Grassl-Rötteler cyclic and consta-cyclic MDS codes are generalised Reed-Solomon codes

Simeon Ball*

Abstract

We prove that the cyclic and constacyclic codes constructed by Grassl and Rötteler in [6] are generalised Reed-Solomon codes. This note can be considered as an addendum to Grassl and Rötteler [6]. It can also be considered as an appendix to Ball and Vilar [4], where Conjecture 11 of [6], which was stated for Grassl-Rötteler codes, is proven for generalised Reed-Solomon codes. The content of this note, together with [4], therefore implies that Conjecture 11 from [6] is true.

1 Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements. The weight of an element of $\mathbb{F}_q^n$ is the number of non-zero coordinates that it has. A k-dimensional linear code of length n and minimum distance d over $\mathbb{F}_q$, denoted as an $[n,k,d]_q$ code, is a k-dimensional subspace of $\mathbb{F}_q^n$ in which every non-zero vector has weight at least d.

The Singleton bound for linear codes states that

$$n \geqslant k + d - 1$$

and a linear code which attains the Singleton bound is called a maximum distance separable code, or MDS code for short. It is a simple matter to prove the bound

$$n \leqslant q + k - 1.$$

The MDS conjecture, for linear codes, states that if $4 \leqslant k \leqslant q-2$ then

$$n \leqslant q + 1.$$

*14 December 2022. The author acknowledges the support of MTM2017-82166-P and PID2020-113082GB-I00 financed by MCIN / AEI / 10.13039/501100011033, the Spanish Ministry of Science and Innovation.

For values of k outside of this range it is not difficult to determine the longest length of a linear MDS code. The MDS conjecture is known to hold for q prime [1], where it was also proven that if $k \neq (q+1)/2$ and q is prime then a $[q+1, k, q+2-k]_q$ MDS code is a generalised Reed-Solomon code.

Let $\{a_1, \ldots, a_q\}$ be the set of elements of $\mathbb{F}_q$.

A *generalised Reed-Solomon code* over $\mathbb{F}_q$ is

$$D = \{(\theta_1 f(a_1), \ldots, \theta_q f(a_q), \theta_{q+1} f_{k-1}) \mid f \in \mathbb{F}_q[X],\ \deg f \leqslant k-1\}, \tag{1}$$

where f_i denotes the coefficient of X^i in $f(X)$ and $\theta_i \in \mathbb{F}_q \setminus \{0\}$.

The Reed-Solomon code is the case in which $\theta_j = 1$, for all j.

We note that our definition of a (generalised) Reed-Solomon code is what some authors call the extended or doubly extended Reed-Solomon code. That is, many authors do not include the final coordinate or the evaluation at zero. However, a more natural definition of the Reed-Solomon code, which is entirely equivalent to the above, is obtained by evaluating homogeneous polynomials $f \in \mathbb{F}_q[X_1, X_2]$ of degree $k-1$, at the points of the projective line,

$$D = \{(\theta_1 f(a_1, 1), \ldots, \theta_q f(a_q, 1), \theta_{q+1} f(1, 0)) \mid f \in \mathbb{F}_q[X_1, X_2],\ \ f \text{ homogeneous},\ \deg f = k-1\}. \tag{2}$$

The Hermitian product code of a linear code C over $\mathbb{F}_{q^2}$ is

$$H(C) = \{u^q \cdot v \mid u, v \in C\}$$

where $u^q = (u_1^q, \ldots, u_n^q)$ and $\cdot$ is the standard inner-product. The puncture code is the intersection of $H(C)^\perp$ (the dual code of $H(C)$) with $\mathbb{F}_q^n$. This note was motivated by Conjecture 11 from [6] which states that the minimum distance d of the puncture code of the Grassl-Rötteler code satisfies

$$d = \begin{cases} 2k & \text{if } 1 \leqslant k \leqslant q/2 \\ (q+1)(k - \frac{1}{2}(q-1)) & \text{if } (q+1)/2 \leqslant k \leqslant q-1,\ q \text{ odd} \\ q(k+1-q/2) & \text{if } q/2 \leqslant k \leqslant q-1,\ q \text{ even} \\ q^2+1 & \text{if } k = q. \end{cases}$$

The equivalent version of this conjecture for generalised Reed-Solomon codes is proven in [4] for generalised Reed-Solomon codes. Combined with the content of this note, this implies that Conjecture 11 from [6] is indeed true.

2 Generalised Reed-Solomon codes

In this section we prove that a generalised Reed-Solomon code can be constructed as an evaluation code, evaluating at the $(q+1)$-th roots of unity of $\mathbb{F}_{q^2}$. Thus, any generalised Reed-Solomon

code can be obtained in this way by multiplying the i-th coordinate by a non-zero $\theta_i \in \mathbb{F}_q$, as in definition (1) and (2).

Let $\{\alpha_1, \ldots, \alpha_{q+1}\}$ be the set of $(q+1)$-th roots of unity of $\mathbb{F}_{q^2}$.

Lemma 1. *If $k \leqslant q$ is odd then the code*

$$C = \{(h(\alpha_1) + h(\alpha_1)^q, \ldots, h(\alpha_{q+1}) + h(\alpha_{q+1})^q) \mid h \in \mathbb{F}_{q^2}[X],\ \deg h \leqslant \tfrac{1}{2}(k-1)\}$$

is a $[q+1, k, q+2-k]_q$ generalised Reed-Solomon code.

Proof. Let σ be the map from the polynomials of $\mathbb{F}_{q^2}[X]$ of degree at most $\frac{1}{2}(k-1)$ to $\mathbb{F}_q^{q+1}$ defined by

$$\sigma(h) = (h(\alpha_1) + h(\alpha_1)^q, \ldots, h(\alpha_{q+1}) + h(\alpha_{q+1})^q).$$

Since, for all $\lambda, \nu \in \mathbb{F}_q$ and $g, h \in \mathbb{F}_{q^2}[X]$,

$$(\lambda h(\alpha_1) + \lambda h(\alpha_1)^q, \ldots, \lambda h(\alpha_{q+1}) + \lambda h(\alpha_{q+1})^q)$$

$$+(\nu g(\alpha_1) + \nu g(\alpha_1)^q, \ldots, \nu g(\alpha_{q+1}) + \nu g(\alpha_{q+1})^q)$$

$$= ((\lambda h + \nu g)(\alpha_1) + ((\lambda h + \nu g)(\alpha_1))^q, \ldots, (\lambda h + \nu g)(\alpha_{q+1}) + ((\lambda h + \nu g)(\alpha_{q+1}))^q),$$

it follows that σ is an $\mathbb{F}_q$-linear map.

Let

$$h(X) = \sum_{i=0}^{\frac{1}{2}(k-1)} c_i X^i.$$

For α, a $(q+1)$-st root of unity, we have

$$h(\alpha) + h(\alpha)^q = c_0 + c_0^q + \sum_{i=1}^{\frac{1}{2}(k-1)} c_i \alpha^i + \sum_{i=1}^{\frac{1}{2}(k-1)} c_i^q \alpha^{-i}.$$

If $c_i \neq 0$ for some $i \neq 0$ or $c_0 + c_0^q \neq 0$ then this implies that at most $k-1 \leqslant q-1$ of the coordinates of $\sigma(h)$ are zero. This implies that $\sigma(h) = 0$ if and only if $c_i = 0$ for all $i \neq 0$ and $c_0 + c_0^q = 0$. Therefore, σ is an $\mathbb{F}_q$-linear map which has a one-dimensional kernel. It follows that the image of the map σ, which is C, has dimension $2\frac{1}{2}(k+1) - 1 = k$. We conclude that C is a k-dimensional subspace of $\mathbb{F}_q^{q+1}$.

Suppose that $\{1, e\}$ is a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

For α, a $(q+1)$-th root of unity, let $x_1, x_2 \in \mathbb{F}_q$ be such that

$$\alpha = (x_1 + e x_2)^{q-1}.$$

Observe that as (x_1, x_2) vary over the points of the projective line, α will run through the distinct $(q+1)$-th roots of unity.

Then

$$h(\alpha) + h(\alpha)^q = \sum_{i=0}^{\frac{1}{2}(k-1)} c_i(x_1 + ex_2)^{i(q-1)} + c_i^q(x_1 + ex_2)^{i(1-q)}$$

$$= \sum_{i=0}^{\frac{1}{2}(k-1)} c_i(x_1 + e^q x_2)^i(x_1 + ex_2)^{-i} + c_i^q(x_1 + ex_2)^i(x_1 + e^q x_2)^{-i}$$

$$= (x_1 + ex_2)^{-\frac{1}{2}(k-1)(q+1)}\Big(\sum_i c_i(x_1 + ex_2)^{\frac{1}{2}(k-1)-i}(x_1 + e^q x_2)^{\frac{1}{2}(k-1)+i}$$

$$+c_i^q(x_1 + ex_2)^{\frac{1}{2}(k-1)+i}(x_1 + e^q x_2)^{\frac{1}{2}(k-1)-i}\Big).$$

Note that $(x_1 + ex_2)^{-\frac{1}{2}(k-1)(q+1)} \in \mathbb{F}_q$, does not depend on $h(X)$.

Thus, the coefficient of $x_1^j x_2^{k-j-1}$ of

$$\sum_{i=0}^{\frac{1}{2}(k-1)} c_i(x_1 + ex_2)^{\frac{1}{2}(k-1)-i}(x_1 + e^q x_2)^{\frac{1}{2}(k-1)+i} + c_i^q(x_1 + ex_2)^{\frac{1}{2}(k-1)+i}(x_1 + e^q x_2)^{\frac{1}{2}(k-1)-i},$$

is also an element of $\mathbb{F}_q$. Hence, the α coordinate of a codeword of C is the evaluation of a homogeneous polynomial in $\mathbb{F}_q[x_1, x_2]$ of degree $k-1$, multiplied by a non-zero element of $\mathbb{F}_q$. By definition (2), we conclude that such a code C is a generalised Reed-Solomon code. □

The previous lemma only applies to the case when k is odd. The following lemma deals with the case k is even.

Lemma 2. *For α_i, a $(q+1)$-th root of unity, let ω_i be such that $\alpha_i = \omega_i^{q-1}$. If k is even then the code*

$$C = \{\omega_1^q h(\alpha_1) + \omega_1 h(\alpha_1)^q, \ldots, \omega_{q+1}^q h(\alpha_{q+1}) + \omega_{q+1} h(\alpha_{q+1})^q) \mid h \in \mathbb{F}_{q^2}[X],\ \deg h \leqslant \tfrac{1}{2}k - 1\}$$

is a $[q+1, k, q+2-k]_q$ generalised Reed-Solomon code.

Proof. The proof is similar to that of Lemma 1. In this case we have that, $\omega = x_1 + ex_2$ and so

$$\omega^q h(\alpha) + \omega h(\alpha)^q = \sum_{i=0}^{\frac{1}{2}k-1} c_i(x_1 + ex_2)^{i(q-1)+q} + c_i^q(x_1 + ex_2)^{i(1-q)+1}$$

$$= (x_1 + ex_2)^{-(\frac{1}{2}k-1)(q+1)} \left(\sum_i c_i(x_1 + ex_2)^{\frac{1}{2}k-1-i}(x_1 + e^q x_2)^{\frac{1}{2}k+i} \right.$$

$$+c_i^q(x_1+ex_2)^{\frac{1}{2}k+i}(x_1+e^qx_2)^{\frac{1}{2}k-1-i}\Bigg).$$

The coefficient of $x_1^j x_2^{k-j-1}$ of

$$\sum_i c_i(x_1+ex_2)^{\frac{1}{2}k-1-i}(x_1+e^qx_2)^{\frac{1}{2}k+i}+c_i^q(x_1+ex_2)^{\frac{1}{2}k+i}(x_1+e^qx_2)^{\frac{1}{2}k-1-i},$$

is an element of $\mathbb{F}_q$. Thus, the lemma follows in the same way as Lemma 1. □

3 Grassl-Rötteler cyclic and constacyclic MDS codes

A k-dimensional cyclic or constacyclic code $\langle g\rangle$ of length n over $\mathbb{F}_q$, with generator polynomial

$$g(X)=\sum_{j=0}^{n-k}c_jX^j\in\mathbb{F}_q[X]$$

of degree $n-k$, is a linear code of length n spanned by the k cyclic shifts of the codeword

$$(c_0,\ldots,c_{n-k},0,\ldots,0).$$

It is a cyclic code if g divides X^n-1 and constacyclic code if g divides $X^n-\eta$, for some $\eta\neq 1$. See [2] or [8] for the basic results concerning cyclic codes.

In [6], Grassl and Rötteler introduced three $[q+1,k,q+2-k]_q$ MDS codes, the first two are constructed as cyclic codes and the third as a constacyclic code. As mentioned in the introduction, it follows from [1] that when q is prime and $k\neq\frac{1}{2}(q+1)$, these codes are generalised Reed-Solomon codes. In this section we shall prove that they are generalised Reed-Solomon codes for all q and k.

Let ω be a primitive element of $\mathbb{F}_{q^2}$ and let $\alpha=w^{q-1}$, a primitive $(q+1)$-th root of unity.

The Grassl-Rötteler codes depend on the parity of q and k.

For q and k both odd, and q and k both even, the Grassl-Rötteler code is $\langle g_1\rangle$, where

$$g_1(X)=\prod_{i=-r}^{r}(X-\alpha^i).$$

For k odd and q even, the Grassl-Rötteler code is the cyclic code $\langle g_2\rangle$, where

$$g_2(X)=\prod_{i=\frac{1}{2}q-r}^{\frac{1}{2}q+r+1}(X-\alpha^i).$$

And for k even and q odd, the Grassl-Rötteler code is the constacyclic code $\langle g_3 \rangle$, where

$$g_3(X) = \prod_{i=-r+1}^{r} (X - \omega\alpha^i).$$

It is a simple matter to check that for $i \in \{1, 2, 3\}$, $g_i \in \mathbb{F}_q[X]$ and for $i \in \{1, 2\}$, the polynomial g_i divides $X^{q+1} - 1$ and g_3 divides $X^{q+1} - \omega^{q+1}$.

We now treat each of the four cases, which depends on the parity of k and q, in turn and prove that they are all generalised Reed-Solomon codes.

Let $\{e_1, \ldots, e_{q+1}\}$ be the canonical basis of $\mathbb{F}_q^{q+1}$.

Let $\beta \in \mathbb{F}_{q^2}$ be such that $\beta + \beta^q = 1$.

Theorem 3. *If k and q are both odd then the $[q+1, k, q+2-k]_q$ code $\langle g_1 \rangle$ is a generalised Reed-Solomon code.*

Proof. Let c_j be defined by

$$g_1(X) = \prod_{i=-r}^{r} (X - \alpha^i) = \sum_{j=0}^{2r+1} c_j X^j.$$

Observe that $k = q - 2r$.

We will prove that, for $a \in \{0, \ldots, k-1\}$,

$$\sum_{s=a}^{q+1-k+a} (-1)^s c_{s-a} e_{s+1} = (\underbrace{0, \ldots, 0}_{a}, (-1)^a c_0, \ldots, (-1)^{q+1-k+a} c_{q+1-k}, \underbrace{0, \ldots, 0}_{k-1-a})$$

are the evaluations of certain polynomials,

$$h(X) + h(X)^q$$

where $h \in \mathbb{F}_{q^2}[X]$ is of degree at most $\frac{1}{2}(k-1)$, evaluated at the $(q+1)$-th roots of unity.

By Lemma 1 these codes are generalised Reed-Solomon codes, which implies that $\langle g_1 \rangle$ is a generalised Reed-Solomon code.

For $a \in \{0, \ldots, k-1\}$, define

$$h_a(X) = \sum_{i=1}^{\frac{1}{2}(q-1)} \sum_{j=0}^{2r+1} c_j \alpha^{i(j+a)} X^{(q+1)/2-i} + \sum_{j=0}^{2r+1} c_j (-1)^{j+a} \beta + \sum_{j=0}^{2r+1} c_j \beta X^{\frac{1}{2}(q+1)}.$$

For all $i \in \{0, \ldots, r\}$,

$$\sum_{j=0}^{2r+1} c_j \alpha^{ij} = 0,$$

since $g_1(\alpha^i) = 0$. Thus, $h_a(X)$ has no terms of degree $X^{\frac{1}{2}(q+1)-i}$ for $i \in \{0, \ldots, r\}$. Hence, the degree of h_a is at most $\frac{1}{2}(q-1) - r = \frac{1}{2}(k-1)$.

We have that

$$h_a(\alpha^s) = \sum_{i=1}^{\frac{1}{2}(q-1)} \sum_{j=0}^{2r+1} c_j \alpha^{i(j+a-s)} (-1)^s + \sum_{j=0}^{2r+1} c_j (-1)^{j+a} \beta + \sum_{j=0}^{2r+1} c_j \beta (-1)^s.$$

Since,

$$\left(\sum_{i=1}^{\frac{1}{2}(q-1)} c_j \alpha^{i(j+a-s)} \right)^q = \sum_{i=(q+3)/2}^{q} c_j \alpha^{i(j+a-s)},$$

and $\beta + \beta^q = 1$, it follows that

$$h_a(\alpha^s) + h_a(\alpha^s)^q = (-1)^s \sum_{j=0}^{2r+1} \sum_{i=0}^{q} c_j \alpha^{i(j+a-s)}.$$

Since $\sum_{i=0}^{q} \alpha^{ij} = 0$ unless $j = 0$, in which case it is one,

$$h_a(\alpha^s) + h_a(\alpha^s)^q = (-1)^s c_{s-a},$$

which is precisely what we had to prove. □

We next deal with the case k and q are both even, since this is again the code $\langle g_1 \rangle$.

Theorem 4. *If k and q are both even then the $[q+1, k, q+2-k]_q$ code $\langle g_1 \rangle$ is a generalised Reed-Solomon code.*

Proof. We can simply copy the proof of Theorem 3 until we define $h_a(X)$. Then we have to define $h_a(X)$ differently, partly because we will apply Lemma 2 in place of Lemma 1.

For $a \in \{0, \ldots, k-1\}$, define

$$h_a(X) = \sum_{i=1}^{\frac{1}{2}q} \sum_{j=0}^{2r+1} c_j \alpha^{i(j+a)} X^{\frac{1}{2}q-i} + \sum_{j=0}^{2r+1} c_j \beta X^{\frac{1}{2}q}.$$

Since $g_1(\alpha^i) = 0$, one has that

$$\sum_{j=0}^{2r+1} c_j \alpha^{ij} = 0$$

for all $i \in \{0, \ldots, r\}$. Thus, $h_a(X)$ has no terms of degree $X^{\frac{1}{2}q-i}$ for $i \in \{0, \ldots, r\}$. Hence, the degree of h_a is at most $\frac{1}{2}q - r - 1 = \frac{1}{2}k - 1$.

As before, let ω be a fixed primitive element of $\mathbb{F}_{q^2}$ and let $\alpha = \omega^{q-1}$, a primitive $(q+1)$-th root of unity. Then

$$h_a(\alpha^s) = \sum_{i=1}^{\frac{1}{2}q} \sum_{j=0}^{2r+1} c_j \alpha^{i(j+a-s)} \alpha^{\frac{1}{2}sq} + \sum_{j=0}^{2r+1} c_j \beta \alpha^{\frac{1}{2}sq}.$$

and so

$$\alpha^{-s} h_a(\alpha^s)^q = \sum_{i=1}^{\frac{1}{2}q} \sum_{j=0}^{2r+1} c_j \alpha^{-i(j+a-s)} \alpha^{-\frac{1}{2}sq-s} + \sum_{j=0}^{2r+1} c_j \beta^q \alpha^{-\frac{1}{2}sq-s}.$$

Since, $\beta + \beta^q = 1$ and $\alpha^{-\frac{1}{2}sq-s} = \alpha^{\frac{1}{2}sq}$, it follows that

$$h_a(\alpha^s) + \alpha^{-s} h_a(\alpha^s)^q = \alpha^{\frac{1}{2}sq} \sum_{j=0}^{2r+1} \sum_{i=0}^{q} c_j \alpha^{i(j+a-s)}.$$

Since $\sum_{i=0}^{q} \alpha^{ij} = 0$ unless $j = 0$, in which case it is one,

$$h_a(\alpha^s) + \alpha^{-s} h_a(\alpha^s)^q = \alpha^{\frac{1}{2}sq} c_{s-a}.$$

Hence,

$$\omega^{sq} h_a(\alpha^s) + \omega^s h_a(\alpha^s)^q = \omega^{\frac{1}{2}s(q+1)} c_{s-a}.$$

Lemma 2 implies that if we multiply the $(s+1)$-th coordinate of the codewords in $\langle g_1 \rangle$ by $\omega^{\frac{1}{2}s(q+1)}$ then we obtain a generalised Reed-Solomon code, which implies that $\langle g_1 \rangle$ is a generalised Reed-Solomon code. □

The next theorem deals with the case k is odd and q is even. In this case the Grassl-Rötteler code is $\langle g_2 \rangle$.

Theorem 5. *If k is odd and q is even then the $[q+1, k, q+2-k]_q$ code $\langle g_2 \rangle$ is a generalised Reed-Solomon code.*

Proof. Let c_j be defined by

$$g_2(X) = \prod_{i=\frac{1}{2}q-r}^{\frac{1}{2}q+r+1} (X - \alpha^i) = \sum_{j=0}^{2r+2} c_j X^j.$$

Observe that $k = q - 2r - 1$.

As in Theorem 3, we look for polynomials $h_a(X)$ which allow us to apply Lemma 1.

For $a \in \{0, \ldots, k-1\}$, let

$$h_a(X) = \sum_{i=1}^{\frac{1}{2}q} \sum_{j=0}^{2r+2} c_j \alpha^{(i+\frac{1}{2}q)(j+a)} X^{\frac{1}{2}q+1-i} + \sum_{j=0}^{2r+2} c_j \beta.$$

Observe that, for all $i \in \{\frac{1}{2}q+1, \ldots, \frac{1}{2}q+r+1\}$,

$$\sum_{j=0}^{2r+2} c_j \alpha^{ij} = 0,$$

since $g_1(\alpha^i) = 0$. Thus, $h_a(X)$ has no terms of degree $X^{\frac{1}{2}q+1-i}$ for $i \in \{0, \ldots, r+1\}$. Hence, the degree of h_a is at most $\frac{1}{2}q + 1 - (r+2) = \frac{1}{2}(k-1)$.

We have that

$$h_a(\alpha^s) = \sum_{i=1}^{\frac{1}{2}q} \sum_{j=0}^{2r+2} c_j \alpha^{(i+\frac{1}{2}q)(j+a-s)} + \sum_{j=0}^{2r+2} c_j \beta.$$

and so

$$h_a(\alpha^s)^q = \sum_{i=1}^{\frac{1}{2}q} \sum_{j=0}^{2r+2} c_j \alpha^{(-i+\frac{1}{2}q+1)(j+a-s)} + \sum_{j=0}^{2r+2} c_j \beta^q.$$

Since, $\beta + \beta^q = 1$, it follows that

$$h_a(\alpha^s) + h_a(\alpha^s)^q = \sum_{j=0}^{2r+2} \sum_{i=0}^{q} c_j \alpha^{i(j+a-s)}.$$

Since $\sum_{i=0}^{q} \alpha^{ij} = 0$ unless $j = 0$, in which case it is one,

$$h_a(\alpha^s) + h_a(\alpha^s)^q = c_{s-a}.$$

Lemma 2 implies that $\langle g_1 \rangle$ is a generalised Reed-Solomon code. □

Finally, we deal with the case k is even and q is odd, which is the constacyclic code $\langle g_3 \rangle$.

Theorem 6. *If k is even and q is odd then the $[q+1, k, q+2-k]_q$ code $\langle g_3 \rangle$ is a generalised Reed-Solomon code.*

Proof. Let c_j be defined by

$$g_3(X) = \prod_{i=-r+1}^{r} (X - \omega\alpha^i) = \sum_{j=0}^{2r} c_j X^j.$$

Observe that $k = q - 2r + 1$.

As in Theorem 4, we look for polynomials $h_a(X)$ which allow us to apply Lemma 2.

For $a \in \{0, \ldots, k-1\}$, let

$$h_a(X) = \sum_{i=1}^{\frac{1}{2}(q+1)} \sum_{j=0}^{2r} \omega^{j+a} c_j \alpha^{i(j+a)} X^{\frac{1}{2}(q+1)-i}.$$

Observe that, for all $i \in \{0, \ldots, r\}$,

$$\sum_{j=0}^{2r} c_j \omega^j \alpha^{ij} = 0,$$

since $g_3(\omega\alpha^i) = 0$. Thus, the degree of h_a is at most $\frac{1}{2}(q+1) - (r+1) = \frac{1}{2}k - 1$.

We have that

$$h_a(\alpha^s) = \sum_{i=1}^{\frac{1}{2}(q+1)} \sum_{j=0}^{2r} \omega^{j+a} c_j \alpha^{i(j+a-s)} (-1)^s.$$

and, since $\omega^q = \omega\alpha$,

$$\alpha^{-s} h_a(\alpha^s)^q = \sum_{i=1}^{\frac{1}{2}(q+1)} \sum_{j=0}^{2r} \omega^{j+a} c_j \alpha^{-(i-1)(j+a-s)} (-1)^s.$$

Hence, it follows that

$$h_a(\alpha^s) + \alpha^{-s} h_a(\alpha^s)^q = \sum_{i=1}^{q+1} \sum_{j=0}^{2r} \omega^{j+a} c_j \alpha^{i(j+a-s)} (-1)^s.$$

Since $\sum_{i=1}^{q+1} \alpha^{ij} = 0$ unless $j = 0$, in which case it is one,

$$h_a(\alpha^s) + \alpha^{-s} h_a(\alpha^s)^q = \omega^s (-1)^s c_{s-a}.$$

Hence,

$$\omega^{sq} h_a(\alpha^s) + \omega^s h_a(\alpha^s)^q = \omega^{s(q+1)} (-1)^s c_{s-a}.$$

Lemma 2 implies that if we multiply the $(s+1)$-th coordinate of the codewords in $\langle g_3 \rangle$ by $(-w^{(q+1)})^s$ then we obtain a generalised Reed-Solomon code, which implies that $\langle g_3 \rangle$ is a generalised Reed-Solomon code. □

4 Conclusions

It may be an interesting and worthwhile exercise to see if the other known $[q+1, k, q+2-k]_q$ MDS codes can be easily obtained as evaluation codes, evaluating at the $(q+1)$-th roots of unity. It may even be that the evaluation is over a more exotic set of elements in some extension of $\mathbb{F}_q$. For completeness sake, we mention the other known $[q+1, k, q+2-k]_q$ MDS codes.

For $k = 3$ and q even, there are many examples known. These can all be extended to a $[q+2, k, q+3-k]_q$ MDS code. The columns of a generator matrix of such a code can be viewed as a set of points in the projective plane $\mathrm{PG}(2, q)$. Such a set of points is known as a *hyperoval*. For a complete list of known hyperovals, see [3, Table 1].

There are only two other known examples, up to duality.

The following is due to Segre [7]. The linear code whose columns are the elements of the set

$$\{(1, t, t^{2^e}, t^{2^e+1}) \mid t \in \mathbb{F}_q\} \cup \{(0, 0, 0, 1)\}$$

is a $[q+1, 4, q-2]_q$ linear MDS code, whenever $q = 2^h$ and $(e, h) = 1$.

The other is due to Glynn [5]. Let η be an element of $\mathbb{F}_9$ such that $\eta^4 = -1$. The linear code whose columns are the elements of the set

$$\{(1, t, t^2 + \eta t^6, t^3, t^4) \mid t \in \mathbb{F}_9\} \cup \{(0, 0, 0, 0, 1)\}.$$

is a $[10, 5, 6]_9$ linear MDS code.

5 Statements and Declarations

Data sharing not applicable to this article as no datasets were generated or analysed during the current study. There are no competing interests that are directly or indirectly related to the work submitted.

I would like to express my gratitude to the referees and the editor whose input was most appreciated.

References

[1] S. Ball, On sets of vectors of a finite vector space in which every subset of basis size is a basis, *J. Eur. Math. Soc.*, **14** (2012) 733–748.

[2] S. Ball, *A Course in Algebraic Error-Correcting Codes*, Compact Textbooks in Mathematics, Birkhauser, 2020.

[3] S. Ball and M. Lavrauw, Arcs in finite projective spaces, *EMS Surveys in Mathematical Science*, **6** (2019)133–172.

[4] S. Ball and R. Vilar, Determining when a truncated generalised Reed-Solomon code is Hermitian self-orthogonal, *IEEE Trans. Inform. Theory*, **68** (2022) 3796–3805.

[5] D. G. Glynn, The non-classical 10-arc of $\mathrm{PG}(4,9)$, *Discrete Math.*, **59** (1986) 43–51.

[6] M. Grassl and M. Rötteler, Quantum MDS codes over small fields, in *Proc. Int. Symp. Inf. Theory (ISIT)*, 1104–1108 (2015).

[7] B. Segre, Le geometrie di Galois. *Ann. Mat. Pura Appl.* **48** (1959) 1–96.

[8] J. H. van Lint, *Introduction to Coding Theory*, Graduate Texts in Mathematics, **86**, Springer, 1999.

Simeon Ball
Departament de Matemàtiques,
Universitat Politècnica de Catalunya,
Mòdul C3, Campus Nord,
Carrer Jordi Girona 1-3,
08034 Barcelona, Spain

email: simeon.michael.ball@upc.edu

Orcid: 0000-0003-4845-2084