(m-1)$. This upper bound, together with the monotonicity of the GHWs 3.2, allows us to obtain a criterion for verifying that the bound from Theorem 3.5 is sharp in many cases. In Table 2, we show the values we obtain for $q = 4$ and $m = 2$. We use dots when the GHWs grow by one unit when increasing r by one unit (note that, for these values, we obtain the exact value of the GHWs). Thus, with the general properties of the GHWs and our bounds, we obtain the exact value of the GHWs, except in 6 cases.

This table can be improved by considering the following result from [132].

Theorem 3.7 (Duality). *Let C be an $[n, k]$ code. Then*

$$\{d_r(C) : 1 \leq r \leq k\} = \{1, 2, \ldots, n\} \setminus \{n + 1 - d_r(C^\perp) : 1 \leq r \leq n - k\}.$$

Table 2: Generalized Hamming weights for $q = 4$, $m = 2$.

$d\backslash r$	2	3	4	5	6	7	8	9	10	11	$\cdots$	20
1	20	21										
2	15	16	19	20	21							
3	10-11	11-12	14	15	16	18	19	20	21			
4	5-7	8	9-10	10-11	12	13	14	15	16	17	$\cdots$	
5	4	5-6	7	8	9	10	11	12	13	14	$\cdots$	
6	3	4	5	6	7	8	9	10	11	12	$\cdots$	21

The set $\{d_r(C) : 1 \leq r \leq k\}$ is called the weight hierarchy of the code C. From Theorem 3.7 we see that the weight hierarchy of a code is completely determined by the weight hierarchy of its dual, and vice versa. Since we know that, for $d \not\equiv 0 \bmod q-1$, the dual of a projective Reed-Muller code is also a projective Reed-Muller code by Theorem 1.4, for a given code $\mathrm{PRM}_d(m)$ we can apply our bounds to its dual code and obtain additional information about the weight hierarchy of $\mathrm{PRM}_d(m)$. In this way, for the case $d \not\equiv 0 \bmod q-1$, we improve the values from Table 2 to the ones in Table 3. We note that we obtain the exact value of all the GHWs with $d \not\equiv 0 \bmod q-1$ in this case. Further examples can be found in Paper D.

Table 3: Improved table of the generalized Hamming weights for $q = 4$, $m = 2$, with $d \not\equiv 0 \bmod q-1$.

$d\backslash r$	2	3	4	5	6	7	8	9	10	11	$\cdots$	18
1	20	21										
2	15	16	19	20	21							
4	5	8	9	11	12	13	14	15	16	17	$\cdots$	
5	4	5	7	8	9	10	11	12	13	14	$\cdots$	21

3.2 GHWs of matrix-product codes

Matrix-product codes (MPCs) were introduced by Blackmore and Norton in [16]. These codes have been object of study for many different applications [50, 51, 92, 93]. From the properties of the constituent codes, one can derive properties of the corresponding MPC. Most notably, one can obtain a lower bound for the minimum distance of the MPC from the minimum distances of the constituent codes [16], but one can also derive self-orthogonality properties for some matrices [51, 81, 95] or decoding algorithms [73, 74, 77].

The aim of this subsection is to study the GHWs of a MPC in terms of those of its constituent codes. By doing this, one can consider families of codes with known GHWs, and derive different codes with bounded GHWs using the MPC construction. This allows us to substantially expand the families of codes for which we have bounds for their GHWs. Some of the results of in subsection are reminiscent of the results from Section 3.1, since the techniques are inspired by the ones used in Paper D. This is mainly due to the fact that the recursive construction from Theorem 2.5 resembles the $(u, u+v)$ construction, a particular case of a matrix-product code construction. We start by defining MPCs as in [16].

Definition 3.8. Let $C_1, \ldots, C_\ell \subset \mathbb{F}_q^n$ be linear codes of length n, which we call *constituent codes*, and let $A = (a_{ij}) \in \mathbb{F}_q^{\ell \times h}$ be an $\ell \times h$ matrix, with $\ell \leq h$. The *matrix-product code* associated to A and $C_1, \ldots, C_\ell$ is denoted $C = [C_1, \ldots, C_\ell] \cdot A$, and it is the set of all matrix products $[v_1, \ldots, v_\ell] \cdot A$, where $v_i = (v_{1i}, \ldots, v_{ni})^t \in C_i$ is an $n \times 1$ column vector, for $i = 1, \ldots, \ell$. Thus, the codewords of C are $n \times h$ matrices

$$c = \begin{pmatrix} v_{11}a_{11} + \cdots + v_{1\ell}a_{\ell 1} & \cdots & v_{11}a_{1h} + \cdots + v_{1\ell}a_{\ell h} \\ \vdots & \ddots & \vdots \\ v_{n1}a_{11} + \cdots + v_{n\ell}a_{\ell 1} & \cdots & v_{n1}a_{1h} + \cdots + v_{n\ell}a_{\ell h} \end{pmatrix}.$$

Let us denote by $R_i = (a_{i,1}, \ldots, a_{i,h})$ the element of $\mathbb{F}_q^h$ given by the i-th row of A, for $1 \leq i \leq \ell$. We denote by $d_1(C_{R_i})$ the minimum distance of the code C_{R_i} generated by $\langle R_1, \ldots, R_i \rangle$ in $\mathbb{F}_q^h$. In [106] it is proven that

$$d_1(C) \geq \min\{d_1(C_1)d_1(C_{R_1}), \ldots, d_1(C_\ell)d_1(C_{R_\ell})\}, \tag{3.1}$$

where $d_1(D)$ denotes the minimum distance the code D. Moreover, in [74], the authors prove that the previous bound is sharp if $C_\ell \subset \cdots \subset C_1$. When working with MPCs, it is usual to consider the following condition, introduced in [16].

Definition 3.9. Let A be an $\ell \times h$ matrix, and let A_t be the matrix formed by the first t rows of A. For $1 \leq j_i < \cdots < j_t \leq h$, we denote by $A(j_1, \ldots, j_t)$ the $t \times t$ matrix consisting of the columns $j_1, \ldots, j_t$ of A_t. A matrix A is *non-singular by columns* (NSC) if $A(j_1, \ldots, j_t)$ is non-singular for each $1 \leq t \leq \ell$ and $1 \leq j_1 < \cdots < j_t \leq h$. In particular, an NSC matrix has full rank.

In [16] it is shown that, if A is NSC, then the codes C_{R_i} are MDS, for $1 \leq i \leq \ell$. This implies that the bound (3.1) becomes

$$d_1(C) \geq \min\{hd_1(C_1), (h-1)d_1(C_2), \ldots, (h-\ell+1)d_1(C_\ell)\} \tag{3.2}$$

for the case of an NSC matrix. One of the goals of this subsection is to generalize the bounds (3.1) and (3.2) to the case of the GHWs of C.

We start by considering a 2×2 NSC matrix A. If we denote

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

since A is NSC, we have $a_{1j} \neq 0$, $1 \leq j \leq 2$, and we will assume (without loss of generality) that $a_{22} \neq 0$. The following result from Paper H bounds from below the GHWs of a MPC in terms of the GHWs of sums and intersections of the constituent codes.

Theorem 3.10 [Thm. H.3.1]**.** *Let $C_1, C_2 \subset \mathbb{F}_q^n$, and let $C = [C_1, C_2] \cdot A$, with A as above. Let $1 \leq r \leq \dim C$ and consider*

$$Y = \left\{ (\alpha_1, \alpha_2) : \begin{array}{c} \max\{r - \dim(C_1 + C_2), 0\} \leq \alpha_1 \leq \min\{\dim C_2, r\} \\ \max\{r - \dim(C_1 + C_2), 0\} \leq \alpha_2 \leq \min\{\dim(C_1 \cap C_2), r\} \\ \alpha_1 + \alpha_2 \leq r \end{array} \right\}.$$

Then

$$d_r(C) \geq \min_{(\alpha_1, \alpha_2) \in Y} B_{\alpha_1, \alpha_2},$$

where

$$B_{\alpha_1,\alpha_2} = \max\{d_{r-\alpha_1}(C_1 + C_2), d_{\alpha_2}(C_1 \cap C_2)\} + \max\{d_{r-\alpha_2}(C_1 + C_2), d_{\alpha_1}(C_2)\}.$$

For the case in which the constituent codes are nested, a lower bound for the MPCs of a code with any number of constituent codes is given in Paper H, in terms of the GHWs of the constituent codes. We show next the explicit bounds we obtain for the case of two and three constituent codes, which are the most frequent cases for applications.

Corollary 3.11 [Cor. H.4.3]**.** *Let $C_2 \subset C_1 \subset \mathbb{F}_q^n$, $C = [C_1, C_2] \cdot A$, for some 2×2 NSC matrix A. Consider $1 \leq r \leq \dim C_1 + \dim C_2$, and let*

$$Y = \left\{ (\alpha_1, \alpha_2) : \begin{array}{c} \max\{r - \dim C_1, 0\} \leq \alpha_i \leq \min\{\dim C_2, r\},\ 1 \leq i \leq 2 \\ \alpha_1 + \alpha_2 \leq r \end{array} \right\}.$$

We consider

$$B_{\alpha_1,\alpha_2} = \max\{d_{r-\alpha_1}(C_1), d_{\alpha_2}(C_2)\} + \max\{d_{r-\alpha_2}(C_1), d_{\alpha_1}(C_2)\}.$$

Then

$$d_r(C) \geq \min_{(\alpha_1,\alpha_2)\in Y} B_{\alpha_1,\alpha_2}.$$

For the following result, when a subindex is greater than 3, we consider its reduction modulo 3. For instance, for $i = 2$, we have $\alpha_{i+1} + \alpha_{i+2} = \alpha_3 + \alpha_1$.

Theorem 3.12 [Thm. H.4.4]**.** *Let $C_3 \subset C_2 \subset C_1 \subset \mathbb{F}_q^n$ and $C = [C_1, C_2, C_3] \cdot A$, for some 3×3 NSC matrix A. Let $\mathbb{Z}^{3,3,1} := \mathbb{Z}^3_{\geq 0} \times \mathbb{Z}^3_{\geq 0} \times \mathbb{Z}_{\geq 0}$. Consider $1 \leq r \leq \sum_{i=1}^3 \dim C_i$, and let*

$$Y = \left\{ (\alpha, \gamma, \beta) \in \mathbb{Z}^{3,3,1} : \begin{array}{c} 0 \leq \gamma_i \leq \dim C_3,\ 1 \leq i \leq 3 \\ \max\{r - \dim C_1, \gamma_{i+1} + \gamma_{i+2}\} \leq \alpha_i,\ 1 \leq i \leq 3 \\ \alpha_{i+1} + \alpha_{i+2} - \gamma_i \leq \beta,\ 1 \leq i \leq 3 \\ \beta \leq \min\left\{ \sum_{i=1}^3 (\alpha_i - \gamma_i), \dim C_2 + \min\{\alpha_i, 1 \leq i \leq 3\}, r \right\} \end{array} \right\}.$$

For $(\alpha, \gamma, \beta) \in Y$, we consider

$$B_{\alpha,\gamma,\beta} = \sum_{i=1}^3 \max\{d_{r-\alpha_i}(C_1), d_{\beta-\alpha_i}(C_2), d_{\gamma_i}(C_3)\}.$$

Then we have

$$d_r(C) \geq \min_{(\alpha,\gamma,\beta)\in Y} B_{\alpha,\gamma,\beta}.$$

Note that Theorem 3.10 simplifies to Corollary 3.11 when assuming $C_2 \subset C_1$. Moreover, for $r = 1$, both Corollary 3.11 and Theorem 3.12 reduce to the bound (3.2). Therefore, they can be seen as a generalization of the usual bound for the minimum distance of MPCs.

In Paper H, for the nested case we also provide an upper bound for the GHWs of MPCs, which is very similar to the bound (3.1) (we recall that this bound is known to be sharp for the nested case).

Proposition 3.13 [Prop. H.5.1]. *Let $C_\ell \subset \cdots \subset C_1$, and $C = [C_1, \ldots, C_\ell] \cdot A$, where $A \subset \mathbb{F}_q^{\ell \times h}$ and has full rank. Let $1 \leq r \leq \dim C_1$ and let $1 \leq i \leq \ell$ be such that $r \leq \dim C_i$. Then*

$$d_r(C) \leq d_r(C_i) d_1(C_{R_i}).$$

As a sample of what can be obtained with our results for particular families of codes, we show the following result for Reed-Solomon codes. Here, $\mathrm{RS}(k)$ denotes a Reed-Solomon code of length $n \leq q$ and dimension k.

Theorem 3.14 [Thm. H.6.1]. *Let $1 \leq k_2 \leq k_1 \leq n \leq q$, let $A \subset \mathbb{F}_q^{2\times 2}$ be a NSC matrix, and let $\mathrm{RS}(k_1, k_2) := [\mathrm{RS}(k_1), \mathrm{RS}(k_2)] \cdot A$. For $1 \leq r \leq \dim \mathrm{RS}(k_1, k_2) = k_1 + k_2$, we have*

$$d_r(\mathrm{RS}(k_1, k_2)) = \begin{cases} 2n + r - (k_1 + k_2) & \text{if } r > \max\{k_1 - k_2, k_2\}, \\ \min\{2d_r(\mathrm{RS}(k_1)), d_r(\mathrm{RS}(k_2))\} & \text{if } r \leq \max\{k_1 - k_2, k_2\}. \end{cases}$$

4 Applications to quantum error-correction

The interest in quantum computation is rapidly growing due to the possibility of implementing algorithms with exponential speedups with respect to the classical counterparts, e.g., Shor's algorithm for finding prime factors of an integer [124]. In this setting, we are mainly interested in quantum computing and quantum communication. In both scenarios, due to noise and decoherence, the physical qudits can be subject to errors. Similarly to the classical case, one can consider *quantum error-correcting codes* (QECCs), first introduced by Shor [123], which allow us to recover the correct quantum state as long as the amount of errors does not surpass the error-correction capabilities of the QECC. Unlike the classical scenario, there are (at least) two types of errors we can consider for qudits, namely *qudit-flip* and *phase-shift errors*, which are not equally likely to occur [79, 121]. This gives rise to asymmetric QECCs, which have two minimum distances, δ_x and δ_z, meaning that they can correct up to $\lfloor (\delta_x - 1)/2 \rfloor$ qudit-flip errors and $\lfloor (\delta_z - 1)/2 \rfloor$ phase-flip errors, respectively. However, most known families QECCs are symmetric, meaning that they only consider one minimum distance $\delta = \min\{\delta_x, \delta_z\}$, that is, they are assumed to have the same error-correction capabilities for each type of error. For instance, one of the constructions we will see below only works for the symmetric case.

Focusing on the problem of constructing quantum codes, Calderbank and Shor [23], and Steane [127], independently showed how to use classical codes to construct QECCs. These constructions require self-orthogonal classical codes with respect to the Euclidean or Hermitian inner product, and the respective constructions are known as the CSS construction and the Hermitian construction, respectively. By considering entanglement between the encoder and the decoder, it is possible to construct entanglement-assisted error-correcting codes (EAQECCs) [21,48] with higher rate than usual QECCs. Even though creating and maintaining entanglement between the encoder and the decoder can be costly, the increase in rate and the fact that EAQECCs can be constructed from classical codes that are not necessarily self-orthogonal make these codes good candidates for quantum communication. Since EAQECCs are a generalization of QECCs, we state now the CSS construction in its general form for EAQECCs [48].

Theorem 4.1 (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 asymmetric EAQECC with parameters $[[n, \kappa, \delta_z/\delta_x; c]]_q$, where*

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

With respect to the parameters of a quantum code, the length n is the number of physical qudits used, the dimension κ is the number of logical qudits, and the meaning of δ_z and δ_x in terms of error-correction capabilities was explained previously. Let $\delta_z^* := d_1(C_1^\perp)$ and $\delta_x^* := d_1(C_2^\perp)$. If $\delta_z = \delta_z^*$ and $\delta_x = \delta_x^*$, we say that the corresponding EAQECC is *pure* (or *nondegenerate*), and we say it is *impure* (or *degenerate*) if $\delta_z > \delta_z^*$ or $\delta_x > \delta_x^*$.

Regarding c, this parameter determines the minimum number required of maximally entangled pairs. Note that if we take $C_1 \subset C_2^\perp$, then $c = 0$. Indeed, the parameter c is determined by the dimension of the *relative hull* of C_1 with respect to C_2, which is defined in [3] as

$$\mathrm{Hull}_{C_2}(C_1) := C_1 \cap C_2^\perp.$$

This justifies the study of the hulls of certain families of codes, since, together with the minimum distance and dimension, they determine the parameters of the corresponding EAQECC.

For the Hermitian construction, we have to introduce first the Hermitian inner product. Let $C \subset \mathbb{F}_{q^2}^n$. The Hermitian product of two vectors $v, w \in \mathbb{F}_{q^2}^n$ is defined as

$$v \cdot_h w = \sum_{i=1}^{n} v_i w_i^q.$$

The Hermitian dual of a code $C \subset \mathbb{F}_{q^2}^n$ is defined as $C^{\perp_h} := \{v \in \mathbb{F}_{q^2}^n \mid v \cdot_h w = 0,\ \forall\, w \in C\}$. With this notation, we can introduce the Hermitian construction [48].

Theorem 4.2 (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*

$$c = k - \dim(C \cap C^{\perp_h}),\ \kappa = n - 2k + c, \quad \text{and } \delta = d_1(C^{\perp_h} \setminus (C \cap C^{\perp_h})).$$

We note that this construction considers only the case of symmetric QECCs. Let $\delta^* = d_1(C^{\perp_h})$. In the symmetric case we say that the corresponding EAQECC is pure (or nondegenerate) if $\delta = \delta^*$, and impure (or degenerate) otherwise. Similarly to the Euclidean setting, we can define the *Hermitian hull* of C as

$$\mathrm{Hull}^H(C) = C \cap C^{\perp_h},$$

which determines the parameter c for the EAQECCs obtained from the Hermitian construction.

4.1 Quantum communication

In this section we highlight some of the results of this thesis which are better suited for quantum communication, although the codes that we obtain in this section with $c = 0$ could also be considered for fault-tolerant computation.

In Paper B, we use subfield subcodes of projective Reed-Solomon codes (mentioned in Section 2) to construct EAQECCs with both the CSS construction and the Hermitian construction. Recall the notation $\Delta_{\mathfrak{J}} = \bigcup_{\mathfrak{J}_a \subset \Delta} \mathfrak{J}_a \subset \Delta$, and we also introduce $\Delta^{\perp} := \{\alpha \in \{0, 1, \ldots, N-1\} \mid \alpha \neq N-1-h, h \in \Delta\}$. Also recall that $N \mid q^s - 1$. The following result shows the parameters of the asymmetric EAQECCs obtained with subfield subcodes of projective Reed-Solomon codes.

Theorem 4.3 [Thm. B.5.11]. *Let $1 \leq d_1, d_2 \leq N-1$, 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 $((\Delta'_{d_1})_{\mathfrak{J}})^{\perp} \subset (\Delta'_{d_2})_{\mathfrak{J}}$, then we can construct an asymmetric EAQECC with parameters*

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

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

The codes from this construction are shown to outperform the ones obtained with BCH codes in [49] in Paper B.

Given $a_i \in \mathcal{A}$, we denote by a'_i the minimal element in $\mathcal{A}$ such that $\mathfrak{J}_{a'_i} = \mathfrak{J}_{-qa_i}$. Let $\Delta = \bigcup_{i=0}^{t} \mathfrak{J}_{a_i}$. We denote $\Delta^{\perp_h} := \{0, 1, \ldots, N-1\} \setminus \bigcup_{i=0}^{t} \mathfrak{J}_{a'_i}$. With the Hermitian construction, the following result is obtained using subfield subcodes of projective Reed-Solomon codes.

Theorem 4.4 [Thm. B.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 $\mathfrak{J}_{a_i}$, $0 \leq i \leq z$, of $\{0, 1, \ldots, N-1\}$ with respect to q^2. Let $\Delta = \bigcup_{i=0}^{t-1} \mathfrak{J}_{a_i} \cup \{a_t\}$ such that $d(\Delta) < N-1$ and $\Delta'' \subset (\Delta'')^{\perp_h}$. 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 $c \leq 1$.*

From this construction, we find 16 new EAQECCs over $\mathbb{F}_2$, which improve the table for EAQECCs from [64].

In Paper E, we study the relative and Hermitian hull of projective Reed-Muller codes over the projective plane. Since the dual of a projective Reed-Muller code is another projective Reed-Muller code by Theorem 1.4 (if $d \not\equiv 0 \bmod q-1$), to study the relative hull we can study $\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2)$ instead. A similar approach can be taken for the Hermitian hull, but we focus on the relative hull now for simplicity. In Paper E, we obtain the following result.

Corollary 4.5 [Cor. E.3.11]. *Let $1 \leq d_1 < d_2 \leq 2(q-1)$. Let $k_1 = \dim \mathrm{RM}_{d_1-1}(2)$. If $d_1 \equiv d_2 \bmod q-1$, then $\dim(\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2)) = \dim \mathrm{PRM}_{d_1}(2)$. If $d_1 \not\equiv d_2 \bmod q-1$, then*

$$\dim(\mathrm{PRM}_{d_1}(2) \cap \mathrm{PRM}_{d_2}(2)) = \begin{cases} k_1 & \text{if } d_2 \leq q-1, \\ k_1 + \min\{d_1, d_2 - (q-1)\} & \text{if } d_1 \leq q-1 < d_2, \\ k_1 + d_2 - q + 2 & \text{if } q \leq d_1. \end{cases}$$

The techniques used to obtain this result are based on the results from Section 1. In fact, in Paper E, we obtain a set of polynomials such that its image by the evaluation map gives precisely the relative hull of the corresponding projective Reed-Muller codes. An

interesting aspect we encountered is that the relative hull (and the Hermitian hull) is not a monomial code in some cases, even though projective Reed-Muller codes are monomial codes (in the sense that they can be generated by the evaluation of monomials). This is specially relevant for the Hermitian case, and it makes the computation for that case much more involved.

By obtaining the dimension of the relative and Hermitian hull, we find all the parameters for the EAQECCs constructed with projective Reed-Muller codes over the projective plane. We obtain the following results from the CSS construction.

Theorem 4.6 [Thm. E.4.4]**.** *Let* $1 \leq d_1 \leq d_2 < 2(q-1)$*,* $d_1 + d_2 \not\equiv 0 \bmod q-1$*,* $d_1 \neq q-1 \neq d_2$*. Let* $k_1 = \dim \mathrm{RM}_{d_1-1}(2)$ *and* $k_2 = \dim \mathrm{RM}_{d_2^\perp-1}(2)$*, where* $d_2^\perp = 2(q-1) - d_2$*. Then we can construct an asymmetric EAQECC with parameters* $[[n, \kappa, \delta_z/\delta_x; c]]_q$*, where* $n = q^2+q+1$*,* $\kappa = n - (\dim \mathrm{PRM}_{d_1}(2) + \dim \mathrm{PRM}_{d_2}(2)) + c$*,* $\delta_z = \mathrm{wt}(\mathrm{PRM}_{d_2}^\perp(2))$*,* $\delta_x = \mathrm{wt}(\mathrm{PRM}_{d_1}^\perp(2))$*, and the value of* c *is the following:*

1. *If* $d_1 + d_2 < 2(q-1)$*:*

$$c = \begin{cases} d_1 + 1 - \min\{d_1, q-1-d_2\} & \text{if } d_2 < q-1, \\ d_1 + 1 & \text{if } q \leq d_2. \end{cases}$$

2. *If* $d_1 + d_2 > 2(q-1)$*:*

$$c = \begin{cases} k_1 - k_2 + d_1 + 1 & \text{if } d_1 < q-1, \\ k_1 - k_2 + q + 1 - \min\{d_2^\perp, d_1 - (q-1)\} & \text{if } q \leq d_1. \end{cases}$$

Moreover, this code is pure.

Since the use of entanglement provides both advantages (e.g., more rate) and disadvantages (it can be costly to maintain entanglement), for each application one might require different amounts of maximally entangled pairs. This gives rise to the study of families of codes with flexibility regarding the parameter c. Such flexibility can be achieved by changing the dimension of the hull via monomially equivalent codes. For this purpose, we need to introduce the following notation. The *Schur product* of two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{F}_q^n$ is defined by

$$x \star y := (x_1 y_1, \ldots, x_n y_n).$$

The *Schur product* of two codes $C_1, C_2 \subset \mathbb{F}_q^n$, denoted by $C_1 \star C_2$, is defined as the code generated by the vectors

$$\{c_1 \star c_2 : c_i \in C_i\} \subset \mathbb{F}_q^n.$$

The main result we use for the Euclidean case is the following theorem from [3].

Theorem 4.7. *For* $i = 1, 2$*, let* C_i *be* $[n, k_i]_q$ *codes with* $q > 2$*. For any* ℓ *with* $\max\{0, k_1 - k_2\} \leq \ell \leq \max \mathrm{wt}((C_1 \star C_2)^\perp) - n + k_1$*, there exists a code* $C_{1,\ell}$ *equivalent to* C_1 *such that*

$$\dim \mathrm{Hull}_{C_2}(C_{1,\ell}) = \ell.$$

In particular, if $\max \mathrm{wt}((C_1 \star C_2)^\perp) = \min\{n, 2n - k_1 - k_2\}$*,* ℓ *runs over all the possible values of* $\dim \mathrm{Hull}_{C_2}(C_1')$*, where* C_1' *is a code equivalent to* C_1*.*

For the Hermitian case, we obtain a similar result by combining the following results from [31] and [91], respectively.

Theorem 4.8. *Let $C \subset \mathbb{F}_{q^2}$ be a linear code. If there is a vector $v \in ((C \star C^q)^{\perp})_q$ with $\mathrm{wt}(v) = n$, then $\langle v \rangle \star C \subset (\langle v \rangle \star C)^{\perp_h}$, i.e., $\langle v \rangle \star C$ is self-orthogonal with respect to the Hermitian product.*

Theorem 4.9. *Let $q > 2$ and let $C \subset \mathbb{F}_{q^2}^n$ with $\dim \mathrm{Hull}_H(C) = \ell$. Then there exists a monomially equivalent code $C_{\ell'}$ with $\dim \mathrm{Hull}_H(C_{\ell'}) = \ell'$, for each $0 \leq \ell' \leq \ell$.*

In Paper F, we use these results to provide families of EAQECCs obtained with the CSS and Hermitian constructions using projective Reed-Muller codes, as we show next.

Theorem 4.10 [Thm. F.3.7]**.** *Let $1 \leq d_1 \leq d_2 < q-2$ such that $d_1 + d_2 < q-2$. Then we can construct a quantum code with parameters $[[n, \kappa + c, \delta_z/\delta_x; c]]_q$, for any $0 \leq c \leq \dim \mathrm{PRM}_{d_1}(m)$, where $n = \frac{q^{m+1}-1}{q-1}$, $\kappa = n - (\dim \mathrm{PRM}_{d_1}(m) + \dim \mathrm{PRM}_{d_2}(m))$, $\delta_z \geq \mathrm{wt}(\mathrm{PRM}_{d_2}^{\perp}(m))$ and $\delta_x \geq \mathrm{wt}(\mathrm{PRM}_{d_1}^{\perp}(m))$.*

Theorem 4.11 [Thm. F.4.6]**.** *Let $1 \leq d < q-2$. Then we can construct an EAQECC with parameters $[[n, \kappa + c, \delta; c]]_q$, for any $0 \leq c \leq \dim \mathrm{PRM}_d(q^2, m)$, where $n = \frac{q^{2(m+1)}-1}{q^2-1}$, $\kappa = n - 2(\dim \mathrm{PRM}_d(q^2, m))$ and $\delta \geq \mathrm{wt}(\mathrm{PRM}_{d^{\perp}}(q^2, m))$.*

With these constructions, we obtain many codes surpassing the quantum Gilbert-Varshamov bounds from [44, 98]. Moreover, we are also able to derive QECCs (without entanglement assistance) with subfield subcodes of projective Reed-Muller codes, using the results from Paper D.

4.2 Fault-tolerant quantum computing

For this subsection, we only consider the case $q = 2$, and we therefore write qubits instead of qudits. To achieve fault-tolerant quantum computation, we can encode the physical qubits using a QECC. By doing this, we obtain κ logical qubits which can be considered resistant to errors. One of the main problems with this approach is obtaining QECCs that implement the desired operations on the logical qubits. Particularly interesting are implementations that only involve transversal gates on the physical qubits, since they split into gates that act on individual physical qubits and they naturally mitigate the proliferation of errors. However, due to Eastin–Knill theorem [41], it is not possible to find a QECC that implements a universal gate set transversely. A common strategy to circumvent this limitation is to consider codes that implement the Clifford group transversely, and then perform magic state distillation to apply a logical non-Clifford gate, usually the T gate [20]. This is enough for implementing any gate, since adding a non-Clifford gate to the Clifford group gives a universal gate set (this is well known for the binary case, and for the general case it can be deduced from [103, Thm 6.5] and [104, Cor. 6.8.2]).

However, this requires a code implementing T transversely. In general, implementing logical non-Clifford gates is more difficult than implementing logical Clifford gates, and logical non-Clifford gates must be induced by a non-Clifford operation on the physical gates [35, 63]. Moreover, Gottesman-Knill theorem [63] also implies that quantum computation is only more powerful than classical computation when it uses gates outside the

Clifford group. The previous discussion highlights the importance of finding transversal implementations of non-Clifford gates. As we already mentioned before, the usual choice for the non-Clifford gate to be implemented via the magic state distillation protocol is the T gate due to its simplicity.

With this motivation, CSS-T were introduced in [111, 112]. These are CSS codes which support a transversal T gate, that is, applying T transversely on the physical qubits gives a logical operation over the logical qubits. This is weaker than requiring the code to implement T transversely on the logical qubits, but studying these codes gives good candidates for codes that may implement logical non-Clifford operations.

Let $C \subset \mathbb{F}_2^n$ and $S \subset \{1, \dots, n\}$. We denote by C_S (resp. C^S) the shortening (res. puncturing) of C in the coordinates indexed by the elements in S. For $x \in C$, we denote $Z(x) := \{1, \dots, n\} \setminus \mathrm{supp}(x)$, where $\mathrm{supp}(x) = \{i \mid x_i \neq 0\}$. We introduce now the definition of CSS-T codes as stated in [111].

Definition 4.12. Let $C_2 \subset C_1 \subset \mathbb{F}_2^n$. Then we say (C_1, C_2) is a *CSS-T pair* if C_2 is even-weighted and, for any $x \in C_2$, the shortening $(C_1^\perp)_{Z(x)}$ contains a self-dual code.

Note that, given a CSS-T pair (D_1, D_2), the corresponding quantum code is obtained from Theorem 4.1 by taking $C_1 = D_2$, $C_2 = D_1^\perp$.

In general, using Definition 4.12 to check if a pair of codes is a CSS-T pair is not efficient, since it would require to check a condition for every $x \in C_2$. In Paper G, we give an alternative definition by using the Schur product of codes, which we introduced previously. We also define now the *t-fold Schur product* of C with itself: $C^{\star t} := \underbrace{C \star \cdots \star C}_{t}$.

In Paper G we obtain the following result.

Theorem 4.13 [Thm. G.2.3]**.** *Let C_1 and C_2 be binary codes of length n. The following are equivalent.*

(1) *(C_1, C_2) is a CSS-T pair.*

(2) *$C_2 \subset C_1$, C_2 is even-weighted, and for any $x \in C_2$ the code $C_1^{Z(x)}$ is self-orthogonal.*

(3) *$C_2 \subset C_1 \cap (C_1^{\star 2})^\perp$.*

(4) *$C_1^\perp + C_1^{\star 2} \subset C_2^\perp$.*

Moreover, if (C_1, C_2) is a CSS-T pair then C_2 is self-orthogonal.

The alternative condition (2) was already proved in [4], but it still requires to check the self-orthogonality condition for every $x \in C_2$, whereas (3) and (4) only depend on global properties of the codes C_1 and C_2. With these alternative conditions, we define the partially ordered set (poset) of CSS-T pairs. In Paper G, we study this poset and, as a consequence, we obtain the following propagation rule for CSS-T pairs.

Corollary 4.14 [Cor. G.3.9]**.** *Let (C_1, C_2) be a CSS-T pair such that the associated $[[n, k, d]]$ CSS-T code is nondegenerate. For any $y \in C_2^\perp \cap (C_1 \star C_2)^\perp$ and $y \notin C_1$, the pair $(C_1 + \langle y \rangle, C_2)$ is a nondegenerate CSS-T pair with parameters*

$$[[n, k+1, d]].$$

Using our characterization of CSS-T pairs, we determine the CSS-T pairs formed by cyclic (and extended cyclic) codes. Take an integer $s > 1$ and consider the field extension $\mathbb{F}_{2^s}/\mathbb{F}_2$. We set n with $n \mid 2^s - 1$. Let $\beta \in \mathbb{F}_{2^s}$ be a primitive n-th root of unity. For the set $\mathbb{Z}/n\mathbb{Z}$, we will consider the representatives between 1 and n, i.e., $\mathbb{Z}/n\mathbb{Z} = \{1, 2, \ldots, n\}$.

Definition 4.15. Let $g \in \mathbb{F}_2[x]$ such that g divides $x^n - 1$. The *defining set* is given by $J := \{j \in \mathbb{Z}/n\mathbb{Z} : g(\beta^j) = 0\}$, and the *generating set* by $I := \{i \in \mathbb{Z}/n\mathbb{Z} : g(\beta^i) \neq 0\}$.

We denote by $C(I)$ the cyclic code generated by g. Note that cyclic codes can be regarded as subfield subcodes of evaluation codes [13], and therefore some of the ideas showed in Section 2 about cyclotomic sets and traces can be applied here. In Paper G, we obtain the following characterization for the CSS-T pairs arising from cyclic codes.

Theorem 4.16 [Thm. G.4.8]**.** *Let $I_1, I_2 \subset \mathbb{Z}/n\mathbb{Z}$ be cyclotomic cosets. Then $(C(I_1), C(I_2))$ is a CSS-T pair if and only if:*

(1) $I_2 \subset I_1$ *and*

(2) $n \notin (I_1 + I_1 + I_2)$.

An analogous result holds for extended cyclic codes. The resulting CSS-T codes have better parameters than the CSS-T codes in the current literature, namely the CSS-T pairs arising from Reed-Muller codes [4], and triorthogonal codes [19, 70, 105]. Note that triorthogonal codes not only support the transversal T gate, but they also induce the logical T gate. Since this is a stronger condition than being CSS-T, it is natural that we obtain better parameters.

Part II

Publications

Paper A

Saturation and vanishing ideals

Philippe Gimenez, Diego Ruano, Rodrigo San-José

Abstract

We consider an homogeneous ideal I in the polynomial ring $S = K[x_1, \ldots, x_m]$ over a finite field $K = \mathbb{F}_q$ and the finite set of projective rational points $\mathbb{X}$ that it defines in the projective space $\mathbb{P}^{m-1}$. We concern ourselves with the problem of computing the vanishing ideal $I(\mathbb{X})$. This is usually done by adding the equations of the projective space $I(\mathbb{P}^{m-1})$ to I and computing the radical. We give an alternative and more efficient way using the saturation with respect to the homogeneous maximal ideal.

Keywords: Projective codes, evaluation codes, vanishing ideal, saturation, radical.
MSC: 13P25, 13M10, 94B27.
DOI: 10.1007/s40863-022-00330-y
Reference: P. Gimenez, D. Ruano, R. San-José. Saturation and vanishing ideals. São Paulo J. Math. Sci., 17, 147-155 (2023).

Paper B

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

Philippe Gimenez, Diego Ruano, Rodrigo San-José

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.

MSC: 81P70, 94B05, 13P25.

DOI: 10.1007/s40314-023-02506-4

Reference: P. Gimenez, D. Ruano, R. San-José. Entanglement-assisted quantum error-correcting codes from subfield subcodes of projective Reed-Solomon codes. Comp. Appl. Math. 42, 363 (2023).

Paper C

Subfield subcodes of projective Reed-Muller codes

Philippe Gimenez, Diego Ruano, Rodrigo San-José

Abstract

Explicit bases for the subfield subcodes of projective Reed-Muller codes over the projective plane and their duals are obtained. In particular, we provide a formula for the dimension of these codes. For the general case over the projective space, we generalize the necessary tools to deal with this case as well: we obtain a universal Gröbner basis for the vanishing ideal of the set of standard representatives of the projective space and we show how to reduce any monomial with respect to this Gröbner basis. With respect to the parameters of these codes, by considering subfield subcodes of projective Reed-Muller codes we obtain long linear codes with good parameters over a small finite field.

Keywords: Evaluation codes, linear codes, projective Reed-Muller codes, subfield subcodes, trace.

MSC: 11T71, 94B05, 14G50, 13P25.

DOI: 10.1016/j.ffa.2023.102353

Reference: P. Gimenez, D. Ruano, R. San-José. Subfield subcodes of projective Reed-Muller codes. Finite Fields Appl. 94, 102353 (2024).

Paper D

A recursive construction for projective Reed-Muller codes

Rodrigo San-José

Abstract

We give a recursive construction for projective Reed-Muller codes in terms of affine Reed-Muller codes and projective Reed-Muller codes in fewer variables. From this construction, we obtain the dimension of the subfield subcodes of projective Reed-Muller codes for some particular degrees that give codes with good parameters. Moreover, from this recursive construction we derive a lower bound for the generalized Hamming weights of projective Reed-Muller codes which is sharp in most of the cases we have checked.

Keywords: Projective Reed-Muller codes, recursive construction, subfield subcodes, generalized Hamming weights.

MSC: 94B05, 11T71, 14G50

DOI: 10.48550/arXiv.2312.05072

Reference: R. San-José. A recursive construction for projective Reed-Muller codes. ArXiv 2312.05072 (2023).

Paper E

Hulls of projective Reed-Muller codes over the projective plane

Diego Ruano, Rodrigo San-José

Abstract

By solving a problem regarding polynomials in a quotient ring, we obtain the relative hull and the Hermitian hull of projective Reed-Muller codes over the projective plane. The dimension of the hull determines the minimum number of maximally entangled pairs required for the corresponding entanglement-assisted quantum error-correcting code. Hence, by computing the dimension of the hull we now have all the parameters of the symmetric and asymmetric entanglement-assisted quantum error-correcting codes constructed with projective Reed-Muller codes over the projective plane. As a byproduct, we also compute the dimension of the Hermitian hull for affine Reed-Muller codes in 2 variables.

Keywords: Projective Reed-Muller codes, hull, entanglement-assisted quantum error-correcting codes, polynomial ring.

MSC: 81P70, 94B05, 13P25.

DOI: 10.48550/arXiv.2312.13921

Reference: D. Ruano, R. San-José. Hulls of projective Reed-Muller codes over the projective plane. SIAM Journal on Applied Algebra and Geometry, to appear (2024). ArXiv 2312.13921.

Paper F

Quantum error-correcting codes from projective Reed-Muller codes and their hull variation problem

Diego Ruano, Rodrigo San-José

Abstract

Long quantum codes using projective Reed-Muller codes are constructed. Projective Reed-Muller codes are evaluation codes obtained by evaluating homogeneous polynomials at the projective space. We obtain asymmetric and symmetric quantum codes by using the CSS construction and the Hermitian construction, respectively. We provide entanglement-assisted quantum error-correcting codes from projective Reed-Muller codes with flexible amounts of entanglement by considering equivalent codes. Moreover, we also construct quantum codes from subfield subcodes of projective Reed-Muller codes.

Keywords: Projective Reed-Muller codes, quantum codes, subfield subcodes, Hermitian product, hull.

MSC: 81P70, 94B05, 13P25.

DOI: 10.48550/arXiv.2312.15308

Reference: D. Ruano, R. San-José. Quantum error-correcting codes from projective Reed-Muller codes and their hull variation problem. ArXiv 2312.15308 (2024).

Paper G

An algebraic characterization of binary CSS-T codes and cyclic CSS-T codes for quantum fault tolerance

Eduardo Camps-Moreno, Hiram H. López, Gretchen L. Matthews, Diego Ruano, Rodrigo San-José, Ivan Soprunov

Abstract

CSS-T codes were recently introduced as quantum error-correcting codes that respect a transversal gate. A CSS-T code depends on a CSS-T pair, which is a pair of binary codes (C_1, C_2) such that C_1 contains C_2, C_2 is even, and the shortening of the dual of C_1 with respect to the support of each codeword of C_2 is self-dual. In this paper, we give new conditions to guarantee that a pair of binary codes (C_1, C_2) is a CSS-T pair. We define the poset of CSS-T pairs and determine the minimal and maximal elements of the poset. We provide a propagation rule for nondegenerate CSS-T codes. We apply some main results to Reed-Muller, cyclic, and extended cyclic codes. We characterize CSS-T pairs of cyclic codes in terms of the defining cyclotomic cosets. We find cyclic and extended cyclic codes to obtain quantum codes with better parameters than those in the literature.

Keywords: CSS-T construction, Schur product of linear codes, Cyclic codes, Quantum codes.

MSC: 94B05, 81P70, 11T71, 14G50.

DOI: 10.1007/s11128-024-04427-5

Reference: E. Camps-Moreno, H.H. López, G.L. Matthews, D. Ruano, R. San-José, I. Soprunov. An algebraic characterization of binary CSS-T codes and cyclic CSS-T codes for quantum fault tolerance. Quantum Inf. Process. 23, 230 (2024).

Paper H

About the generalized Hamming weights of matrix-product codes

Rodrigo San-José

Abstract

We derive a general lower bound for the generalized Hamming weights of nested matrix-product codes, with a particular emphasis on the cases with two and three constituent codes. We also provide an upper bound which is reminiscent of the bounds used for the minimum distance of matrix-product codes. When the constituent codes are two Reed-Solomon codes, we obtain an explicit formula for the generalized Hamming weights of the resulting matrix-product code. We also deal with the non-nested case for the case of two constituent codes.

Keywords: Linear codes, Matrix-product codes, Generalized Hamming weights, Reed-Solomon codes.

MSC: 94B05, 94B65, 11T71.

DOI: 10.48550/arXiv.2407.11810

Reference: R. San-José. About the generalized Hamming weights of matrix-product codes. ArXiv 2407.11810 (2024).

Part III

Conclusion

Conclusion

In this thesis we have studied several interactions between Commutative Algebra and Coding Theory, with an emphasis in applications. In particular, we have studied how to compute the homogeneous vanishing ideal of any finite set of points of the projective space using the saturation in Paper A. The same can be achieved by saturating with respect to the ideal generated by a polynomial that does not vanish at any of the points considered. Therefore, it would be interesting to study which polynomials do not vanish at some particular sets of points for computing the corresponding vanishing ideal.

We have also studied the vanishing ideal of the set of fixed representatives of a set of projective points in Papers B and C. By obtaining Gröbner bases of these ideals, we have obtained bases for the subfield subcodes of projective Reed-Solomon codes and projective Reed-Muller codes, which have been used to construct EAQECCs with good parameters. Using these Gröbner bases, we obtain the hulls of projective Reed-Muller codes over the projective plane in Paper F. This Gröbner basis approach may be used in the future to study other aspects of projective Reed-Muller codes, such as their weight distribution, which has been an extensive object of study for the affine case.

A different approach to study projective Reed-Muller codes is given in Paper D, where a recursive construction is given. With this construction, we also obtain bases for the subfield subcodes of projective Reed-Muller codes for some particular degrees. Moreover, this recursive construction also provides bounds for the GHWs of projective Reed-Muller codes, allowing the exact determination thereof in many examples. Such recursive constructions have been used for the affine case to obtain decoding algorithms and results about their weight distribution. Moreover, another topic of future research is to investigate whether similar constructions can be obtained for similar families of codes, such as nested projective Cartesian codes [27].

Another topic covered by this thesis are the hulls of projective Reed-Muller codes, which have been determined for the case of the projective plane in Paper E. Furthermore, in Paper F we have also explored ways to change the dimension of the hull by using monomially equivalent codes, giving rise to EAQECCs with flexible amounts of entanglement. As before, a future research agenda would be to study if this computations can be carried out for other families of codes.

As we have mentioned in the previous paragraphs, one of the main contributions of this thesis is to fill some of the gaps in knowledge between affine and projective Reed-Muller codes, in particular with respect to their subfield subcodes, hulls and generalized Hamming weights. Nevertheless, some of these topics are still wide open, such as the determination of the hulls for arbitrary projective Reed-Muller codes, and the exact determination of their generalized Hamming weights.

In Paper H we have given lower and upper bounds for the GHWs of MPCs, focusing on the cases with two and three constituent codes. As an application of these bounds, we get the exact value of the GHWs of the MPCs obtained by using two Reed-Solomon codes. The techniques used are inspired by the ones considered with the recursive construction from Paper D for projective Reed-Muller codes. Some of these techniques can be generalized to obtain bounds for the relative generalized Hamming weights of matrix-product codes, which could have applications for secret sharing schemes and quantum codes.

Finally, with respect to quantum fault-tolerant computing, we have given a manageable characterization of CSS-T quantum codes in Paper G. With this new view on CSS-T codes, we have obtained a propagation rule and we have determined the pairs of cyclic codes that give rise to CSS-T codes. This opens the path to considering other families of binary codes to construct CSS-T codes. A more ambitious project would be to obtain similar conditions for a certain non-Clifford operator (analogous to the T gate) in the p-ary case (instead of binary). This would greatly increase the families of classical codes we can consider to construct codes suitable for fault-tolerant computing, which in turn may give better parameters. Triorthogonal codes are a particular case of CSS-T codes which has aroused a lot of attention recently. Finding alternative characterizations for these codes, and obtaining new constructions using cyclic codes (or subfield subcodes of evaluation codes) is also a natural future research project.

Global bibliography

[1] J. Abbott, A. M. Bigatti, and L. Robbiano. CoCoA: a system for doing Computations in Commutative Algebra. Available at `http://cocoa.dima.unige.it`.

[2] J. T. Anderson, G. Duclos-Cianci, and D. Poulin. Fault-tolerant conversion between the Steane and Reed-Muller quantum codes. *Phys. Rev. Lett.*, 113:080501, Aug 2014.

[3] S. E. Anderson, E. Camps-Moreno, H. H. López, G. L. Matthews, D. Ruano, and I. Soprunov. Relative hulls and quantum codes. *IEEE Trans. Inform. Theory*, 70(5):3190–3201, 2024.

[4] E. Andrade, J. Bolkema, T. Dexter, H. Eggers, V. Luongo, F. Manganiello, and L. Szramowski. CSS-T codes from Reed Muller codes for quantum fault tolerance. *ArXiv 2305.06423*, 2023.

[5] S. Ball. Some constructions of quantum MDS codes. *Des. Codes Cryptogr.*, 89(5):811–821, 2021.

[6] T. Ball, E. Camps, H. Chimal-Dzul, D. Jaramillo-Velez, H. López, N. Nichols, M. Perkins, I. Soprunov, G. Vera-Martínez, and G. Whieldon. Coding theory package for Macaulay2. *J. Softw. Algebra Geom.*, 11(1):113–122, 2021.

[7] A. I. Barbero and C. Munuera. The weight hierarchy of Hermitian codes. *SIAM J. Discrete Math.*, 13(1):79–104, 2000.

[8] P. Beelen and M. Datta. Generalized Hamming weights of affine Cartesian codes. *Finite Fields Appl.*, 51:130–145, 2018.

[9] P. Beelen, M. Datta, and S. R. Ghorpade. Maximum number of common zeros of homogeneous polynomials over finite fields. *Proc. Amer. Math. Soc.*, 146(4):1451–1468, 2018.

[10] P. Beelen, M. Datta, and S. R. Ghorpade. Vanishing ideals of projective spaces over finite fields and a projective footprint bound. *Acta Math. Sin. (Engl. Ser.)*, 35(1):47–63, 2019.

[11] P. Beelen, M. Datta, and S. R. Ghorpade. A combinatorial approach to the number of solutions of systems of homogeneous polynomial equations over finite fields. *Mosc. Math. J.*, 22(4):565–593, 2022.

[12] E. Berardini, A. Caminata, and A. Ravagnani. Structure of CSS and CSS-T quantum codes. *Des. Codes Cryptogr.*, 2024.

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

[14] J. Bierbrauer and Y. Edel. New code parameters from Reed-Solomon subfield codes. *IEEE Trans. Inform. Theory*, 43(3):953–968, 1997.

[15] J. Bierbrauer and Y. Edel. Quantum twisted codes. *J. Combin. Des.*, 8(3):174–188, 2000.

[16] T. Blackmore and G. H. Norton. Matrix-product codes over $\mathbb{F}_q$. *Appl. Algebra Engrg. Comm. Comput.*, 12(6):477–500, 2001.

[17] M. Boguslavsky. On the number of solutions of polynomial systems. *Finite Fields Appl.*, 3(4):287–299, 1997.

[18] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[19] S. Bravyi and J. Haah. Magic-state distillation with low overhead. *Phys. Rev. A*, 86:052329, Nov 2012.

[20] S. Bravyi and A. Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A (3)*, 71(2):022316, 14, 2005.

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

[22] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.

[23] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

[24] E. Camps-Moreno, I. García-Marco, H. H. López, I. Márquez-Corbella, E. Martínez-Moro, and E. Sarmiento. On the generalized Hamming weights of hyperbolic codes. *J. Algebra Appl.*, 23(7):Paper No. 2550062, 18, 2024.

[25] E. Camps-Moreno, H. H. López, G. L. Matthews, D. Ruano, R. San-José, and I. Soprunov. An algebraic characterization of binary CSS-T codes and cyclic CSS-T codes for quantum fault tolerance. *Quantum Inf. Process.*, 23(230), 2024.

[26] E. Camps-Moreno, H. H. López, G. L. Matthews, D. Ruano, R. San-José, and I. Soprunov. Parity check matrices for the codes in "An algebraic characterization of binary CSS-T codes and cyclic CSS-T codes for quantum fault tolerance". GitHub repository. Available online: `https://github.com/RodrigoSanJose/Cyclic-CSS-T`, 2024. Accessed on 18 April 2024.

[27] C. Carvalho, V. G. L. Neumann, and H. H. López. Projective nested cartesian codes. *Bull. Braz. Math. Soc. (N.S.)*, 48(2):283–302, 2017.

[28] C. Carvalho, X. Ramírez-Mondragón, V. G. L. Neumann, and H. Tapia-Recillas. Projective Reed-Muller type codes on higher dimensional scrolls. *Des. Codes Cryptogr.*, 87(9):2027–2042, 2019.

[29] I. Cascudo. On squares of cyclic codes. *IEEE Trans. Inform. Theory*, 65(2):1034–1047, 2019.

[30] I. Cascudo, J. S. Gundersen, and D. Ruano. Squares of matrix-product codes. *Finite Fields Appl.*, 62:101606, 21, 2020.

[31] H. Chen. On the hull-variation problem of equivalent linear codes. *IEEE Trans. Inform. Theory*, 69(5):2911–2922, 2023.

[32] S. D. Cohen. Primitive elements and polynomials with arbitrary trace. *Discrete Math.*, 83(1):1–7, 1990.

[33] S. M. Cooper, A. Seceleanu, Ş. O. Tohăneanu, M. V. Pinto, and R. H. Villarreal. Generalized minimum distance functions and algebraic invariants of Geramita ideals. *Adv. in Appl. Math.*, 112:101940, 34, 2020.

[34] D. A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.

[35] S. X. Cui, D. Gottesman, and A. Krishna. Diagonal gates in the Clifford hierarchy. *Phys. Rev. A*, 95(1):012329, 7, 2017.

[36] M. Datta and S. R. Ghorpade. Number of solutions of systems of homogeneous polynomial equations over finite fields. *Proc. Amer. Math. Soc.*, 145(2):525–541, 2017.

[37] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 4-4-0 — A computer algebra system for polynomial computations. `http://www.singular.uni-kl.de`, 2024.

[38] P. Delsarte. On subfield subcodes of modified Reed-Solomon codes. *IEEE Trans. Inform. Theory*, IT-21(5):575–576, 1975.

[39] P. Delsarte, J.-M. Goethals, and F. J. MacWilliams. On generalized Reed-Muller codes and their relatives. *Information and Control*, 16:403–442, 1970.

[40] I. M. Duursma, C. Rentería, and H. Tapia-Recillas. Reed-Muller codes on complete intersections. *Appl. Algebra Engrg. Comm. Comput.*, 11(6):455–462, 2001.

[41] B. Eastin and E. Knill. Restrictions on transversal encoded quantum gate sets. *Phys. Rev. Lett.*, 102:110502, Mar 2009.

[42] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[43] B. Engheta. On the projective dimension and the unmixed part of three cubics. *J. Algebra*, 316(2):715–734, 2007.

[44] K. Feng and Z. Ma. A finite Gilbert-Varshamov bound for pure stabilizer quantum codes. *IEEE Trans. Inform. Theory*, 50(12):3323–3325, 2004.

[45] C. Galindo, O. Geil, F. Hernando, and D. Ruano. On the distance of stabilizer quantum codes from J-affine variety codes. *Quantum Inf. Process.*, 16(4):Paper No. 111, 32, 2017.

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

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

[48] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano. Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. *Quantum Inf. Process.*, 18(4):Paper No. 116, 18, 2019.

[49] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano. Asymmetric entanglement-assisted quantum error-correcting codes and bch codes. *IEEE Access*, 8:18571–18579, 2020.

[50] C. Galindo, F. Hernando, C. Munuera, and D. Ruano. Locally recoverable codes from the matrix-product construction. *ArXiv 2310.15703*, 2023.

[51] C. Galindo, F. Hernando, and D. Ruano. New quantum codes from evaluation and matrix-product codes. *Finite Fields Appl.*, 36:98–120, 2015.

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

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

[54] C. Galindo, F. Hernando, and D. Ruano. Entanglement-assisted quantum error-correcting codes from RS codes and BCH codes with extension degree 2. *Quantum Inf. Process.*, 20(5):Paper No. 158, 26, 2021.

[55] S. R. Ghorpade. A note on Nullstellensatz over finite fields. In *Contributions in algebra and algebraic geometry*, volume 738 of *Contemp. Math.*, pages 23–32. Amer. Math. Soc., 2019.

[56] S. R. Ghorpade and R. Ludhani. On the minimum distance, minimum weight codewords, and the dimension of projective Reed-Muller codes. *Adv. Math. Commun.*, 18(2):360–382, 2024.

[57] P. Gimenez, D. Ruano, and R. San-José. Entanglement-assisted quantum error-correcting codes from subfield subcodes of projective Reed-Solomon codes. *Comput. Appl. Math.*, 42(8):Paper No. 363, 31, 2023.

[58] P. Gimenez, D. Ruano, and R. San-José. Saturation and vanishing ideals. *São Paulo J. Math. Sci.*, 17(1):147–155, 2023.

[59] P. Gimenez, D. Ruano, and R. San-José. Subfield subcodes of projective Reed-Muller codes. *Finite Fields Appl.*, 94:Paper No. 102353, 46, 2024.

[60] M. González-Sarabia, J. Martínez-Bernal, R. H. Villarreal, and C. E. Vivares. Generalized minimum distance functions. *J. Algebraic Combin.*, 50(3):317–346, 2019.

[61] M. González-Sarabia and C. Rentería. The dual code of some Reed-Muller type codes. *Appl. Algebra Engrg. Comm. Comput.*, 14(5):329–333, 2004.

[62] P. Gopalan, V. Guruswami, and P. Raghavendra. List decoding tensor products and interleaved codes. *SIAM J. Comput.*, 40(5):1432–1462, 2011.

[63] D. Gottesman. The Heisenberg representation of quantum computers. In *Group22: Proceedings of the XXII International Colloquium in Group Theoretical Methods in Physics (Hobart, 1998)*, pages 32–43. Int. Press, Cambridge, MA, 1999.

[64] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007. Accessed on 2023-04-04.

[65] M. Grassl. Algebraic quantum codes: linking quantum mechanics and discrete mathematics. *International Journal of Computer Mathematics: Computer Systems Theory*, 6(4):243–259, 2021.

[66] M. Grassl. New quantum codes from CSS codes. *Quantum Inf. Process.*, 22(1):Paper No. 86, 11, 2023.

[67] D. R. Grayson and M. E. Stillman. Macaulay2, a software system for research in algebraic geometry.

[68] G.-M. Greuel and G. Pfister. *A* **Singular** *introduction to commutative algebra*. Springer, Berlin, extended edition, 2008. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann.

[69] V. Guruswami. List decoding from erasures: bounds and code constructions. *IEEE Trans. Inform. Theory*, 49(11):2826–2833, 2003.

[70] M. B. Hastings and J. Haah. Distillation with sublogarithmic overhead. *Phys. Rev. Lett.*, 120:050504, Jan 2018.

[71] M. Hattori, R. J. McEliece, and G. Solomon. Subspace subcodes of Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 44(5):1861–1880, 1998.

[72] P. Heijnen and R. Pellikaan. Generalized Hamming weights of q-ary Reed-Muller codes. *IEEE Trans. Inform. Theory*, 44(1):181–196, 1998.

[73] F. Hernando, T. Høholdt, and D. Ruano. List decoding of matrix-product codes from nested codes: an application to quasi-cyclic codes. *Adv. Math. Commun.*, 6(3):259–272, 2012.

[74] F. Hernando, K. Lally, and D. Ruano. Construction and decoding of matrix-product codes from nested codes. *Appl. Algebra Engrg. Comm. Comput.*, 20(5-6):497–507, 2009.

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

[76] F. Hernando, M. E. O'Sullivan, E. Popovici, and S. Srivastava. Subfield-subcodes of generalized toric codes. In *2010 IEEE International Symposium on Information Theory*, pages 1125–1129, 2010.

[77] F. Hernando and D. Ruano. Decoding of matrix-product codes. *J. Algebra Appl.*, 12(4):1250185, 15, 2013.

[78] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[79] L. Ioffe and M. Mézard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75:032345, Mar 2007.

[80] D. Jaramillo, M. Vaz Pinto, and R. H. Villarreal. Evaluation codes and their basic parameters. *Des. Codes Cryptogr.*, 89(2):269–300, 2021.

[81] S. Jitman and T. Mankean. Matrix-product constructions for Hermitian self-orthogonal codes. *Chamchuri J. Math.*, 9:35–51, 2017.

[82] N. Kaplan and J.-L. Kim. Hulls of Projective Reed-Muller Codes. *ArXiv 2406.04757*, 2024.

[83] T. Kasami, S. Lin, and W. W. Peterson. New generalizations of the Reed-Muller codes. I. Primitive codes. *IEEE Trans. Inform. Theory*, IT-14:189–199, 1968.

[84] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, 2006.

[85] M. Kreuzer and L. Robbiano. *Computational commutative algebra. 1.* Springer-Verlag, Berlin, 2000.

[86] M. Kreuzer and L. Robbiano. *Computational commutative algebra. 2.* Springer-Verlag, Berlin, 2005.

[87] G. G. La Guardia. *Quantum error correction—symmetric, asymmetric, synchronizable, and convolutional codes*. Quantum Science and Technology. Springer, Cham, 2020.

[88] G. Lachaud. Projective Reed-Muller codes. In *Coding theory and applications (Cachan, 1986)*, volume 311 of *Lecture Notes in Comput. Sci.*, pages 125–129. Springer, Berlin, 1988.

[89] G. Lachaud. The parameters of projective Reed-Muller codes. *Discrete Math.*, 81(2):217–221, 1990.

[90] H. H. López, I. Soprunov, and R. H. Villarreal. The dual of an evaluation code. *Des. Codes Cryptogr.*, 89(7):1367–1403, 2021.

[91] G. Luo, M. F. Ezerman, M. Grassl, and S. Ling. Constructing quantum error-correcting codes that require a variable amount of entanglement. *Quantum Inf. Process.*, 23(1):Paper No. 4, 28, 2024.

[92] G. Luo, M. F. Ezerman, and S. Ling. Three new constructions of optimal locally repairable codes from matrix-product codes. *IEEE Trans. Inform. Theory*, 69(1):75–85, 2023.

[93] G. Luo, M. F. Ezerman, S. Ling, and X. Pan. New families of MDS symbol-pair codes from matrix-product codes. *IEEE Trans. Inform. Theory*, 69(3):1567–1587, 2023.

[94] J. MacWilliams. Error-correcting codes for multiple-level transmission. *Bell System Tech. J.*, 40:281–308, 1961.

[95] T. Mankean and S. Jitman. Matrix-product constructions for self-orthogonal linear codes. In *2016 12th International Conference on Mathematics, Statistics, and Their Applications (ICMSA)*, pages 6–10, 2016.

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

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

[98] R. Matsumoto. Improved Gilbert–Varshamov bound for Entanglement-Assisted Asymmetric Quantum Error Correction by Symplectic Orthogonality. *IEEE Trans. Quantum Eng.*, 1:1–4, 2020.

[99] D.-J. Mercier and R. Rolland. Polynômes homogènes qui s'annulent sur l'espace projectif $\mathrm{P}^m(\mathbf{F}_q)$. *J. Pure Appl. Algebra*, 124(1-3):227–240, 1998.

[100] C. Munuera. On the generalized Hamming weights of geometric Goppa codes. *IEEE Trans. Inform. Theory*, 40(6):2092–2099, 1994.

[101] N. Nakashima and H. Matsui. Decoding of projective reed-muller codes by dividing a projective space into affine spaces. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E99.A(3):733–741, 2016.

[102] L. P. Natarajan and P. Krishnan. Berman codes: a generalization of Reed-Muller codes that achieve BEC capacity. *IEEE Trans. Inform. Theory*, 69(11):6956–6980, 2023.

[103] G. Nebe, E. M. Rains, and N. J. A. Sloane. The invariants of the Clifford groups. *Des. Codes Cryptogr.*, 24(1):99–121, 2001.

[104] G. Nebe, E. M. Rains, and N. J. A. Sloane. *Self-dual codes and invariant theory*, volume 17 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006.

[105] S. Nezami and J. Haah. Classification of small triorthogonal codes. *Phys. Rev. A*, 106(1):Paper No. 012437, 13, 2022.

[106] F. Özbudak and H. Stichtenoth. Note on Niederreiter-Xing's propagation rule for linear codes. *Appl. Algebra Engrg. Comm. Comput.*, 13(1):53–56, 2002.

[107] R. Pellikaan, X.-W. Wu, S. Bulygin, and R. Jurrius. *Codes, cryptology and curves with computer algebra*. Cambridge University Press, Cambridge, 2018.

[108] D.-X. Quan, L.-L. Zhu, C.-X. Pei, and B. C. Sanders. Fault-tolerant conversion between adjacent Reed-Muller quantum codes based on gauge fixing. *J. Phys. A*, 51(11):115305, 16, 2018.

[109] E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45(6):1827–1832, 1999.

[110] H. Randriambololona. On products and powers of linear codes under componentwise multiplication. In *Algorithmic arithmetic, geometry, and coding theory*, volume 637 of *Contemp. Math.*, pages 3–78. Amer. Math. Soc., Providence, RI, 2015.

[111] N. Rengaswamy, R. Calderbank, M. Newman, and H. D. Pfister. Classical coding problem from transversal T gates. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 1891–1896, 2020.

[112] N. Rengaswamy, R. Calderbank, M. Newman, and H. D. Pfister. On optimality of CSS codes for transversal T. *IEEE J. Sel. Areas Inf. Theory*, 1(2):499–514, 2020.

[113] C. Rentería and H. Tapia-Recillas. Reed-Muller codes: an ideal theory approach. *Comm. Algebra*, 25(2):401–413, 1997.

[114] C. Rentería-Márquez, A. Simis, and R. H. Villarreal. Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields. *Finite Fields Appl.*, 17(1):81–104, 2011.

[115] D. Ruano and R. San-José. Hulls of projective Reed-Muller codes over the projective plane. *ArXiv 2312.13921*, 2023.

[116] D. Ruano and R. San-José. Quantum error-correcting codes from projective Reed-Muller codes and their hull variation problem. *ArXiv 2312.15308*, 2024.

[117] R. San-José. A recursive construction for projective Reed-Muller codes. *ArXiv 2312.05072*, 2023.

[118] R. San-José. About the generalized Hamming weights of matrix-product codes. *ArXiv 2407.11810*, 2024.

[119] P. Sarvepalli and A. Klappenecker. Nonbinary quantum reed-muller codes. In *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, pages 1023–1027, 2005.

[120] P. K. Sarvepalli, S. A. Aly, and A. Klappenecker. Nonbinary stabilizer codes. In *Mathematics of quantum computation and quantum technology*, Chapman & Hall/CRC Appl. Math. Nonlinear Sci. Ser., pages 287–308. Chapman & Hall/CRC, Boca Raton, FL, 2008.

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

[122] P. Shor. Fault-tolerant quantum computation. In *Proceedings of 37th Conference on Foundations of Computer Science*, pages 56–65, 1996.

[123] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, Oct 1995.

[124] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[125] A. B. Sørensen. Projective Reed-Muller codes. *IEEE Trans. Inform. Theory*, 37(6):1567–1576, 1991.

[126] A. B. Sørensen. A note on a gap in the proof of the minimum distance for projective Reed-Muller codes. *ArXiv 2310.03574*, 2023.

[127] A. Steane. Multiple-Particle Interference and Quantum Error Correction. *Proceedings of the Royal Society of London Series A*, 452(1954):2551–2577, Nov. 1996.

[128] A. M. Steane. Simple quantum error-correcting codes. *Phys. Rev. A (3)*, 54(6):4741–4751, 1996.

[129] A. M. Steane. Quantum Reed-Muller codes. *IEEE Trans. Inform. Theory*, 45(5):1701–1703, 1999.

[130] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.3)*, 2023. `https://www.sagemath.org`.

[131] Ş. O. Tohăneanu. *Commutative Algebra Methods for Coding Theory*. De Gruyter, Berlin, Boston, 2024.

[132] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.