Partial permutation decoding for MacDonald codes

J.D. Key*
Department of Mathematics
and Applied Mathematics
University of the Western Cape
7535 Bellville, South Africa

P. Seneviratne†
Department of Mathematics
Texas A&M University-Commerce
2600 South Neal Street, Commerce
TX 75428, U.S.A.

January 28, 2016

Abstract

We show how to find s-PD-sets of the minimal size $s+1$ for the $\left[\frac{q^n-q^u}{q-1}, n, q^{n-1}-q^{u-1}\right]_q$ MacDonald q-ary codes $C_{n,u}(q)$ where $n \geq 3$ and $1 \leq u \leq n-1$. The construction of [6] can be used and gives s-PD-sets for s up to the bound $\lfloor \frac{q^{n-u}-1}{(n-u)(q-1)} \rfloor - 1$, of effective use for u small; for $u \geq \lfloor \frac{n}{2} \rfloor$ an alternative construction is given that applies up to a bound that depends on the maximum size of a set of vectors in $V_u(\mathbb{F}_q)$ with each pair of vectors distance at least 3 apart.

Keywords: MacDonald codes, simplex codes, PD-sets
Mathematics Subject Classifications (2010): 05B05, 94B05

1 Introduction

The MacDonald codes, introduced by MacDonald [12] for binary codes, with the definition extended to q-ary codes in [2, 15], are punctured simplex codes, of length $\frac{q^n-q^u}{q-1}$ for any n and $1 \leq u \leq n-1$. They have parameters $\left[\frac{q^n-q^u}{q-1}, n, q^{n-1}-q^{u-1}\right]_q$ and are 2-weight codes with the non-zero words of weight $q^{n-1}-q^{u-1}$ and q^{n-1}. Following [2], we denote the codes by $C_{n,u}(q)$.

In [6] permutation decoding for the simplex codes was considered and s-PD-sets of the minimal size $s+1$ were found for s up to some large bound. Since the efficiency of the decoding depends on the size of the PD-set, those of minimal size as determined by the Gordon-Schönheim bound (see Result 1) are the best ones to obtain. The ideas behind the establishment of these PD-sets for the simplex codes can be applied to the MacDonald codes, and we obtain here some similar results. The automorphism group used for the permutation decoding is a subgroup of the general linear group and thus described as $n \times n$ matrices. A general construction of suitable matrices allows us to prove a general theorem:

Theorem 1. *For $n \geq 3$ and $1 \leq u \leq n-1$, q a prime power, let $C_{n,u}(q)$ denote the $\left[\frac{q^n-q^u}{q-1}, n, q^{n-1}-q^{u-1}\right]_q$ MacDonald q-code. Then $C_{n,u}(q)$ has s-PD-sets of size $s+1$*

*keyj@clemson.edu
†Padmapani.Seneviratne@tamuc.edu

- *for all* s *such that* $1 \leq s \leq f_{n-u}(\mathbb{F}_q) = \left\lfloor \frac{q^{n-u}-1}{(n-u)(q-1)} \right\rfloor - 1$;
- *for* $n \geq 4$ *for all* s *such that* $1 \leq s \leq |D| - 1$ *where* D *is a set of vectors in* $V_u(\mathbb{F}_q)$ *which is such that any two members of* D *are distance at least* 3 *apart.*

Such s*-PD-sets can be explicitly given in terms of matrices in* $GL_n(\mathbb{F}_q)$.

The construction for the first bound is given in Proposition 2 and Corollary 1, using Result 3, and for the second in Proposition 3 and Corollary 2. The s-PD-sets are all nested in the sense that if $1 \leq r \leq s$ then any subset of the set of size $r+1$ will correct r errors.

Unlike in the simplex case, these sets from Corollary 1 are too small, and therefore correct too few errors, if u is large. In that case one uses the second construction (of Proposition 3), and particular examples of these arise from any q-ary code of length u and minimum weight at least 3: for example, the Hamming codes. Other examples exist by finding sets of $s+1$ vectors in $V_u(\mathbb{F}_q)$ such that the distance between any two vectors in the set is at least 3.

We describe our notation and give some background definitions in Section 2 and Section 3, and prove the results on the s-PD-sets of size $s+1$ in Section 4. Included as Section 6 is an appendix giving some tables showing the best size of s for sets of size $s+1$ using our methods, for $4 \leq n \leq 10$, $1 \leq u \leq n-1$, and $q = 2, 3, 4, 5$. Magma [3, 5] was used for any computations, and in particular to find the sets in the case where u is large.

2 Background and terminology

The notation for codes is standard and can be found in [1]. The codes here are all **linear codes**, and the notation $[n, k, d]_q$ will be used for a q-ary code C of length n, dimension k, and minimum weight d, where the **weight** $\mathbf{wt}(v)$ of a vector v is the number of non-zero coordinate entries. The **distance**, $d(u, v)$, between two vectors u, v is $\mathrm{wt}(u-v)$, i.e. the number of coordinate places in which they differ. A **generator matrix** for an $[n, k, d]_q$ code C is a $k \times n$ matrix whose rows form a basis for C, and the **dual** code $C^\perp$ is the orthogonal under the standard inner product $(,)$, i.e. $C^\perp = \{v \in F^n \mid (v, c) = 0 \text{ for all } c \in C\}$. A **check matrix** for C is a generator matrix for $C^\perp$.

Following [1, Definition 2.2.3], two linear codes over the same field are called **equivalent** if each can be obtained from the other by permuting the coordinate positions and multiplying each coordinate by a non-zero field element. The codes will be said to be **isomorphic** if a permutation of the coordinate positions suffices to take one to the other. Generally, an **automorphism** of a code C is a code equivalence from C to C, and the set of all these gives the automorphism group of the code, written $\mathrm{Aut}(C)$ or $\mathrm{MAut}(C)$ (following [8, Chapter 7,Section 1.3]), since they are given by monomial matrices, and we do not consider here the more general case that includes field automorphisms, or the Galois groups. If only permutations of the coordinate positions are allowed then the group of permutation automorphisms is, again following [8, Chapter 7, Section 1.3], called the permutation automorphism group, written $\mathrm{PAut}(C)$. Any code is isomorphic to a code with generator matrix in so-called **standard form**, i.e. the form $[I_k \mid A]$; a check matrix then is given by $[-A^T \mid I_{n-k}]$. The set of the first k coordinate positions in the standard form is called an **information set** for the code, and the set of the last $n-k$ coordinate positions is the corresponding **check set**.

Permutation decoding was developed by MacWilliams [13] and involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and

Sloane [14, Chapter 16, p. 513] and Huffman [8, Section 8]. In [9] and [11] the definition of PD-sets was extended to that of s-PD-sets for s-error-correction:

Definition 1. *If C is a t-error-correcting code with information set $\mathcal{I}$ and check set $\mathcal{C}$, then a* **PD-set** *for C is a set $\mathcal{S}$ of automorphisms of C which is such that every t-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into the check positions $\mathcal{C}$.*

For $s \leq t$ an s-**PD-set** *is a set $\mathcal{S}$ of automorphisms of C which is such that every s-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into $\mathcal{C}$.*

The algorithm for permutation decoding is as follows: we have a t-error-correcting $[n, k, d]_q$ code C with check matrix H in standard form. Thus the generator matrix $G = [I_k|A]$ and $H = [-A^T|I_{n-k}]$, for some A, and the first k coordinate positions correspond to the information symbols. Any vector v of length k is encoded as vG. Suppose x is sent and y is received and at most t errors occur. Let $S = \{g_1, \ldots, g_s\}$ be the PD-set. Compute the syndromes $H(yg_i)^T$ for $i = 1, \ldots, s$ until an i is found such that the weight of this vector is t or less. Compute the codeword c that has the same information symbols as yg_i and decode y as cg_i^{-1}.

Notice that this algorithm actually uses the PD-set as a sequence. Thus it is expedient to index the elements of the set S by the set $\{1, 2, \ldots, |S|\}$ so that elements that will correct a small number of errors occur first. Thus if **nested** s-**PD-sets** are found for all $1 < s \leq t$ then we can order S as follows: find an s-PD-set S_s for each $0 \leq s \leq t$ such that $S_0 \subset S_1 \ldots \subset S_t$ and arrange the PD-set S as a sequence in this order:

$$S = [S_0, (S_1 - S_0), (S_2 - S_1), \ldots, (S_t - S_{t-1})].$$

(Usually one takes $S_0 = \{id\}$.)

There is a bound on the minimum size that a PD-set S may have, due to Gordon [7], from a formula due to Schönheim [16], and quoted and proved in [8]:

Result 1. *If S is a PD-set for a t-error-correcting $[n, k, d]_q$ code C, and $r = n - k$, then*

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \ldots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \ldots \right\rceil \right\rceil \right\rceil. \quad (1)$$

This result can be adapted to s-PD-sets for $s \leq t$ by replacing t by s in the formula. Note that since $r < n$, the innermost term for any s is 2, and since there are s terms in the formula, it follows that the size of an s-PD-set is at least $s + 1$.

We will use the following from [10, Lemma 7]:

Result 2. *Let C be a code with minimum distance d, $\mathcal{I}$ an information set, $\mathcal{C}$ the corresponding check set and $\mathcal{P} = \mathcal{I} \cup \mathcal{C}$. Let A be an automorphism group of C, and n the maximum of $|\mathcal{O} \cap \mathcal{I}|/|\mathcal{O}|$, where $\mathcal{O}$ is an A-orbit. If $s = \min(\lceil \frac{1}{n} \rceil - 1, \lfloor \frac{d-1}{2} \rfloor)$, then A is an s-PD-set for C.*

3 MacDonald codes

The q-ary simplex code $\mathcal{S}_n(\mathbb{F}_q)$, for any prime-power q, is a q-ary code with generator matrix having for columns any set of $\frac{q^n-1}{q-1}$ representatives of the distinct 1-dimensional subspaces of $V_n(\mathbb{F}_q)$, i.e. the points of the projective space $PG_{n-1}(\mathbb{F}_q)$: see, for example, [1, Section 2.5]. Thus for $q > 2$ the actual code depends on the representatives chosen, but the codes are of course all equivalent. It follows that $\mathcal{S}_n(\mathbb{F}_q)$ is a $[\frac{q^n-1}{q-1}, n, q^{n-1}]_q$ code and all the non-zero words have weight q^{n-1}: see [1, Section 2.5]. The coordinate positions are labelled by the projective points $PG_{n-1}(\mathbb{F}_q)$. The automorphism group is isomorphic to $\Gamma L_n(q)$, as shown in [8, Section 7].

The MacDonald codes were introduced by MacDonald [12] for $p = 2$ and in [15] (see also [2]) for any q, and are simplex codes punctured in a particular way. Thus for any number u such that $1 \leq u \leq n-1$, if e_i denotes the i^{th} basis element of the standard basis for the vector space $V_n(\mathbb{F}_q) = \mathbb{F}_q^n$, let $U = \langle e_i \mid n-u+1 \leq i \leq n \rangle$, i.e. all the vectors with the first $n-u$ positions equal to 0. The $\frac{q^u-1}{q-1}$ coordinate positions for the vectors in U are removed to produce a code of length $\frac{q^n-q^u}{q-1}$, with coordinate positions labelled by the points of $PG_{n-1}(\mathbb{F}_q)$ that are not in the projective space $PG_{u-1}(\mathbb{F}_q)$. The code still has dimension n but now it is a two-weight code, with words of weight q^{n-1} and $q^{n-1} - q^{u-1}$, as can easily be seen. We denote these codes by $C_{n,u}(q)$, following [2]. If $q > 2$ then different choices of the representatives of the projective points (columns of the generator matrix) will produce different codes, but the codes will be equivalent.

Thus for all q, n, u where $1 \leq u \leq n-1$, $C_{n,u}(q)$ is a

$$\left[\frac{q^n - q^u}{q-1}, n, q^{n-1} - q^{u-1}\right]_q$$

q-ary code with non-zero codewords of weight q^{n-1} or $q^{n-1} - q^{u-1}$.

It is clear that if

$$\mathcal{I}_{n,u} = \{e_i \mid 1 \leq i \leq n-u\} \cup \{e_1 + e_i \mid n-u+1 \leq i \leq n\} = \{w_i \mid 1 \leq i \leq n\}, \qquad (2)$$

then the corresponding projective points will form an information set for $C_{n,u}(q)$ for any n, u, q, where we write $w_i = e_i$ for $1 \leq i \leq n-u$, and $w_i = e_1 + e_i$ for $n-u+1 \leq i \leq n$.

As in [6] we will write our vectors as rows and have an $n \times n$ matrix A act on $v \in V_n(\mathbb{F}_q) \setminus \{0\}$ (i.e. $\langle v \rangle \in PG_{n-1}(\mathbb{F}_q)$) as vA. However, if $q > 2$, it could happen that vA is not the chosen representative of the projective point $\langle vA \rangle$. In such cases automorphisms of the code C are still produced, but do not correspond to permutations of the code, i.e. they are in $\mathrm{MAut}(C)$ but not in $\mathrm{PAut}(C)$. In this case the action of the $n \times n$ matrix A on the code is as described in [6, Corollary 5], and involves using a generator matrix G, in standard form, for the code, and finding a monomial matrix M such that $G^T A = MG^T$. Then the action on the code is given by $c \mapsto cM^T$ for any codeword c, and permutation decoding may still be used. In the binary case we can always just use the matrix itself.

For simplicity, we will choose the columns of the defining generating matrix to have first entry 1. In this way any suitable matrix in upper triangular form with 1's on the diagonal will directly give a member of $\mathrm{PAut}(C)$.

Let $M_{m,n}(\mathbb{F}_q)$ denote the $m \times n$ matrices over $\mathbb{F}_q$. We take $n \geq 3$ to avoid trivial cases or codes that would not be used for permutation decoding.

Proposition 1. *Let $n \geq 3$, q a prime power, $1 \leq u \leq n-1$, $C_{n,u}(q)$ the MacDonald code,*

$$K = \{ \left[\begin{array}{c|c} A & C \\ \hline 0 & B \end{array}\right] \mid A \in GL_{n-u}(\mathbb{F}_q), B \in GL_u(\mathbb{F}_q), C \in M_{n-u,u}(\mathbb{F}_q)\},$$

and

$$H = \{M \mid M \in G, B = I_u\}.$$

Then K preserves $C_{n,u}(q)$, and H acts transitively on the coordinate positions of $C_{n,u}(q)$.

Furthermore, H is an s-PD-set for $C_{n,u}(q)$, for any information set, where

$$s = \min(\lceil \frac{q^n - q^u}{n(q-1)} \rceil - 1, \lfloor \frac{q^{n-1} - q^{u-1} - 1}{2} \rfloor).$$

Proof: Clearly any such matrix will map a vector of the form $(0, \dots, 0, a_{n-u+1}, \dots, a_n)$ to one of the same form so the vectors corresponding to the coordinate positions are preserved. To show the group H is transitive on the coordinate positions we can show that e_1 can map to any vector v from the coordinate set by taking a matrix with v as the first row. Thus any member of the coordinate set can be mapped to any other by some automorphism of the code induced by a member of H.

To show that H is an s-PD-set as stated, use Result 2. ■

Note: The permutation group $\mathrm{PAut}(C_{n,u}(q))$ may not be transitive for $q > 2$.

Example 1. For $u = n-1$, $H = \{\left[\begin{array}{c|c} 1 & c \\ \hline 0 & I_{n-1} \end{array}\right] \mid c \in V_{n-1}(\mathbb{F}_q)\}$. Thus $|H| = q^{n-1}$ and the group H will be a s-PD-set for $C_{n,n-1}(q)$ for $n \geq 3$, where $s = \lceil \frac{q^n - q^{n-1}}{n(q-1)} \rceil - 1 = \lceil \frac{q^{n-1}}{n} \rceil - 1$, since this is smaller than, or equal to, $\lfloor \frac{q^{n-1} - q^{n-2} - 1}{2} \rfloor$.

4 s-PD-sets of size $s+1$

We can use the results of [6] to obtain s-PD-sets of size $s+1$ for the MacDonald codes using automorphisms from the matrix group $GL_n(\mathbb{F}_q)$ acting on the coordinate positions. Recall that we noted after giving Result 1 (the Gordon-Schönheim bound) that for correcting s errors the PD-set must have size at least $s+1$.

We consider the binary case, since the ideas can be extended to the q-ary case as well, as in [6]. The coordinate positions for $C_{n,u}(2)$ are the vectors from $V_n(\mathbb{F}_2) \setminus U$, where $U = \langle e_i \mid n-u+1 \leq i \leq n \rangle$. The information set is $\mathcal{I}_{n,u}$ as given in Equation (2).

Proposition 2. *For $n \geq 3$, $1 \leq u \leq n-1$, let $C_{n,u}(2)$ be the $[2^n - 2^u, n, 2^{n-1} - 2^{u-1}]_2$ MacDonald code with information set $\mathcal{I}_{n,u}$ and check set $\mathcal{C}_{n,u}$. For fixed $k \geq 1$, let*

$$P_k = \{M_i = \left[\begin{array}{c|c} N_i & 0 \\ \hline 0 & I_u \end{array}\right] \mid 0 \leq i \leq k\}$$

where $N_i \in GL_{n-u}(\mathbb{F}_2)$, be a set of $k+1$ matrices in $GL_n(\mathbb{F}_2)$ such that no two matrices N_i^{-1} and N_j^{-1} for $i \neq j$ have a row in common. Then P_k is a k-PD-set of $k+1$ elements for $C_{n,u}(2)$ with information set $\mathcal{I}_{n,u}$. Furthermore, any subset of P_k of size $s+1$ where $1 \leq s \leq k$ is an s-PD-set for $C_{n,u}(2)$.

Conversely, if $R_k = \{L_i = \left[\begin{array}{c|c} H_i & 0 \\ \hline 0 & I_u \end{array}\right] \mid 0 \leq i \leq k\} \subseteq K$ is a k-PD-set for $C_{n,u}(2)$ then no two matrices H_i^{-1} and H_j^{-1} for $i \neq j$ have a row in common.

Proof: Note first that $M_i^{-1} = \left[\begin{array}{c|c} N_i^{-1} & 0 \\ \hline 0 & I_u \end{array}\right]$. Suppose $P_k = \{M_i \mid 0 \leq i \leq k\}$ as shown, and no two matrices N_i^{-1} and N_j^{-1} for $i \neq j$ have a row in common. Let $T = \{v_1, \dots, v_k\}$ be a set of k

distinct vectors in $V_n(\mathbb{F}_2)\setminus U$. Suppose that we cannot map T into $\mathcal{C}_{n,u}$ by any element of P_k. Then for each i such that $0 \le i \le k$, there is a $v_j \in T$, for $1 \le j \le k$, such that $v_j M_i \in \mathcal{I}_{n,u}$. Since there are $k+1$ values of i but only k of j we must have $v_j M_i$ and $v_j M_l$, for some j, and $l \neq i$, both in $\mathcal{I}_{n,u}$. Suppose $v_j M_i = w_r$ and $v_j M_l = w_t$; then $v_j = w_r M_i^{-1} = w_t M_l^{-1}$. There are three cases to consider:
Case (1): $r,t \le n-u$. Then $w_r = e_r$ and $w_t = e_t$, so the r^{th} row of M_i^{-1} is the t^{th} row of M_l^{-1}, contradicting our assumption.
Case (2): $r \le n-u$, $t > n-u$. Then $w_r = e_r$ and $w_t = e_1 + e_t$. Thus $w_r M_i^{-1}$ is the r^{th} row of M_i^{-1}, which has the last u digits equal to 0, and $w_t M_l^{-1} = (e_1+e_t)M_l^{-1}$, i.e. the sum of the first row of M_l^{-1} and the t^{th} row, and this does not have 0's in the last u digits.
Case (3): $r > n-u$, $t > n-u$. Then $w_r = e_1 + e_r$ and $w_t = e_1 + e_t$. Thus $w_r M_i^{-1}$ is the sum of the first and r^{th} rows of M_i^{-1}, and $w_t M_l^{-1}$ is the sum of the first and t^{th} rows of M_l^{-1}. This is again a contradiction, since the first rows of M_i^{-1} and M_l^{-1} are different.

Clearly the above argument works for any s with $1 \le s \le k$.

The proof of the remaining statement is virtually the same as that given in [6, Proposition 1]. ■

The proof of the proposition extends easily to $C_{n,u}(q)$ for any q, noting that we take the rows of the matrices N_i^{-1} to be normalized and the action of the matrix on the code might not be a permutation automorphism, as described in Section 3.

The construction of sets of matrices as required here is discussed in [6] and the reader is referred to that paper and references there to see how this can be achieved. In particular, the number

$$f_n(\mathbb{F}_q) = \left\lfloor \frac{q^n - 1}{n(q-1)} \right\rfloor - 1 \tag{3}$$

for $n \ge 1$, was introduced, it being the maximum value of s for which an s-PD-set of size $s+1$ for the simplex codes can exist: see [6, Lemma 2]. This also allows for construction of the matrices N_i with the properties required in Proposition 2; a specific construction is given in [6, Lemma 5]:

Result 3. *For $n \ge 2$, $q \ge 2$ a prime power, let $K = \mathbb{F}_{q^n}$ and let ζ be a primitive element of K^*. For $0 \le i \le f_n(\mathbb{F}_q)$, if $B_i = \{\zeta^{j+in} \mid 0 \le j \le n-1\}$, then $\{B_i \mid 0 \le i \le f_n(\mathbb{F}_q)\}$ is a set of $f_n(\mathbb{F}_q)+1$ mutually disjoint bases for $V_n(\mathbb{F}_q)$.*

For our purposes we need matrices of size $(n-u)$, but the same construction holds. Each matrix N_i^{-1} has for its rows the field elements of a basis B_i expressed as vectors in $V_{n-u}(\mathbb{F}_q)$, and normalized. Thus we have:

Corollary 1. *For $n \ge 3$ and $1 \le u \le n-1$, q a prime power, the MacDonald code $C_{n,u}(q)$ has s-PD-sets of size $s+1$ for all s such that $1 \le s \le f_{n-u}(\mathbb{F}_q) = \left\lfloor \frac{q^{n-u}-1}{(n-u)(q-1)} \right\rfloor - 1$.*

Example 2. If $q = 3$ and $n-u = 3$ we have $f_3(\mathbb{F}_3) = 3$, and we use Result 3 to construct, with the computational help of Magma [3, 5], four normalized matrices, $I_3 = N_0^{-1}$ and N_i^{-1} for $1 \le i \le 3$, such that $\{\left[\begin{array}{c|c} N_i & 0 \\ \hline 0 & I_u \end{array}\right] \mid 0 \le i \le 3\}$ forms a 3-PD-set of minimal size 4 for $C_{n,n-3}(3)$, with the usual information set.

Thus we took $\mathbb{F}_{27}$ with primitive polynomial x^3+2x+1, primitive root ζ, and $B_0 = \{1, \zeta, \zeta^2\}$, $B_1 = \zeta^3 B_0$, $B_2 = \zeta^6 B_0$, $B_3 = \zeta^9 B_0$. Expressing these as vectors in $V_3(\mathbb{F}_3)$ and normalising gives the matrices:

$$I_3, N_1^{-1} = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix}, N_2^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 0 & 1 \end{bmatrix}, N_3^{-1} = \begin{bmatrix} 1 & 2 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix},$$

with inverses

$$I_3, N_1 = \begin{bmatrix} 0 & 1 & 1 \\ 2 & 1 & 1 \\ 2 & 0 & 1 \end{bmatrix}, N_2 = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{bmatrix}, N_3 = \begin{bmatrix} 1 & 0 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 2 \end{bmatrix}.$$

These matrices may now be used for decoding $C_{n,n-3}(3)$ for any $n \geq 4$, recalling of course that simple matrix multiplication will not give the automorphism here, so that the corresponding monomial matrices as described in Section 3 will need to be constructed to complete the decoding. ■

If $n-u$ is small it is not possible to find suitable matrices N_i, and in particular if $u = n-1$, or $n-2$, unless the field is large in the latter case. A different approach is needed here.

Proposition 3. *For $n \geq 4$, $3 \leq u \leq n-1$, q any prime, let $C_{n,u}(q)$ be the $[\frac{q^n-q^u}{q-1}, n, q^{n-1} - q^{u-1}]_q$ q-ary MacDonald code with information set $\mathcal{I}_{n,u}$ and check set $\mathcal{C}_{n,u}$. For fixed $k \geq 1$, let*

$$P_k = \{M_i = \left[\begin{array}{c|c} I_{n-u} & B_i \\ \hline 0 & I_u \end{array}\right] \mid 0 \leq i \leq k\}$$

where $B_i \in M_{n-u,u}(\mathbb{F}_q)$, with rows $r_{i,l}$ for $1 \leq l \leq n-u$, such that for any $i \neq j$:

$$\text{wt}(r_{i,l} - r_{j,m}) \geq 2 \textit{ for all } l, m \textit{ and } \text{wt}(r_{i,1} - r_{j,1}) \geq 3.$$

Then P_k is a k-PD-set of $k+1$ elements for $C_{n,u}(q)$ with information set $\mathcal{I}_{n,u}$. Furthermore, any subset of P_k of size $s+1$ where $1 \leq s \leq k$ is an s-PD-set for $C_{n,u}(q)$.

Proof: We proceed in the same way as in Proposition 2. Note first that $M_i^{-1} = \left[\begin{array}{c|c} I_{n-u} & -B_i \\ \hline 0 & I_u \end{array}\right]$ for $0 \leq i \leq k$ so the same set of conditions apply to the rows of $-B_i$. Let $T = \{v_1, \ldots, v_k\}$ be a set of k distinct vectors in $V_n(\mathbb{F}_q) \setminus U$. Suppose that we cannot map T into $\mathcal{C}_{n,u}$ by any element of P_k. Then for each i such that $0 \leq i \leq k$, there is a $v_j \in T$, for $1 \leq j \leq k$, such that $v_j M_i \in \mathcal{I}_{n,u}$. Since there are $k+1$ values of i but only k of j we must have $v_j M_i$ and $v_j M_l$, for some j, and $i \neq l$, both in $\mathcal{I}_{n,u}$. Suppose $v_j M_i = w_r$ and $v_j M_l = w_t$; then $v_j = w_r M_i^{-1} = w_t M_l^{-1}$. There are three cases to consider:
Case (1): $r, t \leq n-u$. Then $w_r = e_r$, $w_t = e_t$. Since the r^{th} and t^{th} rows of B_i and B_l are distinct, this is not possible.
Case (2): $r \leq n-u$ and $t > n-u$. So $w_r = e_1$ and $w_t = e_1 + e_t$. Thus $w_r M_i^{-1} = w_t M_l^{-1}$ becomes the r^{th} row of M_i^{-1} equal to the sum of the first and t^{th} rows of M_l^{-1}, which implies that $r_{i,r} - r_{l,1}$ has weight 1, which is not possible.
Case (3): $r, t > n-u$. Then we have $(e_1 + e_r)M_i^{-1} = (e_1 + e_t)M_l^{-1}$, and thus $r_{i,1} - r_{l,1}$ is a vector of weight at most 2, again not possible.

The last statement follows as before. ■

Note: (1) Since $\mathrm{wt}(r_{i,1} - r_{j,1}) \geq 3$ for $i \neq j$, we can, without loss of generality, take B_i to be the $(n-u) \times u$ matrix all of whose rows are $r_{i,1}$. We can thus search for $k+1$ vectors in $V_u(\mathbb{F}_q)$ such that any two are distance at least 3 apart.
(2) If $u = 2$ we must use the method of Proposition 2. This will yield some sets as long as $n > 3$. For $n = 3$ and $u = 2$ the q-ary code is a $[q^2, 3, q^2 - q]_q$ code and other methods could be employed.
(3) Since the matrices in this construction are all upper triangular, with 1's on the diagonal, they are in the permutation group of the code so the action on the coordinate positions is by direct multiplication.

Using the matrices B_i as defined in the first note above, we have:

Corollary 2. *Let $n \geq 4$, $3 \leq u \leq n-1$, any q. Let D be a set of vectors in $V_u(\mathbb{F}_q)$ which is such that any two members of D are distance at least 3 apart. Then the $|D|$ matrices B_i, for $1 \leq i \leq |D|$, where B_i is an $(n-u) \times u$ matrix with all rows the i^{th} vector from D, will give a set of $|D|$ automorphisms of $C_{n,u}(q)$ that form a $(|D|-1)$-PD-set using the information set $\mathcal{I}_{n,u}$.*

Note: A subspace of minimum weight at least 3 could serve as the set D. Methods for constructing codes with a prescribed minimum distance are given in [4] for the binary case, and [17] for the $q > 2$ case.

Example 3. For the code $C_{6,5}(3)$, a $[243, 6, 162]_3$ code, the construction of Proposition 3 yields the following nine matrices (using Magma) giving automorphisms of $C_{6,5}(3)$ that correct eight errors, using the information set $\mathcal{I}_{6,5}$.

$$P_8 = \{ \left[\begin{array}{c|c} 1 & c \\ \hline 0 & I_5 \end{array}\right] \mid c \in \langle (1,1,1,0,0), (2,1,0,1,0) \rangle \}$$

5 Conclusion

We include an appendix showing the best values for s for an s-PD-set of size $s+1$ that we have obtained for these MacDonald codes from these two constructions for some small set of values for n and q and $1 \leq u \leq n-1$. It can be seen that the second construction gives the better result when u is greater than $\lfloor \frac{n}{2} \rfloor$. It should be emphasised that we have used a specific information set, $\mathcal{I}_{n,u}$, and that other information sets might yield better results. Of course the set from Proposition 1 is independent of the information set but is rather large.

6 Appendix

In the tables to follow: for $C_{n,u}(q)$, q is a prime power, n, u as before, ℓ is the length of the code, mw is the minimum weight, t is the error correcting capability, gb is the Gordon-Schönheim bound for the size of the PD-set for full error correction, $s_1 = f_{n-u}$ (for the first construction), s_2 the computationally found value of s for the second construction when $u \geq 3$. Thus the size of the set is $s_1 + 1$, $s_2 + 1$, respectively.

Table 1: s-PD-sets of size $s+1$ for $C_{n,u}(q)$

q	n	u	ℓ	mw	t	gb	s_1	s_2
2	4	1	14	7	3	5	1	0
	4	2	12	6	2	3	0	0
	4	3	8	4	1	2	0	1
	5	1	30	15	7	11	2	0
	5	2	28	14	6	9	1	0
	5	3	24	12	5	8	0	1
	5	4	16	8	3	5	0	1
	6	1	62	31	15	25	5	0
	6	2	60	30	14	22	2	0
	6	3	56	28	13	21	1	1
	6	4	48	24	11	18	0	1
	6	5	32	16	7	13	0	3
	7	1	126	63	31	59	9	0
	7	2	124	62	30	55	5	0
	7	3	120	60	29	53	2	1
	7	4	112	56	27	48	1	1
	7	5	96	48	23	41	0	3
	7	6	64	32	15	29	0	7
	8	1	254	127	63	136	17	0
	8	2	252	126	62	132	9	0
	8	3	248	124	61	131	5	1
	8	4	240	120	59	127	2	1
	8	5	224	112	55	118	1	3
	8	6	192	96	47	102	0	7
	8	7	128	64	31	70	0	15
	9	1	510	255	127	328	30	0
	9	2	508	254	126	322	17	0
	9	3	504	252	125	320	9	1
	9	4	496	248	123	315	5	1
	9	5	480	240	119	302	2	3
	9	6	448	224	111	283	1	7
	9	7	384	192	95	243	0	15
	9	8	256	128	63	163	0	15
	10	1	1022	511	255	787	55	0
	10	2	1020	510	254	779	30	0
	10	3	1016	508	253	782	17	1
	10	4	1008	504	251	773	9	1
	10	5	992	496	247	762	5	3
	10	6	960	480	239	736	2	7
	10	7	896	448	223	691	1	15
	10	8	768	384	191	590	0	15
	10	9	512	256	127	396	0	31

q	n	u	ℓ	mw	t	gb	s_1	s_2
3	4	1	39	26	12	18	3	0
	4	2	36	24	11	16	1	0
	4	3	27	18	8	12	0	2
	5	1	120	80	39	68	9	0
	5	2	117	78	38	67	3	0
	5	3	108	72	35	61	1	2
	5	4	81	54	26	47	0	8
	6	1	363	242	120	267	23	0
	6	2	360	240	119	265	9	0
	6	3	351	234	116	260	3	2
	6	4	324	216	107	237	1	8
	6	5	243	162	80	181	0	8
	7	1	1092	728	363	1051	59	0
	7	2	1089	726	363	1044	23	0
	7	3	1080	729	359	1035	9	2
	7	4	1053	702	350	1010	3	8
	7	5	972	648	323	931	1	8
	7	6	729	486	242	700	0	23
	8	1	3279	2186	1092	4170	155	0
	8	2	3276	2184	1091	4159	59	0
	8	3	3267	2178	1088	4151	23	2
	8	4	3240	2160	1079	4118	9	8
	8	5	3159	2106	1052	4017	3	8
	8	6	2916	1944	971	3706	1	23
	8	7	2187	1458	728	2780	0	71
	9	1	9840	6560	3279	16740	409	0
	9	2	9837	6558	3278	16746	155	0
	9	3	9828	6552	3275	16723	59	2
	9	4	9801	6534	3266	16688	23	8
	9	5	9720	6480	3239	16536	9	8
	9	6	9477	6318	3158	16131	3	23
	9	7	8748	5832	2915	14881	1	71
	9	8	6561	4374	2186	11180	0	197
	10	1	29523	19682	9849	67894	1092	0
	10	2	29520	19680	9839	67885	409	0
	10	3	29511	19674	9836	67861	155	2
	10	4	29484	19656	9827	67783	59	8
	10	5	29403	19602	9800	67606	23	8
	10	6	29160	19440	9719	67040	9	23
	10	7	28431	18954	9476	65365	3	71
	10	8	26244	17496	8747	60334	1	197
	10	9	19683	13122	6560	45254	0	518

q	n	u	ℓ	mw	t	gb	s_1	s_2
4	4	1	84	63	31	51	6	0
	4	2	80	60	29	47	1	0
	4	3	64	48	23	37	0	3
	5	1	340	255	127	263	20	0
	5	2	336	252	125	258	6	0
	5	3	320	240	119	245	1	3
	5	4	256	192	95	196	0	15
	6	1	1364	1023	511	1430	67	0
	6	2	1360	1020	509	1420	20	0
	6	3	1344	1008	503	1406	6	3
	6	4	1280	960	479	1337	1	15
	6	5	1024	768	383	1072	0	63
	7	1	5460	4095	2047	7905	226	0
	7	2	5456	4092	2045	7894	67	0
	7	3	5440	4080	2039	7873	20	3
	7	4	5376	4032	2015	7775	6	15
	7	5	51207	3840	1919	7408	1	63
	7	6	4096	3072	1535	5932	0	63
	8	1	21844	16383	8191	44423	779	0
	8	2	21840	16380	8189	44396	226	0
	8	3	21824	16368	8183	44376	67	3
	8	4	21760	16320	8159	44245	20	15
	8	5	21504	16128	8063	43715	6	63
	8	6	20480	15360	7679	41641	1	63
	8	7	16384	12288	6143	33319	0	255
	9	1	87380	65535	32767	252567	2729	0
	9	2	87376	65532	32765	252536	779	0
	9	3	87360	65520	32759	252480	226	3
	9	4	87296	65472	32735	252300	67	15
	9	5	87040	765280	32639	251556	20	63
	9	6	86016	64512	32255	248597	6	63
	9	7	81920	61440	30719	236754	1	255
	9	8	65536	49152	24575	189409	0	1023
	10	1	349524	262143	131071	1451611	9708	0
	10	2	349520	262140	131069	1451557	2729	0
	10	3	349504	262128	131063	1451482	779	3
	10	4	349440	262080	131039	1451227	226	15
	10	5	349184	261888	130943	1450159	67	63
	10	6	348160	261120	130559	1445916	20	63
	10	7	344064	258048	129023	1428896	6	255
	10	8	327680	245760	122879	1360863	1	1023
	10	9	262144	196608	98303	1088719	0	4095

q	n	u	ℓ	mw	t	gb	s_1	s_2
5	4	1	155	124	61	104	9	0
	4	2	150	120	59	100	2	0
	4	3	125	100	49	84	0	4
	5	1	780	624	311	720	38	0
	5	2	775	620	309	718	9	0
	5	3	750	600	299	694	2	4
	5	4	625	500	249	581	0	16
	6	1	3905	3124	1561	5084	155	0
	6	2	3900	3120	1559	5074	38	0
	6	3	3875	3100	1549	5040	9	4
	6	4	3750	3000	1499	4877	2	16
	6	5	3125	2500	1249	4065	0	73
	7	1	19530	15624	7811	36509	650	0
	7	2	19525	15620	7809	36502	155	0
	7	3	19500	15600	7799	36457	38	4
	7	4	19375	15500	7749	36228	9	16
	7	5	18750	15000	7499	35055	2	73
	7	6	15625	12500	6249	29222	0	264
	8	1	97655	78124	39061	266388	2789	0
	8	2	97650	78120	39059	266379	650	0
	8	3	97625	78100	39049	266310	155	4
	8	4	97500	78000	38999	265959	38	16
	8	5	96875	77500	38749	264254	9	73
	8	6	93750	75000	374999	255748	2	264
	8	7	78125	62500	31249	213124	0	1112
	9	1	488280	390624	195311	1968014	12206	0
	9	2	488275	390620	195309	1967995	2789	0
	9	3	488250	390600	195299	1967896	650	4
	9	4	488125	390500	195249	1967389	155	16
	9	5	487500	390000	194999	1964873	38	73
	9	6	484375	387500	193749	1952282	9	264
	9	7	468750	375000	187499	1889299	2	1112
	9	8	390625	312500	156249	1574452	0	4694

References

[1] E. F. Assmus, Jr and J. D. Key, *Designs and their codes*, Cambridge: Cambridge University Press, 1992, Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[2] M.C. Bhandar and C.Durairajan, *A note on covering radius of MacDonald codes*, Proceedings of the International Conference on Information Technology: Computers and Communications (ITCC03) 0-7695-1916-4/03,IEEE, 2003.

[3] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24, 3/4** (1997), 235–265.

[4] Richard A. Brualdi and Vera S. Pless, *Greedy codes*, J. Combin. Theory, Ser. A **64** (1993), 10–30.

[5] J. Cannon, A. Steel, and G. White, *Linear codes over finite fields*, Handbook of Magma Functions (J. Cannon and W. Bosma, eds.), Computational Algebra Group, Department of Mathematics, University of Sydney, 2006, V2.13, http://magma.maths.usyd.edu.au/magma, pp. 3951–4023.

[6] Washiela Fish, Jennifer D. Key, and Eric Mwambene, *Partial permutation decoding for simplex codes*, Adv. Math. Commun. **6** (2012), 505–516.

[7] Daniel M. Gordon, *Minimal permutation sets for decoding the binary Golay codes*, IEEE Trans. Inform. Theory **28** (1982), 541–543.

[8] W. Cary Huffman, *Codes and groups*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), Amsterdam: Elsevier, 1998, Volume 2, Part 2, Chapter 17, pp. 1345–1440.

[9] J. D. Key, T. P. McDonough, and V. C. Mavron, *Partial permutation decoding for codes from finite planes*, European J. Combin. **26** (2005), 665–682.

[10] ______, *Information sets and partial permutation decoding for codes from finite geometries*, Finite Fields Appl. **12** (2006), 232–247.

[11] Hans-Joachim Kroll and Rita Vincenti, *PD-sets related to the codes of some classical varieties*, Discrete Math. **301** (2005), 89–105.

[12] J.E. MacDonald, *Design methods for maximum minimum-distance error-correcting codes*, IBM J. Res. and Develop. **4** (1960), 43–57.

[13] F. J. MacWilliams, *Permutation decoding of systematic codes*, Bell System Tech. J. **43** (1964), 485–505.

[14] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, Amsterdam: North-Holland, 1983.

[15] A. M. Patel, *Maximal q-ary linear codes with large minimum distance*, IEEE Trans. Inform. Theory **21** (1975), 106–110.

[16] J. Schönheim, *On coverings*, Pacific J. Math. **14** (1964), 1405–1411.

[17] A. J. van Zanten and I. Nengah Suparta, *On the construction of linear q-ary lexicodes*, Des. Codes Cryptogr. **37 (1)** (2005), 1529.