About weighted projective Reed-Muller codes

Jade Nardi

Arithmetic, **G**eometry, **C**ryptography and **C**oding **T**heory conference
June 10, 2025

Joint works with Yağmur Çakıroğlu[⋆], Rodrigo San-José[⋄] and Mesut Şahin[⋆]
[⋆] Hacettepe University, Ankara, Turkey
[⋄] IMUVA-Mathematics Research Institute, Universidad de Valladolid, Spain

Picture: Neighbourhood *Le Panier* in Marseille

Weighted Projective Space

Definition

The *weighted projective space* over $\mathbb{K}(=\overline{\mathbb{F}}_q)$ with weights $w = (w_0, \dots, w_m) \in \mathbb{N}_{\geqslant 1}^{m+1}$ is the quotient

$$\mathbb{P}(w_0, \dots, w_m) = (\mathbb{K}^{m+1} \backslash \{0\})/\sim$$

under the action of $\mathbb{K}^*$ defined by $\lambda \cdot (x_0, \dots, x_m) = (\lambda^{w_0} x_0, \dots, \lambda^{w_r} x_m)$ for $\lambda \in \mathbb{K}^*$.

Example

$\mathbb{P}(1, 1, \dots, 1)$ is the classical projective space $\mathbb{P}^m$.

Weighted Projective Space

Definition

The *weighted projective space* over $\mathbb{K}(=\overline{\mathbb{F}}_q)$ with weights $w=(w_0,\dots,w_m)\in\mathbb{N}_{\geqslant 1}^{m+1}$ is the quotient

$$\mathbb{P}(w_0,\dots,w_m)=(\mathbb{K}^{m+1}\backslash\{0\})/\sim$$

under the action of $\mathbb{K}^*$ defined by $\lambda\cdot(x_0,\dots,x_m)=(\lambda^{w_0}x_0,\dots,\lambda^{w_r}x_m)$ for $\lambda\in\mathbb{K}^*$.

Example

$\mathbb{P}(1,1,\dots,1)$ is the classical projective space $\mathbb{P}^m$.

Proposition: Isomorphisms of weighted projective spaces

$\mathbb{P}(cw_0,cw_1,\dots,cw_m)\simeq\mathbb{P}(w_0,w_1,\dots,w_m)$ $\mathbb{P}(w_0,cw_1,\dots,cw_m)\simeq\mathbb{P}(w_0,w_1,\dots,w_m)$.

Delorme

Example (Delorme's reduction)

$\mathbb{P}(w_0,w_1)\simeq\mathbb{P}(w_0,1)\simeq\mathbb{P}(1,1)=\mathbb{P}^1$. $\mathbb{P}(1,w_1,w_2)\simeq\mathbb{P}(1,w_1',w_2')$ with $\gcd(w_1',w_2')=1$.

W.l.o.g. $w=(w_0,\dots,w_m)$ is well-formed: $\gcd(w)=1$ and $\gcd(w_0,\dots,\widehat{w}_i,\dots,w_m)=1$ $\forall i$.

(Rational) points of weighted projective spaces over $\mathbb{K} = \overline{\mathbb{F}_q}$

Recall: $(x_0, \dots, x_m) \sim \lambda \cdot (x_0, \dots, x_m) = (\lambda^{w_0} x_0, \dots, \lambda^{w_r} x_m)$ for $\lambda \in \mathbb{K}^*$

A point P in $\mathbb{P}(w_0, \dots, w_m)$ is an equivalence class $[x_0 : \dots : x_m]$ for $\sim$.
A point $P = [x_0 : \dots : x_m] \in \mathbb{P}(w_0, \dots, w_m)$ is $\mathbb{F}_q$-rational if $(x_0^q, \dots, x_m^q) \sim (x_0, \dots, x_m)$. We write $\mathbb{P}(w_0, \dots, w_m)(\mathbb{F}_q)$ for the set of $\mathbb{F}_q$-rational points.

Theorem [Per03]

An $\mathbb{F}_q$-rational point $P \in \mathbb{P}(w_0, \dots, w_m)(\mathbb{F}_q)$ admits $q - 1$ representatives in $\mathbb{F}_q^{m+1}$.

(Rational) points of weighted projective spaces over $\mathbb{K} = \overline{\mathbb{F}_q}$

Recall: $(x_0,\dots,x_m)\sim\lambda\cdot(x_0,\dots,x_m) = (\lambda^{w_0}x_0,\dots,\lambda^{w_r}x_m)$ for $\lambda\in\mathbb{K}^*$

A point P in $\mathbb{P}(w_0,\dots,w_m)$ is an equivalence class $[x_0:\cdots:x_m]$ for $\sim$.
A point $P=[x_0:\cdots:x_m]\in\mathbb{P}(w_0,\dots,w_m)$ is $\mathbb{F}_q$-rational if $(x_0^q,\dots,x_m^q)\sim(x_0,\dots,x_m)$. We write $\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$ for the set of $\mathbb{F}_q$-rational points.

Theorem [Per03]

An $\mathbb{F}_q$-rational point $P\in\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$ admits $q-1$ representatives in $\mathbb{F}_q^{m+1}$.

For $\mathbb{P}(1,\dots,1)=\mathbb{P}^m$, we choose the representatives of $\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$ as follows:

$$\underbrace{(1,x_1,\dots,x_m)}_{q^m},\ \underbrace{(0,1,x_2,\dots,x_m)}_{+q^{m-1}},\ \underbrace{\dots}_{+\dots},\ \underbrace{(0,\dots,0,1)}_{+1} \text{ with } x_i\in\mathbb{F}_q.$$

For $\mathbb{P}(w_0,\dots,w_m)$, we can do the same if $\gcd(q-1,w_i)=1$ for every $i\in\{0,\dots,m-1\}$.

Example

In $\mathbb{P}(1,2,3)$ over $\mathbb{F}_3$, $2\cdot(0,1,1)=(0,2^2,2^3)=(0,1,2)$. So $(0,1,1)\sim(0,1,2)$.
⚠ Not every rational point of the line $x_0=0$ can be represented by a triple of the form $(0,1,x_2)$.

Why you may be interested in weighted projective spaces: a non-exhaustive list

- WPS are examples of **toric varieties**.
- WPS have **finite quotient singularities**.
- **Classification of surfaces:** Any surface with $K^2 = 1$ is a weighted complete intersection of type $(6, 6)$ in $\mathbb{P}(1, 2, 2, 3, 3)$. Catanese (1970)
- **Invariants and moduli spaces:**
  - The moduli spaces of elliptic curves up to isomorphism over $\mathbb{K}$ (with $char(\mathbb{K}) \notin \{2, 3\}$) is

$$\mathcal{M}_{1,1} = \left\{(a : b : \Delta) : \Delta = -16(4a^3 + 27b^2)\right\} \subset \underbrace{\mathbb{P}(2, 3, 6)}_{\simeq \mathbb{P}(1,2,3)}.$$

  - Genus-2 curves up to isomorphism over $\mathbb{K}$ (with $char(\mathbb{K}) \neq 2$) can be characterized by Igusa invariants $(J_2, J_4, J_6, J_{10}) \in \underbrace{\mathbb{P}(2, 4, 6, 10)}_{\simeq \mathbb{P}(1,2,3,5)}$ with $J_{10} \neq 0$.

Weighted Projective Reed-Muller code

A *linear code* C over $\mathbb{F}_q$ of length n is a vector subspace $\mathbb{F}_q^n$. We note k its dimension.
The weight of a word $x \in \mathbb{F}_q^n$ is given by $\mathrm{wt}(x) = \#\{i \in \{1, \dots, n\}, x_i \neq 0\}$.
The minimum distance of C is defined by $d = \min\{\mathrm{wt}(c) \mid c \in C, c \neq 0\}$.

Weighted Projective Reed-Muller code

A *linear code* C over $\mathbb{F}_q$ of length n is a vector subspace $\mathbb{F}_q^n$. We note k its dimension.
The weight of a word $x \in \mathbb{F}_q^n$ is given by $\mathrm{wt}(x) = \#\{i \in \{1, \ldots, n\}, x_i \neq 0\}$.
The minimum distance of C is defined by $d = \min\{\mathrm{wt}(c) \mid c \in C, c \neq 0\}$.

Fix $w = (w_0, \ldots, w_m) \in \mathbb{N}_{\geqslant 1}^{m+1}$.
The ring $S = \mathbb{F}_q[x_0, \ldots, x_m]$ is graded by $\deg_w \left(\prod_{i=0}^m x_i^{a_i}\right) = a_0 w_0 + \cdots + a_m w_m$.
Then $S = \bigoplus_{d \geqslant 0} S_d$ where $S_d = \mathrm{Span}\left\{M = \prod_{i=0}^m x_i^{a_i} : \deg_w(M) = d\right\}$.

Definition: Denumerant

For $d \in \mathbb{N}$, we define the denumerant of d w.r.t. to w as

$$\mathrm{den}(d; w) = \#\left\{(a_0, \ldots, a_m) \in \mathbb{N}^{m+1} : w_0 a_0 + \cdots + w_m a_m = d\right\}.$$

$\Rightarrow \dim S_d = \mathrm{den}(d; w)$

Weighted Projective Reed-Muller code

A *linear code* C over $\mathbb{F}_q$ of length n is a vector subspace $\mathbb{F}_q^n$. We note k its dimension.
The weight of a word $x \in \mathbb{F}_q^n$ is given by $\mathrm{wt}(x) = \#\{i \in \{1,\dots,n\},\ x_i \neq 0\}$.
The minimum distance of C is defined by $d = \min\{\mathrm{wt}(c) \mid c \in C,\ c \neq 0\}$.

Fix $w = (w_0,\dots,w_m) \in \mathbb{N}_{\geqslant 1}^{m+1}$.
The ring $S = \mathbb{F}_q[x_0,\dots,x_m]$ is graded by $\deg_w\left(\prod_{i=0}^m x_i^{a_i}\right) = a_0 w_0 + \cdots + a_m w_m$.
Then $S = \bigoplus_{d\geqslant 0} S_d$ where $S_d = \mathrm{Span}\left\{M = \prod_{i=0}^m x_i^{a_i} : \deg_w(M) = d\right\}$.

Definition: Denumerant

For $d \in \mathbb{N}$, we define the denumerant of d w.r.t. to w as

$$\mathrm{den}(d; w) = \#\left\{(a_0,\dots,a_m) \in \mathbb{N}^{m+1} : w_0 a_0 + \cdots + w_m a_m = d\right\}.$$

$\Rightarrow \dim S_d = \mathrm{den}(d; w)$

Definition: Weighted Projective Reed-Muller (WPRM) code of w-degree d

Set $\{P_1,\dots,P_n\} = \mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$ and define $ev_d : \left\{\begin{array}{ccc} S_d & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1),\dots,f(P_n)) \end{array}\right.$

The weighted projective Reed-Muller code of w-degree d $\mathrm{WPRM}_d(w)$ is the image of ev_d.

Evaluating a polynomial at a point of $\mathbb{P}(w_0, \ldots, w_m)$

Recall: $\mathrm{WPRM}_d(w) = \{(f(P_1), \ldots, f(P_n)) : f \in S_d\}$ with $\{P_1, \ldots, P_n\} = \mathbb{P}(w_0, \ldots, w_m)(\mathbb{F}_q)$.

Fix $f \in S_d \subset \mathbb{F}_q[x_0, \ldots, x_m]$ and $P \in \mathbb{P}(w_0, \ldots, w_m)(\mathbb{F}_q)$.
To evaluate f at P, choose an $\mathbb{F}_q$-representative $\mathrm{x}_P = (x_0, \ldots, x_m) \in \mathbb{F}_q^{m+1}$ of P and define $f(P) = f(x_0, \ldots, x_m)$.

What happens if you choose another representative?

Evaluating a polynomial at a point of $\mathbb{P}(w_0,\dots,w_m)$

Recall: $\mathrm{WPRM}_d(w) = \{(f(P_1),\dots,f(P_n)) : f \in S_d\}$ with $\{P_1,\dots,P_n\} = \mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$.

Fix $f \in S_d \subset \mathbb{F}_q[x_0,\dots,x_m]$ and $P \in \mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$.
To evaluate f at P, choose an $\mathbb{F}_q$-representative $\mathrm{x}_P = (x_0,\dots,x_m) \in \mathbb{F}_q^{m+1}$ of P and define $f(P) = f(x_0,\dots,x_m)$.

What happens if you choose another representative?

As $f \in S_d$ is weighted homogeneous, $f(\lambda^{w_0}x_0,\dots,\lambda^{w_m}x_m) = \lambda^d f(x_0,\dots,x_m)$.
Given two sets of representatives $\{\mathrm{x}_P\}$ and $\{\mathrm{y}_P\}$ of $\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$,
(so that $y_P = \lambda_P \cdot x_P$ for some $\lambda_P \neq 0$)

$$(f(y_{P_1}),\dots,f(y_{P_n})) = \begin{pmatrix} \lambda_{P_1}^d & & \\ & \ddots & \\ & & \lambda_{P_n}^d \end{pmatrix} (f(x_{P_1}),\dots,f(x_{P_n}))$$

$$\Rightarrow \mathrm{wt}\left((f(y_{P_1}),\dots,f(y_{P_n}))\right) = \mathrm{wt}\left((f(x_{P_1}),\dots,f(x_{P_n}))\right).$$

☺ The parameters of the code $\mathrm{WPRM}_d(w)$ do not depend on the choice of representatives.

Literature on Reed-Muller type codes

- Projective Reed-Muller codes $(w = (1, \dots, 1))$ were introduced by Lachaud [Lac88] and comprehensively studied by Sørensen [Sør92].
- San-José [SJ24] provided a recursive construction for projective Reed-Muller codes.
- Aubry, et al. [ACG+17] gave the parameters of $\mathrm{WPRM}_d(1, w_1, w_2)$ and $w_1 w_2 \mid d \leqslant q$.
- Çakıroğlu and Sahin [ÇȘ25] gave the parameters of $\mathrm{WPRM}_d(1, 1, w_2)$ and $d < q w_2$.
- Aubry and Perret [AP24] gave the minimum distance for $w = (1, w_1, w_2, \dots, w_m)$ for $\mathrm{lcm}(w) \mid d \leqslant w_1 q$.

Literature on Reed-Muller type codes

- Projective Reed-Muller codes $(w = (1, \ldots, 1))$ were introduced by Lachaud [Lac88] and comprehensively studied by Sørensen [Sør92].
- San-José [SJ24] provided a recursive construction for projective Reed-Muller codes.
- Aubry, et al. [ACG+17] gave the parameters of $\mathrm{WPRM}_d(1, w_1, w_2)$ and $w_1 w_2 \mid d \leqslant q$.
- Çakıroğlu and Sahin [ÇŞ25] gave the parameters of $\mathrm{WPRM}_d(1, 1, w_2)$ and $d < q w_2$.
- Aubry and Perret [AP24] gave the minimum distance for $w = (1, w_1, w_2, \ldots, w_m)$ for $\mathrm{lcm}(w) \mid d \leqslant w_1 q$.

In this talk, I am going to

- give the parameters of $WPRM_d(1, w_1, w_2)$ for any degree d
  with Yağmur Çakıroğlu, Mesut Şahin (https://arxiv.org/abs/2410.11968)
  to appear in Design, Codes and Cryptography (WCC 2024)
- discuss how the methods can (or cannot) be generalized to general weights $w = (w_0, \ldots, w_m)$
  with Rodrigo San-José (ongoing work).

Vanishing Ideal of $\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$

Recall: $\mathrm{WPRM}_d(w) = \{(f(P_1),\dots,f(P_n)) : f \in S_d\}$ with $\{P_1,\dots,P_n\} = \mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$.

The vanishing ideal $I = I(\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q))$ is the (homogeneous) ideal generated by homogeneous polynomials vanishing on $\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$: $I = \bigoplus_{d\geqslant 0} I_d$.

$$\mathrm{WPRM}_d(w) \simeq S_d/I_d.$$

Theorem [Şa22, Proposition 5.6]

$I(\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q))$ is **binomial**, i.e. generated by differences of monomials.

Vanishing Ideal of $\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$

Recall: $\mathrm{WPRM}_d(w) = \{(f(P_1),\dots,f(P_n)) : f \in S_d\}$ with $\{P_1,\dots,P_n\} = \mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$.

The vanishing ideal $I = I(\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q))$ is the (homogeneous) ideal generated by homogeneous polynomials vanishing on $\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$: $I = \bigoplus_{d\geqslant 0} I_d$.

$$\mathrm{WPRM}_d(w) \simeq S_d/I_d.$$

Theorem [Şa22, Proposition 5.6]

$I(\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q))$ is **binomial**, i.e. generated by differences of monomials.

Theorem [Şa22, Corollary 5.8]

$I(\mathbb{P}(1,w_1,w_2)(\mathbb{F}_q))$ is generated by the following binomials:

$$f_0 = x_1x_2\left(x_2^{(q-1)w_1} - x_1^{(q-1)w_2}\right),\ f_1 = x_0x_2\left(x_2^{q-1} - x_0^{(q-1)w_2}\right),\ f_2 = x_0x_1\left(x_1^{q-1} - x_0^{(q-1)w_1}\right).$$

Theorem

$\{f_0, f_1, f_2\}$ is the unique minimal generating set and is also a universal Groebner basis.

Vanishing Ideal of $\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$

Recall: $\mathrm{WPRM}_d(w) = \{(f(P_1),\dots,f(P_n)) : f \in S_d\}$ with $\{P_1,\dots,P_n\} = \mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$.

The vanishing ideal $I = I(\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q))$ is the (homogeneous) ideal generated by homogeneous polynomials vanishing on $\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q)$: $I = \bigoplus_{d\geqslant 0} I_d$.

$$\mathrm{WPRM}_d(w) \simeq S_d/I_d.$$

Theorem [Şa22, Proposition 5.6]

$I(\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q))$ is **binomial**, i.e. generated by differences of monomials.

In general, $\prod_{i=0}^{m} x_i^{a_i} - \prod_{i=0}^{m} x_i^{b_i} \in I(\mathbb{P}(w_0,\dots,w_m)(\mathbb{F}_q))$ if and only if for every $i \in \{0,\dots,m\}$,

$$a_i = 0 \Leftrightarrow b_i = 0 \text{ and } q-1 \mid b_i - a_i.$$

[Şa22, §3] or [Nar22, Theorem 3.5]

⚠ Generators highly depend on the structure of the numerical semigroup $\langle w_0,\dots,w_m\rangle_{\mathbb{N}}$.

Monomials as integral points

Recall: $S = \mathbb{F}_q[x_0,\dots,x_m] = \bigoplus_{d\geqslant 0} S_d$ is graded by $\deg_w\left(\prod_{i=0}^m x_i^{a_i}\right) = a_0 w_0 + \cdots + a_m w_m$.

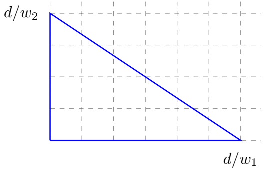
Assume $w = (1, w_1, w_2)$ with $w_1 \leqslant w_2$ coprime.

A degree $d \in \mathbb{N}$ defines a triangle

$$P_d := \left\{(x,y) \in \mathbb{R}^2 \;:\; x \geqslant 0,\; y \geqslant 0,\; w_1 x + w_2 y \leqslant d\right\}$$

whose integral points give a basis of $S_d = \operatorname{Span} \mathbb{M}_d$, where

$$\mathbb{M}_d := \left\{\mathrm{x}^{\mathrm{a},d} := x_0^{d-w_1a_1-w_2a_2} x_1^{a_1} x_2^{a_2} : \mathrm{a} = (a_1,a_2) \in P_d \cap \mathbb{Z}^2\right\}.$$



P_{12} for $w = (1,2,3)$

Monomials as integral points

Recall: $S = \mathbb{F}_q[x_0,\dots,x_m] = \bigoplus_{d\geqslant 0} S_d$ is graded by $\deg_w\left(\prod_{i=0}^m x_i^{a_i}\right) = a_0 w_0 + \cdots + a_m w_m$.

$$\prod_{i=0}^m x_i^{a_i} - \prod_{i=0}^m x_i^{b_i} \in I(\mathbb{P}(w)(\mathbb{F}_q)) \text{ iif } (a_i = 0 \Leftrightarrow b_i = 0) \text{ and } q-1 \mid b_i - a_i.$$

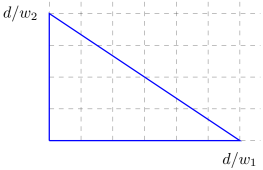
Assume $w = (1, w_1, w_2)$ with $w_1 \leqslant w_2$ coprime.

A degree $d \in \mathbb{N}$ defines a triangle

$$P_d := \left\{(x,y) \in \mathbb{R}^2 \;:\; x \geqslant 0,\; y \geqslant 0,\; w_1 x + w_2 y \leqslant d\right\}$$

whose integral points give a basis of $S_d = \operatorname{Span} \mathbb{M}_d$, where

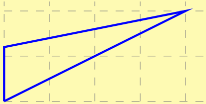
$$\mathbb{M}_d := \left\{\mathrm{x}^{\mathrm{a},d} := x_0^{d - w_1 a_1 - w_2 a_2} x_1^{a_1} x_2^{a_2} : \mathrm{a} = (a_1, a_2) \in P_d \cap \mathbb{Z}^2\right\}.$$



P_{12} for $w = (1,2,3)$

For general $w = (w_0,\dots,w_m)$, $P_d \subset \mathbb{R}^m$ is a simplex of dimension m.

Hermite Normal Form of $w^\top$ → normal fan of P_d

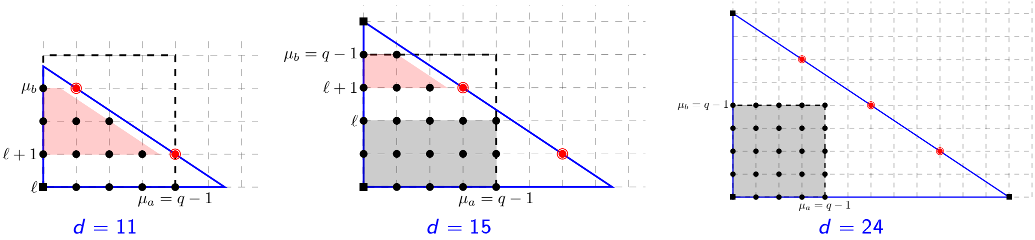


P_{12} for $w = (2,3,5)$

Given $a, b \in P_d \cap \mathbb{Z}^m$, $x^{a,d} - x^{b,d} \in I(\mathbb{P}(w)(\mathbb{F}_q))$ if and only if a and b lie exactly exactly on the same faces and $b - a \in (q-1)\mathbb{Z}^m$.

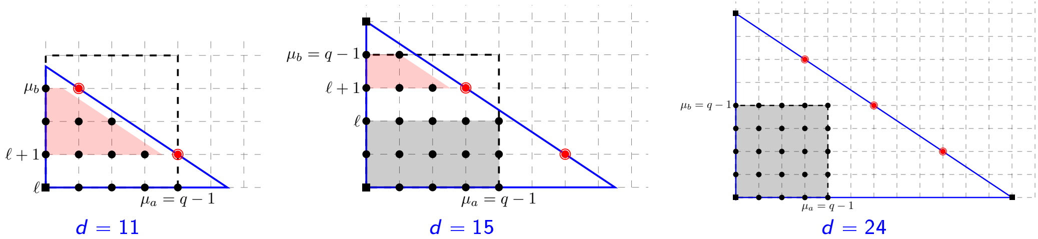
Basis of $\mathrm{WPRM}_d(w) = \mathbb{M}_d$ modulo $I(\mathbb{P}(w)(\mathbb{F}_q)) \simeq P_d \cap \mathbb{Z}^m$ modulo $q-1$ face by face.

Reduction and formula for the dimension of $\mathrm{WPRM}_d(1, w_1, w_2)$



Reduction of P_d with $w = (1, 2, 3)$ and $q = 5$.

Reduction and formula for the dimension of $\mathrm{WPRM}_d(1, w_1, w_2)$



Reduction of P_d with $w = (1, 2, 3)$ and $q = 5$.

Theorem: a closed formula for the dimension for $w = (1, w_1, w_2)$

$$\mu_i = \min\left\{\left\lfloor \frac{d-1}{w_i} \right\rfloor, q-1\right\},\ \ell = \max\left\{0, \min\left\{q-1, \left\lfloor \frac{d-1-w_1(q-1)}{w_2} \right\rfloor\right\}\right\}.$$

$$\text{Then } \dim_{\mathbb{F}_q}(\mathrm{WPRM}_d(1, w_1, w_2)) = (\ell+1)\mu_1 + \mu_2 + 1 + \sum_{y=\ell+1}^{\mu_2} \left\lfloor \frac{d-1-w_2 y}{w_1} \right\rfloor + |H(d)|$$

rectangular part — trapezoidal part — slope

$$\text{where } |H(d)| = \begin{cases} \mathrm{den}(d; (w_1, w_2)) & \text{if } d \leqslant w_1 w_2 (q-1), \\ q - 1 + 1_{w_1 | d} + 1_{w_2 | d} & \text{if } d > w_1 w_2 (q-1). \end{cases}$$

Minimum distance (1/2) *i.e. closed formulae that nobody wants to read*

Lower bound on the minimum distance using the footprint bound (Gröbner basis theory)

⚠ Footprint lower bound **never** achieved for $w = (1, \ldots, 1)$. [BDG19]

☺ For $w = (1, w_1, w_2) \neq (1, 1, 1)$ the footprint bound is achieved when $d < qw_2$.

Minimum distance (1/2) *i.e. closed formulae that nobody wants to read*

Lower bound on the minimum distance using the footprint bound (Gröbner basis theory)

⚠ Footprint lower bound **never** achieved for $w = (1, \ldots, 1)$. [BDG19]

☺ For $w = (1, w_1, w_2) \neq (1,1,1)$ the footprint bound is achieved when $d < qw_2$.

Theorem: Minimum distance of $\mathrm{WPRM}_d(1, w_1, w_2)$ with $\gcd(w_1, w_2 = 1)$ and $w_1 < w_2$

Set $\ell = \left\lfloor \frac{d-1-w_1(q-1)}{w_2} \right\rfloor$. Then $d_{min}(\mathrm{WPRM}_d(1, w_1, w_2)) = \begin{cases} q(q-d+1) & \text{if } d \leqslant q-1, \\ q - \ell & \text{if } q \leqslant d < w_2 q. \end{cases}$

Assume that $d \geqslant w_2 q$.

- If $w_1 = 1$, then $d_{min}(\mathrm{WPRM}_d(1, w_1, w_2)) = 1$.
- Assume $w_1 \geqslant 2$.
  - If $w_2 \geqslant w_1 + 2$, then $d_{min}(\mathrm{WPRM}_d(w) = \begin{cases} q - \ell & \text{if } w_1(q-1) < d \leqslant (w_1 + w_2)(q-1), \\ 1 & \text{if } d > (w_1 + w_2)(q-1). \end{cases}$
  - If $w_2 = w_1 + 1$, then

    $d_{min}(\mathrm{WPRM}_d(w)) = \begin{cases} q - \ell & \text{if } w_1(q-1) < d < w_2 q \text{ **OR** } d \geqslant w_2 q + \frac{q}{w_1 - 1} + 1, \\ 1 & \text{if } d > (w_1 + w_2)(q-1). \end{cases}$

    If $w_2 q \leqslant d < w_2 q + \frac{q}{w_1 - 1} + 1$, several cases have to be distinguished.

Minimum distance (2/2) *i.e. lower bounds (not even always equalities!) that nobody wants to read*

Theorem: Minimum distance of $\mathrm{WPRM}_d(1, w_1, w_2)$ with $w_2 = w_1 + 1$

If $w_2 q \leqslant d < w_2 q + \frac{q}{w_1 - 1} + 1$, several cases have to be distinguished.

⚠ **The footprint bound may not be achieved!**

- If $d - (w_1+1)q \notin \langle w_1, w_1+1 \rangle_{\mathbb{N}}$, then $d_{min}(\mathrm{WPRM}_d(1, w_1, w_2)) = q - \ell$.
- If $d - (w_1+1)q \in \langle w_1, w_1+1 \rangle_{\mathbb{N}}$, set $s = d - \left\lfloor \frac{d}{w_1(w_1+1)} \right\rfloor w_1(w_1+1)$. Then $d_{min}(\mathrm{WPRM}_d(1, w_1, w_2))$ is **bounded from below** by

$$\begin{cases} q - \max\left\{\ell, \left\lfloor \frac{d}{w_1(w_1+1)} \right\rfloor - 1\right\} & \text{if } s = 0 \text{ (i.e. } w_1(w_1+1) \mid d), \\ q - \max\left\{\ell, \left\lfloor \frac{d}{w_1(w_1+1)} \right\rfloor\right\} & \text{if } s \notin \langle w_1, w_1+1 \rangle_{\mathbb{N}} \text{ or } w_1 \mid s \text{ or } w_1 + 1 \mid s, \\ q - \max\left\{\ell, \left\lfloor \frac{d}{w_1(w_1+1)} \right\rfloor + 1\right\} & \text{if } s \in \langle w_1, w_1+1 \rangle_{\mathbb{N}} \text{ with } w_1 \nmid s \text{ and } w_1 + 1 \nmid s. \end{cases}$$

☺ The equality holds when the value is $q - \ell$ or when $w_1 \mid q - 1$.

Conclusion and open questions

What we have for $\mathrm{WPRM}_d(1, w_1, w_2)$:

- universal Gröbner basis of the vanishing ideal of $\mathbb{P}(1, w_1, w_2)(\mathbb{F}_q)$,
- regularity set of $\mathbb{P}(1, w_1, w_2)(\mathbb{F}_q)$,
- dimension for every degree d,
- minimum distance for *almost* every degree d.

(only a lower bound when $w_2 = w_1 + 1$ for a certain range of d)

What about more general w?

When $\gcd(w_i, q-1) = 1$ for all i's but 2, we can extend the recursive construction of PRM.

→ dimension, bound on generalized weights, subfield subcodes...

Research directions

- My current obsession: $\mathbb{P}(2, 3, 5)$ over $\mathbb{F}_{31}$ $(31 - 1 = 2 \cdot 3 \cdot 5)$
- a universal Gröbner basis for every w?
- Comparing the parameters $\mathrm{WPRM}_d(w)$ with existing codes
- How good are their local properties (decodability/recoverability)?

Conclusion and open questions

What we have for $\mathrm{WPRM}_d(1, w_1, w_2)$**:**

- universal Gröbner basis of the vanishing ideal of $\mathbb{P}(1, w_1, w_2)(\mathbb{F}_q)$,
- regularity set of $\mathbb{P}(1, w_1, w_2)(\mathbb{F}_q)$,
- dimension for every degree d,
- minimum distance for *almost* every degree d.

(only a lower bound when $w_2 = w_1 + 1$ for a certain range of d)

What about more general w**?**

When $\gcd(w_i, q-1) = 1$ for all i's but 2, we can extend the recursive construction of PRM.

$\rightarrow$ dimension, bound on generalized weights, subfield subcodes...

Research directions

- My current obsession: $\mathbb{P}(2, 3, 5)$ over $\mathbb{F}_{31}$ $(31 - 1 = 2 \cdot 3 \cdot 5)$
- a universal Gröbner basis for every w?
- Comparing the parameters $\mathrm{WPRM}_d(w)$ with existing codes
- How good are their local properties (decodability/recoverability)?

Thank you for your attention!

Regularity Set

Definition

The regularity set of $\mathbb{P}(w)(\mathbb{F}_q)$ is

$$\mathrm{reg}_{w,q} = \{d \in \langle w_0, \dots, w_m \rangle_{\mathbb{N}} : \dim_{\mathbb{F}_q} \mathrm{WPRM}_d(w) = \#\mathbb{P}(w)(\mathbb{F}_q)\}.$$

If $d \in \mathrm{reg}_{w,q}$ then $\mathrm{WPRM}_d(w) = \mathbb{F}_q^n$, where $n = \#\mathbb{P}(w)(\mathbb{F}_q)$. Thus, it is a trivial code $[n, n, 1]$.

Regularity Set for $w=(w_1,w_2)$ with $\gcd(w_1,w_2=1)$

Definition

The regularity set of $\mathbb{P}(w)(\mathbb{F}_q)$ is

$$\mathrm{reg}_{w,q} = \{d \in \langle w_0,\ldots,w_m\rangle_{\mathbb{N}} : \dim_{\mathbb{F}_q} \mathrm{WPRM}_d(w) = \#\mathbb{P}(w)(\mathbb{F}_q)\}.$$

If $d \in \mathrm{reg}_{w,q}$ then $\mathrm{WPRM}_d(w) = \mathbb{F}_q^n$, where $n = \#\mathbb{P}(w)(\mathbb{F}_q)$. Thus, it is a trivial code $[n,n,1]$.

Proposition

$d \in \mathrm{reg}_{(1,w_1,w_2),q}$ iif there exists $d_0 \geqslant q$ such that $d = d_0 w_1 w_2$ and $(w_1+w_2)(q-1) < d$.

$q+1$ integral points on the slope

$(q-1)^2$ integral points in the interior

Theorem

If $1 < w_1 < w_2$, then $\mathrm{reg}_{(1,w_1,w_2),q} = \{d \in \mathbb{N} : d = d_0 w_1 w_2 \text{ with } d_0 \geqslant q\} = q w_1 w_2 + \mathbb{N} w_1 w_2$.
If $w_1 = 1$, then

$$\mathrm{reg}_{(1,1,w_2),q} = \left\{ d \in \mathbb{N} : d = d_0 w_2 \text{ with } d_0 \geqslant q + \left\lfloor \frac{q-1}{w_2} \right\rfloor \right\} = \left(q + \left\lfloor \frac{q-1}{w_2} \right\rfloor \right) w_2 + \mathbb{N} w_2.$$

References

[ACG+17] Yves Aubry, Wouter Castryck, Sudhir R. Ghorpade, Gilles Lachaud, Michael E. O'Sullivan, and Samrith Ram. Hypersurfaces in weighted projective spaces over finite fields with applications to coding theory. In *Algebraic geometry for coding theory and cryptography*, volume 9 of *Assoc. Women Math. Ser.*, pages 25–61. Springer, Cham, 2017.

[AP24] Yves Aubry and Marc Perret. Maximum number of rational points on hypersurfaces in weighted projective spaces over finite fields. *Journal of Algebra and Its Applications*, 24.

[BDG19] Peter Beelen, Mrinmoy Datta, and Sudhir 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.

[ÇŞ25] Yağmur Çakıroğlu and Mesut Şahin. Algebraic invariants of codes on weighted projective planes. *Journal of Algebra and Its Applications*, (to be published):2550348, 2025.

[Lac88] Gilles 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.

[Nar22] Jade Nardi. Projective toric codes. *Int. J. Number Theory*, 18(1):179–204, 2022.

[Per03] Marc Perret. On the number of points of some varieties over finite fields. *Bulletin of the London Mathematical Society*, 35(3):309–320, 2003.

[SJ24] Rodrigo San-José. A recursive construction for projective reed-muller codes. *IEEE Transactions on Information Theory*, 70(12):8511–8523, 2024.

[Sør92] Anders Bjært Sørensen. Weighted Reed-Muller codes and algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 38(6):1821–1826, 1992.

[Şa22] Mesut Şahin. Computing vanishing ideals for toric codes, 2022.