s-Elusive codes in Hamming graphs

Daniel R. Hawtin

Received: 7 July 2020 / Revised: 20 December 2020 / Accepted: 13 March 2021 / Published online: 6 April 2021
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract
A code is a subset of the vertex set of a Hamming graph. The set of s-neighbours of a code is the set of all vertices at Hamming distance s from their nearest codeword. A code \(C\) is s-elusive if there exists a distinct code \(C'\) that is equivalent to \(C\) under the full automorphism group of the Hamming graph such that \(C\) and \(C'\) have the same set of s-neighbours. We show that the minimum distance of an s-elusive code is at most \(2s + 2\), and that an s-elusive code with minimum distance at least \(2s + 1\) gives rise to a \(q\)-ary \(t\)-design with certain parameters. This leads to the construction of: an infinite family of 1-elusive and completely transitive codes, an infinite family of 2-elusive codes, and a single example of a 3-elusive code. Answers to several open questions on elusive codes are also provided.

Keywords Elusive codes · Completely transitive codes · Automorphism groups · Hamming graph

Mathematics Subject Classification 05E18 · 94B60 · 05B05

1 Introduction
A code in a Hamming graph \(\Gamma = H(m, q)\) is a subset \(C\) of its vertex set \(V\Gamma\). The elements of \(C\) are called codewords and the automorphism group of \(C\) is the setwise stabiliser of \(C\) in the full automorphism group of \(H(m, q)\). An s-neighbour of \(C\) is a vertex \(\alpha\) whose nearest codeword in \(C\) is Hamming distance \(s\) from \(\alpha\). A code \(C\) is called s-elusive if there exists an equivalent code \(C'\) to \(C\) such that the sets of s-neighbours of \(C\) and \(C'\) are the same. Note that the notion of equivalence used here is more general than the standard one; see Sect. 2.
The concept studied here is a generalisation of one originally studied in [16]. We consider the question of whether, given a code \( C \) in a Hamming graph \( H(m, q) \), the automorphism group \( \text{Aut}(C_s) \) of the set \( C_s \) of \( s \)-neighbours could be larger than the automorphism group \( \text{Aut}(C) \) of the code itself (see Sect. 2). This question was encountered, for \( s = 1 \), when Gillespie and Praeger were deciding upon the definition for a neighbour-transitive code (see [11]). In [16] they give an affirmative answer via the construction of an infinite family of examples. Similarly, the significance of the existence of \( s \)-elusive codes relates to the precise definition of \( s \)-neighbour-transitive codes (see [12,13,15,19]).

Theorem 1.1 exhibits examples of \( s \)-elusive codes, for \( s = 1, 2 \) and 3. The definition of the relevant Reed–Muller codes is given at the beginning of Sect. 4, and can be found for instance in [1, Sect. 5.4]; the definition of the Preparata codes can be found in [7, (16.12)]. Part 1 of Theorem 1.1 is proved in Sect. 4 and the remaining parts in Sect. 5. Note that a code \( C \) is completely transitive if each \( C_i \), for \( i \in \{0, \ldots, \rho\} \), is an \( \text{Aut}(C) \)-orbit, where \( \rho \) is the covering radius of \( C \) (see, for instance, [17]), and we say that a linear code \( C \) of length \( m \), dimension \( \ell \) and minimum distance \( \delta \) has parameters \([m, \ell, \delta]\). Note also that the result that \( \mathcal{R}M_q(k, d) \) is completely transitive is new.

Theorem 1.1 1. The Reed–Muller codes \( \mathcal{R}M_q(k, d) \), where \( q \) is a prime power and \( k = (q - 1)d - 2 \), are completely transitive and \( 1 \)-elusive with parameters \([q^d, q^d - d - 1, \delta]\) where \( \delta = 4 \) when \( q = 2 \) and \( \delta = 3 \) otherwise.
2. The Preparata codes \( \mathcal{P}(2d) \) in \( H(2^{2d}, 2) \) (which are non-linear) are \( 2 \)-elusive with minimum distance \( \delta = 6 \) and size \( 2^{2^{2d} - 4d} \).
3. The punctured code of the even weight subcode of the perfect binary Golay code is \( 3 \)-elusive with parameters \([22, 11, 7]\).

For a code \( C \) to be \( s \)-elusive, there must be an automorphism \( x \in \text{Aut}(C_s) \setminus \text{Aut}(C) \). It follows that \( C^x \) and \( C \) are not equal, but are equivalent codes, each with the same \( s \)-neighbour set \( C_s \). As such, given knowledge only of the \( s \)-neighbour set and minimum distance of an \( s \)-elusive code, knowledge of the code itself remains elusive. In many results below it is assumed that \( \delta \geq 2s + 1 \). If an \( s \)-elusive code \( C \) has minimum distance \( \delta \geq 2s + 1 \) then each element of \( C_s \) is distance \( s \) from a unique codeword. Thus, the assumption that \( \delta \geq 2s + 1 \) is a way of ensuring that \( C \) is minimal, in the sense that \( C \) contains no proper \( s \)-elusive code. This assumption avoids certain technicalities and makes it possible to prove some interesting results.

The property of being \( s \)-elusive seems to be related to the minimum distance \( \delta \) of the code, namely the smallest distance between two distinct codewords. In [16] it is shown that (i) if \( C \) is a \( 1 \)-elusive code then it has minimum distance \( \delta \leq 4 \), (ii) if \( C \) is a \( 1 \)-elusive code with \( \delta = 4 \) then \( q = 2 \), and (iii) an infinite family of binary \( 1 \)-elusive codes with \( \delta = 4 \) exists. Theorems 5.6 and 5.7 together generalise [16, Theorem 1], showing that the minimum distance of an \( s \)-elusive code is at most \( 2s + 2 \), and that any \( s \)-elusive code with minimum distance at least \( 2s + 1 \) has a set of \( q \)-ary \( s \)-(\( m, 2s, 1 \)) designs associated to it. Note that the latter fact allowed for the identification of those codes in Parts 2 and 3 of Theorem 1.1.

Codes with regularity properties often give rise to designs. For instance, [3, Theorem 2] states that the set of all weight \( k \) codewords of a completely regular code having minimum distance \( \delta \) in \( H(m, q) \) form a \( q \)-ary \( \left[ \frac{n}{k} \right] -(m, k, \lambda_k) \) design, for some integer \( \lambda_k \) (see [3] for more on completely regular codes). Below we discuss the fact that each code appearing in Theorem 1.1 is in fact completely regular and compare design parameters from [3, Theorem 2] and Theorem 5.6. Note each \( s \)-elusive example \( C \) in fact has covering radius \( 2s \) and the code \( C \cup C_{2s} \) (which also happen to be completely regular in each case) has the same \( s \)-neighbour set as \( C \); this idea is used implicitly in the proofs that the codes in Theorem 1.1 are \( s \)-elusive.
1. If $C = \mathcal{R}M_q(k, d)$, where $k = (q - 1)d - 2$, then Theorem 1.1 shows that $C$ is completely transitive, and hence completely regular. The minimum weight codewords form a $q$-ary $1$-(q^d, 3, 1) design when $q \geq 3$, or a $2$-(2^d, 4, 2^{d-1} - 1) design when $q = 2$ (via Eqs. (4.1) and (4.2)). The dual of the repetition code turns out to be $C \cup C_{2x}$, has the same $1$-neighbour set $C_1$ as $C$ (see Lemma 4.3), and its minimum weight codewords form a $q$-ary $1$-(q^d, 2, q^d - 1) design. Compare this with the $q$-ary $1$-(q^d, 2, 1) design arising from $C$ under Theorem 5.6.

2. Let $C = \mathcal{P}(2d)$. Then $C$ is shown to be completely regular in [21], and the minimum weight codewords of $C$ form a $3$-(2^d, 6, (2^d - 4)/3) design (see [7, Example 16.19]). The Reed–Muller code $\mathcal{R}M_2(2d - 2, 2d)$ is then $C \cup C_{2x}$, has the same 2-neighbour set as $C$ (see the proof of Proposition 5.8), and the minimum weight codewords of $\mathcal{R}M_2(2d - 2, 2d)$ form a $2$-(2^d, 4, 2^{d-1} - 1) design. Compare with Theorem 5.6, under which $C$ gives rise to a $2$-(2^d, 4, 1) design.

3. Let $C$ be the punctured code of the even weight subcode of the perfect binary Golay code. Then $C$ is completely regular (see [3, Sect.5 (S.6)]) and the minimum weight codewords of $C$ form a $3$-(22, 7, 4) design. Moreover, $C \cup C_{2x}$ is the punctured code of the perfect binary Golay code, which is also completely regular (see [3, Sect. 5 (S.5)]) and has the same 3-neighbour set as $C$ (see the proof of Proposition 5.10). The minimum weight codewords of $C \cup C_{2x}$ form a $3$-(22, 6, 1) design, which, in this case, is indeed the design corresponding to Theorem 5.6.

In [18], for each $q \geq 3$, an infinite family of $1$-elusive codes with $\delta = 3$ in $H(m, q)$ was constructed. It was observed in that paper that for all known examples the length $m$ of the code is divisible by the alphabet size $q$. In [18, Question 1.3] it was asked whether this was true in general. This does indeed hold in the binary case, by [16, Theorem 1], since $q = 2$ implies that $m(q - 1) = m$ must be even, regardless of $\delta$. The author thanks Andries Brouwer for sending in private correspondence [4] the basis of the beautiful argument contained in Sect.3. This argument shows that the answer to the question is positive, that is, for a $1$-elusive code to exist in $H(m, q)$ it must be that $q$ divides $m$. This generalises and simplifies [14, Theorem 1.2] in the unpublished manuscript of the author.

The family $\mathcal{R}M_q(k, d)$ of $1$-elusive codes, as in Part 1 of Theorem 1.1, provides answers to further questions raised in [18].

1. In that paper there are only two images of each example code $C$ under $\text{Aut}(C_1)$; [18, Question 1.4] asks if this is always the case.

2. A code $C$ is neighbour-transitive if each of the sets $C$ and $C_1$ are $\text{Aut}(C)$-orbits. In [18, Question 1.5] it is asked whether the images under $\text{Aut}(C_1)$ of a $1$-elusive and neighbour-transitive code $C$ must be pairwise disjoint.

**Theorem 1.2** Let $C = \mathcal{R}M_q(k, d)$, where $k = (q - 1)d - 2$ as in Part 1 of Theorem 1.1. If $q$ is a power of the prime $p$ then:

1. there are at least $p$ distinct images of $C$ under $\text{Aut}(C_1)$; and,
2. there exists some $x \in \text{Aut}(C_1) \setminus \text{Aut}(C)$ such that $\mathcal{O} \in C \cap C^x$.

It is of note that studying the $s$-neighbour set of a code, usually when $s$ equals the covering radius $\rho$, arises in cryptography. Bent functions are functions with “maximal non-linearity”, which turns out to be the same as being a vertex in $H(q^d, q)$ at distance $\rho$ from the first order Reed–Muller code $\mathcal{R}M_q(1, d)$; see [20, Chap. 14, Sect. 5], or [8, 22] for extensions of this concept.

The next section introduces some notation, Sect. 3 answers [18, Question 1.3], before Sects. 4 and 5 provide the proof of Theorem 1.1.
2 Preliminaries

Let the two sets $M$ and $Q$ have sizes $m$ and $q$ respectively. For any set $S$ with $0 \in S$ write $S^x = S \setminus \{0\}$. The vertex set of the Hamming graph $\Gamma = H(m, q)$ consists of all $m$-tuples with entries labelled by the set $M$ and taken from the set $Q$. An edge exists between two vertices if they differ as $m$-tuples in exactly one position. For vertices $\alpha, \beta \in \Gamma$ the Hamming distance $d(\alpha, \beta)$ (that is the distance in $\Gamma$) is the number of entries in which $\alpha$ and $\beta$ differ.

For any vertex $\alpha \in \Gamma$, the set of $r$-neighbours of $\alpha$ is $\Gamma_r(\alpha) = \{\beta \in \Gamma \mid d(\alpha, \beta) = r\}$. The set of entries in which $\alpha, \beta \in \Gamma$ differ is $\text{diff}(\alpha, \beta) = \{i \in M \mid \alpha_i \neq \beta_i\}$.

Let $C$ be a code in $H(m, q)$. Then the minimum distance $d$ of $C$ is

$$d = \min\{d(\alpha, \beta) \mid \alpha, \beta \in C, \alpha \neq \beta\}$$

If $0 \in Q$ then the weight $\text{wt}(\alpha)$ of a vertex $\alpha$ of $H(m, q)$ is the number of non-zero entries of $\alpha$, that is, $\text{wt}(\alpha) = d(\alpha, 0)$. For a vertex $\alpha$ of $\Gamma$, define $d(\alpha, C) = \min\{d(\alpha, \beta) \mid \beta \in C\}$. Then the covering radius $\rho = \max\{d(\alpha, C) \mid \alpha \in \Gamma\}$. As in Sect. 1, for any $r \leq \rho$ let $C_r = \{\alpha \in \Gamma \mid d(\alpha, C) = r\}$. Note that if $\delta \geq 2r$, then the set of $r$-neighbours $C_r$ of the code $C$ satisfies $C_r = \bigcup_{\alpha \in C} \Gamma_r(\alpha)$ and if $\delta \geq 2r + 1$ this is a disjoint union.

The repetition code $\text{Rep}(m, q)$ in $H(m, q)$ is the code consisting of all $m$-tuples $(a, \ldots, a)$ where $a \in Q$. A code $C$ is linear if $Q \cong \mathbb{F}_q$ and $C$ is a subspace of the vertex set $V \Gamma \cong \mathbb{F}_q^m$. If $C$ is a linear code then $\text{Aut}(C)$ contains the subgroup $T_C$ consisting of all translations $t_{\alpha}$, where $\alpha \in C$, defined by $\beta \mapsto \alpha + \beta$ for all $\beta \in V \Gamma$. We denote the dual of a linear code $C$ under the standard inner product by $C^\perp$. The code $\text{Rep}(m, 2)$ in $H(m, 2)$ is linear and its dual $\text{Rep}(m, 2)^\perp$ is the code consisting of all vertices of even weight. The even-weight subcode of any code $C$ in $H(m, 2)$ is given by $C \cap \text{Rep}(m, 2)^\perp$.

Let $S_n$ denote the symmetric group on $\{1, \ldots, n\}$. The automorphism group $\text{Aut}(\Gamma)$ of the Hamming graph is the semi-direct product $B \rtimes L$, where $B \cong S_q^m$ and $L \cong S_m$ (see [5, Theorem 9.2.1]). Let $g = (g_1, \ldots, g_m) \in B, \sigma \in L$ and $\alpha = (\alpha_1, \ldots, \alpha_m) \in \Gamma$. Then $g$ and $\sigma$ act on $\alpha \in \Gamma$ as follows:

$$\alpha^g = (\alpha_1^g, \ldots, \alpha_m^g) \quad \text{and} \quad \alpha^\sigma = (\alpha_{\sigma^{-1}}^1, \ldots, \alpha_{\sigma^{-1}}^m).$$

The automorphism group of a code $C$ in $\Gamma = H(m, q)$ is $\text{Aut}(C) = \text{Aut}(\Gamma)_C$, the setwise stabiliser of $C$ in $\text{Aut}(\Gamma)$. The group of pure permutations on entries is $\text{PermAut}(C) = \text{Aut}(C) \cap L$. This notation will be used for any subset of vertices, in particular the automorphism group of the set of $r$-neighbours of $C$ is $\text{Aut}(C_r) = \text{Aut}(\Gamma)_{C_r}$.

Two codes, $C$ and $C'$, in $H(m, q)$, are equivalent if there exists $x \in \text{Aut}(\Gamma)$ such that $C^x = C'$. Equivalence preserves minimum distance. (See [16, Lemma 4]).

3 Alphabet size divides length

The adjacency matrix of a graph has rows and columns indexed by the vertices of the graph, with an entry $1 \in \mathbb{R}$ if the corresponding vertices are adjacent and $0 \in \mathbb{R}$ otherwise. Let $A$ be the adjacency matrix of the Hamming graph. A subset of the vertex set of a graph, and hence a code $C$, can be represented by a characteristic vector $\chi(C)$, where the entries are labelled by the vertices of the graph and take the value $1 \in \mathbb{R}$ if the vertex is in $C$ and $0 \in \mathbb{R}$ otherwise. It follows that $A \cdot \chi(C)$ is related to the characteristic vector of $C_1$, the entry of $A \cdot \chi(C)$ corresponding to the vertex $\beta$ takes the value $|\Gamma_1(\beta) \cap C|$. In particular, if $\delta \geq 3$ then each element of $C_1$ is distance 1 from a unique codeword, and hence $A \cdot \chi(C) = \chi(C_1)$. 

© Springer
Proposition 3.1 Suppose that there exist distinct codes $C$ and $C'$ in $H(m, q)$ such that $C_1 = C_1'$, with both $C$ and $C'$ having minimum distance at least 3. Then $q$ divides $m$.

Proof (Argument as in [4]) Let $A$ be the adjacency matrix of the Hamming graph $H(m, q)$ and let $u = \chi(C)$, $v = \chi(C')$. Since both $C$ and $C'$ have minimum distance at least 3, it follows (from the discussion immediately preceding this result) that $Au = \chi(C_1) = \chi(C_1') = Av$. Since $u \neq v$, it follows that $A$ is singular and has at least one zero eigenvalue. The Hamming graph is the Cartesian product of $m$ copies of the complete graph $K_q$ on $q$ vertices. Thus, by [9, Theorem 2.3.4] and the fact that the eigenvalues of $K_q$ are $-1$ and $q-1$, the Hamming graph has eigenvalues $(m-i)(q-1)-i = (q-1)m-iq$, where $0 \leq i \leq m$. Since $A$ has an eigenvalue zero this implies $(q-1)m-iq = 0$, for some integer $i$, and hence $q \mid m$. \hfill \Box

Corollary 3.2 Let $C$ be a 1-elusive code in $H(m, q)$ with $\delta \geq 3$. Then $q$ divides $m$.

Proof If $C$ is a 1-elusive code, then there exists $x \in \text{Aut}(C_1) \setminus \text{Aut}(C)$ such that $C^x \neq C$ but $C^x_1 = C_1$. Hence, since $\delta \geq 3$, Proposition 3.1 applies with $C' = C^x$. \hfill \Box

4 Elusive Reed–Muller codes

This section concerns Part 1 of Theorem 1.1, that is, we give an infinite family of 1-elusive and completely transitive codes. Each code is the dual of a first order $q$-ary Reed–Muller code and is contained in the dual of the repetition code of the respective length.

Fix the following notation throughout this section. Let $q$ be a prime power, $Q = \mathbb{F}_q$ and $M = \mathbb{F}_q^d$, so that $V\Gamma$ is an $\mathbb{F}_q$-vector space. For $\alpha \in V\Gamma$, consider the following equations:

\[ \sum_{v \in M} \alpha_v = 0, \quad \text{and}, \]

\[ \sum_{v \in M} \alpha_v v = 0. \]  

Moreover, fix $k = (q-1)d - 2$, as well as:

\[ C = \mathcal{R.M}_q(k, d) \quad \text{and} \quad C' = \mathcal{R.M}_q(k+1, d) = \text{Rep}(q^d, q)^\perp, \]

in $H(q^d, q)$ (where $\text{Rep}(q^d, q)^\perp$ is the dual of the repetition code). The significance of (4.1) and (4.2) is that $\alpha \in C'$ if and only if $\alpha$ satisfies (4.1), and $\alpha \in C$ if and only if $\alpha$ satisfies both equations (4.1) and (4.2) (see [1, Sect. 5.4]).

The next lemma shows some well-known facts about $C'$, the dual of the repetition code. As the author was unable to find an exact reference, a short proof is included.

Lemma 4.1 The code $C'$ is a linear $[q^d, q^d-1, 2]$ code with covering radius $\rho' = 1$ and $|C'_1| = (q-1)q^{d-1}$.

Proof If $\alpha \in \Gamma^1(0)$ then $\alpha$ does not satisfy the equation (4.1). However, if $\alpha$ is a vertex in $H(m, q)$ and $i, j \in M$ such that $i \neq j$, $\alpha_i = -\alpha_j \neq 0$ but $\alpha_k = 0$ for all $k \neq i, j$ then $\alpha$ does satisfy equation (4.1). Hence $C'$ minimum distance 2. The code $C'$ is the dual of the repetition code, and the repetition code is a linear code with dimension 1, and hence $C'$ has dimension $q^d - 1$. Any non-zero codeword of the repetition code has weight $m$, and hence it follows from [3, Theorem 3] that the covering radius of $C'$ is 1. \hfill \Box

The next result also gathers together some well-known facts.

\begin{figure}[h]
Lemma 4.2  The code \( C \) is a linear \([q^d, q^d - (d + 1), \delta]\) code with covering radius \( \rho = 2 \), where

\[
\delta = \begin{cases} 
4 & \text{if } q = 2, d \geq 2, \\
3 & \text{if } q \geq 3, d \geq 1.
\end{cases}
\]

Proof  The minimum distances follow from [1, Corollary 5.5.4]. The code \( C \) is the dual of \( \mathcal{R}_q \mathcal{M}_q(1, d) \), which has dimension \( d + 1 \) (see [1, Example 5.4.3 (1)]). Moreover, \( \mathcal{R}_q \mathcal{M}_q(1, d) \) is the two-weight code see (see [6]) arising from the projective \((q^d, d + 1, q^{d-1}, 0)\) set associated to the affine plane \( \text{AG}_d(2) \); (see [6, Theorem 3.1]). Hence, by [3, Theorem 3], the covering radius of \( C \) is 2. \( \square \)

Lemma 4.3  The sets \( C_1 \) and \( C'_1 \) of neighbours of \( C \) and \( C' \) satisfy \( C_1 = C'_1 \).

Proof  By Lemma 4.2, \(|C| = q^{q^d-(d+1)}\). Since \( \delta' = 2 \) and \( C \subset C' \) it follows that \( C_1 \subseteq C'_1 \). Also, since \( \delta \geq 3 \), \(|C_1| = m(q - 1)|C| = q^d(q - 1)q^{q^d-(d+1)} = q^{d^2} - q^{d-1} \), and thus \( C_1 = C'_1 \) by Lemma 4.1. \( \square \)

Lemma 4.4  The Reed–Muller code \( \mathcal{C} = \mathcal{R}_q \mathcal{M}_q(k, d) \) is a 1-elusive code.

Proof  By Lemma 4.3, \( C_1 = C'_1 \), and, by Lemma 4.1, \( V \Gamma = C' \cup C' \). Hence \( \text{Aut}(C_1) = \text{Aut}(C') \). Since \( C' \) is linear, \( \text{Aut}(C_1) = \text{Aut}(C') \) contains the translation \( t_\alpha \) by the vertex \( \alpha \) for each \( \alpha \in C' \). If \( \alpha \in C' \setminus C \) then \( t_\alpha \) does not fix \( C \) setwise, so \( t_\alpha \notin \text{Aut}(C) \), and hence the image \( C'^\alpha \neq C \), so \( C \) is 1-elusive. \( \square \)

Recall from Sect. 2 that \( \text{PermAut}(C) = \text{Aut}(C) \cap L \) is the group of pure permutations on entries fixing the code \( C \). By [2, Theorem 5], \( \text{PermAut}(C) \cong \text{AGL}(d, q) \). Since \( C' \) is the dual of the repetition code in \( H(m, q) \), it follows that \( \text{PermAut}(\mathcal{R}_q \mathcal{M}_q(k + 1, d)) \cong S_m \).

The proof of Theorem 1.2 is below, which provides answers to two open questions regarding elusive codes.

Proof of Theorem 1.2  If \( p \) is the characteristic of the field \( \mathbb{F}_q \), then any non-trivial translation in \( \text{Aut}(C_1) \) has order \( p \). As in the proof of Lemma 4.4 there is a translation in \( \text{Aut}(C_1) \setminus \text{Aut}(C) \), so there are at least \( p \) distinct images of \( C \) under elements of \( \text{Aut}(C_1) \). This proves part 1. Note also that \( \sigma \in \text{Aut}(C') \) for any \( \sigma \in \text{Sym}(M) \), where \( \sigma \) acts by permuting entries. However, by [2, Theorem 5], \( \sigma \in \text{PermAut}(C) \) if and only if \( \sigma \in \text{AGL}(d, q) \). Thus if \( \sigma \in \text{Sym}(M) \setminus \text{AGL}(d, q) \), then \( C^\sigma \neq C \). However \( \emptyset \in C^\sigma \cap C \), proving part 2. \( \square \)

Lemma 4.5  The Reed–Muller code \( \mathcal{C} = \mathcal{R}_q \mathcal{M}_q(k, d) \) is \( \text{Aut}(C) \)-completely transitive.

Proof  Since \( C \) is linear, \( \text{Aut}(C) \) is transitive on \( C \). By Lemma 4.2, \( C \) has covering radius 2, so it remains to prove that \( \text{Aut}(C) \) acts transitively on \( C_1 \) and \( C_2 \). Since \( \delta \geq 3 \), \( \emptyset \in C \) and \( \text{Aut}(C) \) is transitive on \( C \), to prove that \( \text{Aut}(C) \) is transitive on \( C_1 \) it is sufficient to prove \( \text{Aut}(C)_0 \) is transitive on the set of weight one vertices. Let \( v \) be the weight one vertex with \( v_i = a \in Q^\times \) for a unique \( i \in M \). By [2, Theorem 5], \( \text{PermAut}(\mathcal{R}_q \mathcal{M}_q(k, d)) \cong \text{AGL}(d, q) \) acting 2-transitively as pure permutations on entries. Since \( C \) is linear \( \text{Aut}(C) \) also contains a subgroup isomorphic to the multiplicative group \( \mathbb{F}_q^\times \) acting as scalar multiplication. Hence, multiplying by \( a^{-1} \) and then applying a permutation of the entries \( \sigma \in \text{Aut}(C) \) which maps \( i \) to \( 0 \in M \), will map \( v \) to the weight one vertex \( \mu \) with \( \mu_0 = 1 \).

We now prove \( \text{Aut}(C) \) is transitive on \( \Gamma_2(0) \cap C_2 \), which will complete the proof. Recall \( C' = \mathcal{R}_q \mathcal{M}_q(k + 1, d) \). Now \( \Gamma_2(0) \cap C_2 \) consists of the weight two vertices \( v \) with \( v_i = a \in \mathbb{F}_q^\times \)

\( \square \)

Springer
Let \( C \) be a code in \( H(m, q) \). Recall that \( C \) is s-elusive if \( \text{Aut}(C_s) \) is strictly larger than \( \text{Aut}(C) \). Note that for any \( x \in \text{Aut}(C_s) \) the code \( C^x \) is equivalent to \( C \), and thus has the same size and minimum distance, and has conjugate automorphism group.

**Lemma 5.1** Let \( C \) be an s-elusive code and \( x \in \text{Aut}(C_s) \). Then \( (C_s)^x = (C^x)_s = C_s \).

**Proof** Note that \( x \in \text{Aut}(C_s) \) and thus fixes \( C_s \) setwise, so it follows that \( (C_s)^x = C_s \). It remains to be shown that \( (C^x)_s = C_s \). Let \( v \in C_s \), be distance \( s \) from \( x \in C \). Note that \( C^x \) and \( C \) are equivalent codes, so that \( |(C^x)_s| = |C_s| \) and it suffices to show that \( v^x \in (C^x)_s \). We have that \( d(v^x, x^x) = s \) and hence \( d(v^x, C^x) < s \). Suppose that \( d(v^x, C^x) < s \), that is, there exists some \( \beta \in C^x \) such that \( d(v, \beta) < s \). Then \( d(v^{x^{-1}}, \beta^{x^{-1}}) < s \). However \( \beta^{x^{-1}} \in C \), which contradicts the fact that \( x \) fixes \( C_s \) setwise. Hence \( v \in (C^x)_s \) and thus \( (C^x)_s = C_s \). □

If \( C \) is an s-elusive code then there exists an automorphism \( x \in \text{Aut}(C_s) \setminus \text{Aut}(C) \). This implies that \( C^x \neq C \), so that there is some codeword \( \alpha \in C \) such that \( \alpha^x \notin C \).

**Definition 5.2** Let \( C \) be an s-elusive code in \( H(m, q) \), \( x \in \text{Aut}(C_s) \setminus \text{Aut}(C) \) and \( \alpha \in C \) such that \( \alpha^x \notin C \). Then we call the triple \( (C, \alpha, x) \) an s-elusive triple.

**Lemma 5.3** Let \( (C, \alpha, x) \) be an s-elusive triple in \( H(m, q) \) with \( C \) having minimum distance \( \delta \geq 2s + 1 \). Then for each \( v \in \Gamma_s(\alpha) \) there exists a unique \( \pi \in C_{2s} \cap \Gamma_{s}(v) \) such that \( \pi \in C^x \).

**Proof** Since \( \delta \geq 2s + 1 \), the union \( C_s = \cup_{\gamma \in C} \Gamma_s(\gamma) \) is disjoint. The codes \( C^x \) and \( C \) are equivalent and, by Lemma 5.1, \( C^x_s = C_s \). Thus each \( v \in C_s \) is distance \( s \) from some vertex \( \pi \) in \( C^x \). That is, if \( v \in \Gamma_s(\alpha) \) then there exists some vertex \( \pi \in \Gamma_s(v) \cap C^x \). Now, \( d(\alpha, \pi) \leq d(\alpha, v) + d(v, \pi) = 2s \) and hence \( \pi \notin C \) since \( \delta \geq 2s + 1 \). Moreover, this means \( \pi \in C_k \) for some \( k \) such that \( 1 \leq k \leq 2s \).

Suppose \( \pi \in C_k \), where \( 1 \leq k < 2s \). Then there exists \( \beta \in C \) such that \( \pi \in \Gamma_k(\beta) \). Recall that the union \( C_k = \cup_{\gamma \in C} \Gamma_k(\gamma) \) is disjoint. However, \( d(\beta, \pi) = k < 2s \) implies the existence of a vertex \( \mu \in \Gamma_k(\beta) \), and hence in \( C_s \), such that \( d(\pi, \mu) < s \), contradicting the fact that \( C^x_s = C_s \), by Lemma 5.1.

Suppose there exists \( \pi' \in \Gamma_k(v) \cap C^x \) such that \( \pi' \neq \pi \). Then \( \pi, \pi' \) are in the code \( C^x \) which is equivalent to \( C \). However \( d(\pi, \pi') \leq d(\pi, v) + d(v, \pi') = 2s \) contradicting \( \delta \geq 2s + 1 \). Thus \( \pi \) is unique. □
The next definition introduces the concept of a $q$-ary $t$-design, which helps to describe the structure of an $s$-elusive code. Designs arise in many other contexts, for instance when considering $s$-regular codes [10]. First the notion of covering a vertex is required.

**Definition 5.4** Let $0 \in Q$ and $v, \alpha \in H(m, q)$. The vertex $v$ is said to be covered by $\alpha$, if $v_i = \alpha_i$ for every $i \in M$ such that $v_i \neq 0$.

In other words $\alpha$ covers $v$ if each non-zero entry of $v$ agrees with the corresponding entry of $\alpha$.

**Definition 5.5** A $q$-ary $t$-$(m, k, \lambda)$ design consists of a subset $D \subseteq \Gamma_k(0)$ of weight $k$ vertices of $H(m, q)$ such that each vertex $v \in \Gamma_k(0)$ is covered by exactly $\lambda$ vertices of $D$. When $q = 2$, $D$ is simply a $t$-$(m, k, \lambda)$ design and if additionally $\lambda = 1$, $D$ is called an $S(t, k, m)$ Steiner system.

As discussed in the introduction, where Theorem 5.6 is compared with [3, Theorem 2], designs often arise in coding theory.

**Theorem 5.6** Let $(C, 0, x)$ be an $s$-elusive triple in $H(m, q)$ with $\delta \geq 2s + 1$. Then the set $\Gamma_2s(0) \cap C^x$ forms a $q$-ary $s$-$(m, 2s, 1)$ design. In particular, if $q = 2$, then $\Gamma_2s(0) \cap C^x$ forms an $S(s, 2s, m)$ Steiner system.

**Proof** By Lemma 5.3, every vertex of $\Gamma_s(0)$ is covered by a unique element of $\Gamma_2s(0) \cap C^x$, with respect to $0$ and thus the result follows. $\square$

This gives the following bound for the minimum distance of an $s$-elusive code.

**Theorem 5.7** Let $C$ be an $s$-elusive code in $H(m, q)$. Then
1. if $q = 2$ then $\delta \leq 2s + 2$, and,
2. if $q \geq 3$ then $\delta \leq 2s + 1$.

**Proof** If $\delta \leq 2s$, or $2s + 1 \geq m$, then the result holds trivially. Suppose $\delta \geq 2s + 1$ and $2s + 1 < m$. Now, there exists some $x \in \text{Aut}(C_s)$ and $\alpha \in C$ such that $\alpha^x \notin C$, where we may assume that $\alpha = 0$. Then, by Theorem 5.6, $\Gamma_2s(0) \cap C^x$ forms a $q$-ary $s$-$(m, 2s, 1)$ design $D$. Hence, for all $\mu \in \Gamma_s(0)$, there exists some $\beta \in \Gamma_2s(0) \cap C^x$ such that $\beta$ covers $\mu$.

Suppose that $q = 2$. Since $2s < m − 1$, it follows that there exists some $i \in M$ such that $\beta_i = 0$. Thus, there exists $v \in \Gamma_s(0)$ with $v_i = 1$ and $d(\mu, v) = 2$. Note that $\beta$ does not cover $v$. Hence, there exists some block $\gamma$ of $D$ covering $v$. It then follows from the triangle inequality that

$$d(\beta, \gamma) \leq d(\beta, \mu) + d(\mu, v) + d(v, \gamma) = 2s + 2.$$

As $\beta, \gamma \in C^x$, and $C^x$ is equivalent to $C$, this proves part 1.

Let $q \geq 3$. Choose $i \in M$ such that $\mu_i \neq 0$. Since $q \geq 3$, there exists an $a \in Q^x$ such that $\mu_i = a$. Let $v \in \Gamma_s(0)$ with $v_i = a$ and $v_j = \mu_j$ for $j \neq i$. Then $\beta$ does not cover $v$, so there exists a block $\gamma$ of $D$ covering $v$. It then follows from the triangle inequality that

$$d(\beta, \gamma) \leq d(\beta, \mu) + d(\mu, v) + d(v, \gamma) = 2s + 1.$$

Since $\beta, \gamma \in C^x$, and $C^x$ is equivalent to $C$, this proves part 2. $\square$

The Preparata codes are a family of binary codes of length $2^{2d}$ for each integer $d \geq 2$. In addition to satisfying equations (4.1) and (4.2), codewords of the Preparata codes satisfy one extra non-linear equation. For a full definition see [7, (16.12)], taking note that $\tilde{P}(\sigma)$ is denoted as $P(2d)$ here, with $\sigma$ arbitrary.
Proposition 5.8 The Preparata codes $\mathcal{P}(2d)$ are 2-elusive codes.

Proof Let $C = R\cdot M_2(2d - 2, 2d)$ and $\mathcal{P} = \mathcal{P}(2d)$. It suffices to prove that the 2-neighbour sets $\mathcal{P}_2$ and $C_2$ are equal and that $\mathcal{P}$ is properly contained in $C$. It then follows that $\text{Aut}(C)$ fixes $\mathcal{P}_2$ but not $\mathcal{P}$, since $\text{Aut}(C)$ contains the translations by any codeword. Thus $\mathcal{P}$ is 2-elusive.

First, [7, (16.12) (a) and (b)] gives $\mathcal{P} \subset C$. Since $\delta(C) = 4$ it follows that $\mathcal{P}_2 \subset C_2$. Now, by Lemma 4.2, $C$ has covering radius 2 and dimension $2^{2d} - 2d - 1$. Hence $H(2^{2d}, 2) = C \cup C_1 \cup C_2$. This gives

$$|C_2| = |H(2^{2d}, 2)| - |C| - |C_1| = 2^{2^{2d}} - 2^{2^{2d} - 2d - 1} - 2^{2^{2d} - 2d - 1} \cdot 2^{2d} = 2^{2^{2d} - 1} - 2^{2^{2d} - 2d - 1}.$$ 

Furthermore, by [7, (16.16)], $\mathcal{P}$ has minimum distance 6 so is properly contained in $C$. Since $|\mathcal{P}| = 2^{2^{2d} - 4d}$, this also gives,

$$|\mathcal{P}_2| = |\mathcal{P}| \left(\frac{m}{2}\right) (q - 1)^2 = 2^{2^{2d} - 4d} 2^{2d - 1} (2^{2d} - 1) = 2^{2^{2d} - 1} - 2^{2^{2d} - 2d - 1}.$$ 

\[\square\]

Corollary 5.9 Let $Q \in \mathcal{P}(2d)$ and $x \in \text{Aut}(C_2) \setminus \text{Aut}(C)$. Then $\Gamma_4(Q) \cap \mathcal{P}(2d)^x$ is an $S(2, 4, 2^{2d})$ Steiner system.

Proof This follows from Theorem 5.6 and Proposition 5.8. \[\square\]

There exists a 3-(22, 6, 1)-design, namely the Witt design $W_{22}$. This suggests an elusive code with these parameters may exist. Indeed, taking the even weight subcode of the binary perfect Golay code $G_{23}$ and puncturing the resulting code produces a 3-elusive code.

Proposition 5.10 Let $\mathcal{P}G$ and $\mathcal{E}G$ be the codes obtained by puncturing the binary perfect Golay code $G_{23}$ and the even weight subcode of the Golay code $G_{23}$, respectively. Then $\mathcal{P}G_3 = \mathcal{E}G_3$ and $\mathcal{E}G$ is 3-elusive with minimum distance $\delta = 7$.

Proof The code $G_{23}$ is a linear [23, 12, 7] code with covering radius 3, and $\text{PermAut}(G_{23})^M \cong M_{23}$ acts transitively on $M$. Thus, puncturing $G_{23}$ results in the linear [22, 12, 6] code $\mathcal{P}G$ with covering radius $\rho = 3$. The even weight subcode of $G_{23}$ is a linear [23, 11, 8] code, again with $M_{23}$ acting as pure permutations on entries, so puncturing results in the [22, 11, 7] code $\mathcal{E}G$.

Since $\mathcal{P}G$ has covering radius 3 and minimum distance 6 it follows that $V \Gamma = \mathcal{P}G \cup \mathcal{P}G_1 \cup \mathcal{P}G_2 \cup \mathcal{P}G_3$, where this union is disjoint. So,

$$|\mathcal{P}G_3| = |V \Gamma| - |\mathcal{P}G| - |\mathcal{P}G_1| - |\mathcal{P}G_2| = 2^{22} - 2^{12} - 2^{12} \cdot 22 - 2^{12} \cdot \frac{22 \cdot 21}{2} = 2^{12}(2^{10} - 1 - 22 - 11 \cdot 21) = 2^{13} \cdot 5 \cdot 7 \cdot 11.$$
The code $\mathcal{E}G$ has minimum distance 7, and hence $|\mathcal{E}G_3| = 2^{11} \cdot 22 \cdot 21 \cdot 20 / 6 = 2^{13} \cdot 5 \cdot 7 \cdot 11 = |PG_3|$. Since $PG$ is linear, any translation by a vertex in $PG \setminus \mathcal{E}G$ fixes $PG_3 = \mathcal{E}G_3$. However this automorphism is not an element of $\text{Aut}(\mathcal{E}G)$. □

Acknowledgements The author thanks Neil Gillespie, Cheryl Praeger and Andrea Švob for kindly reading drafts of this manuscript, and the anonymous referees for their very helpful comments.

References

1. Assmus Jr. E.F., Key J.D.: Designs and Their Codes, vol. 103. Cambridge Tracts in Math. Cambridge University Press, Cambridge (1994).
2. Berger T., Charpin P.: The automorphism group of generalized Reed-Muller codes. Discret. Math. 117(1), 1–17 (1993).
3. Borges J., Rifà J., Zinoviev V.A.: On completely regular codes. Probl. Inf. Transm. 55(1), 1–45 (2019).
4. Brouwer A.E.: Private communication (2014). Accepted April 10 2014.
5. Brouwer A.E., Cohen A.M., Neumaier A.: Distance-Regular Graphs, vol. 18. Springer, Berlin (1989).
6. Calderbank R., Kantor W.M.: The geometry of two-weight codes. Bull. Lond. Math. Soc. 18(2), 97–122 (1986).
7. Cameron P.J., van Lint J.H.: Designs, Graphs. Codes and Their Links. Cambridge University Press, Cambridge (1991).
8. Carlet C., Gaborit P.: Hyper-bent functions and cyclic codes. J. Comb. Theory Ser. A 113(3), 466–482 (2006).
9. Cvetkovic D., Rowlinson P., Simic S.: Eigenspaces of Graphs. Encyclopedia Math. Appl. Cambridge University Press, Cambridge (2008).
10. Delsarte P.: An Algebraic Approach to the Association Schemes of Coding Theory. Philips Research reports: Supplements. N. V. Philips’ Gloeilampenfabrieken (1973).
11. Gillespie N.I.: Neighbour transitivity on codes in Hamming graphs. Ph.D. thesis, The University of Western Australia, Perth, Australia (2011).
12. Gillespie N.I., Giudici M., Hawtin D.R., Praeger C.E.: Entry-faithful 2-neighbour transitive codes. Des. Codes Cryptogr. 79(3), 549–564 (2016). https://doi.org/10.1007/s10623-015-0069-3.
13. Gillespie N.I., Hawtin D.R.: Alphabet-almost-simple 2-neighbour-transitive codes. Ars Math. Contemp. 14(2), 345–357 (2017).
14. Gillespie N.I., Hawtin D.R., Praeger C.E.: The structure of elusive codes in Hamming graphs. Preprint (arXiv:1404.0950v1) (2014).
15. Gillespie N.I., Hawtin D.R., Praeger C.E.: 2-Neighbour-transitive codes with small blocks of imprimitivity. Electron. J. Comb. 27(1), 1–16 (2020).
16. Gillespie N.I., Praeger C.E.: Neighbour transitivity on codes in Hamming graphs. Des. Codes Cryptogr. 67(3), 385–393 (2013). https://doi.org/10.1007/s10623-012-9614-5.
17. Giudici M., Praeger C.E.: Completely transitive codes in Hamming graphs. Eur. J. Comb. 20(7), 647–662 (1999).
18. Hawtin D.R., Gillespie N.I., Praeger C.E.: Elusive codes in Hamming graphs. Bull. Aust. Math. Soc. 88, 286–296 (2013). https://doi.org/10.1017/S0004972713000051.
19. Hawtin D.R., Praeger C.E.: Minimal binary 2-neighbour-transitive codes. J. Comb. Theory Ser. A 171, (2020).
20. MacWilliams F.J., Sloane N.J.A.: The Theory of Error Correcting Codes. North-Holland Mathematical Library, North-Holland (1978).
21. Semakov N.V., Zinoviev V.A., Zaitsev G.V.: Uniformly packed codes. Probl. Inf. Transm. 7(1), 30–39 (1971).
22. Tokareva N.: Bent Functions: Results and Applications to Cryptography. Elsevier, Amsterdam (2015).

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

.springer