Discrete Mathematics xxx (xxxx) xxx

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Some codes in symmetric and linear groups

Holly M. Green, Martin W. Liebeck *

Department of Mathematics, Imperial College, London SW7 2BZ, UK

A R T I C L E   I N F O

Article history:
Received 29 July 2019
Received in revised form 14 October 2019
Accepted 29 October 2019
Available online xxxx

Keywords:
Codes
Cayley graphs
Symmetric groups
linear groups

A B S T R A C T

For a finite group G, a positive integer λ, and subsets X, Y of G, write $\lambda G = XY$ if the products xy ($x \in X, y \in Y$), cover G precisely λ times. Such a subset Y is called a code with respect to X, and when $\lambda = 1$ it is a perfect code in the Cayley graph Cay (G, X). In this paper we present various families of examples of such codes, with X closed under conjugation and Y a subgroup, in symmetric groups, and also in special linear groups $SL_2(q)$. We also propose conjectures about the existence of some much wider families.

1. Introduction

According to [2], a *perfect code* in a finite graph Γ is a set C of vertices such that every vertex of Γ is at distance at most 1 from a unique vertex in C. This generalizes the classical notion of a perfect t-error correcting code over an alphabet A of size q, which can be defined as a perfect code in the graph $H(n, q, t)$ defined as follows: the vertex set is A^n, and two vertices are joined if and only if their Hamming distance is at most t (i.e. they differ in at most t positions). Together with the observation that $H(n, q, t)$ is a Cayley graph of the group $(\mathbb{Z}/q\mathbb{Z})^n$, this leads naturally to the study of perfect codes in Cayley graphs [2].

If G is a finite group with a subset X not containing the identity, we define the Cayley graph Cay(G, X) to have vertex set G, with an edge from g to h if and only if $gh^{-1} \in X$. A subset Y of G is a perfect code in this graph if and only if every element of G can be written uniquely as a product xy with $x \in X$, $y \in Y$. More generally, following [4], for a positive integer λ and subsets X, Y of G we write

$$\lambda G = XY$$

to mean that for every element $g \in G$, there are precisely λ pairs $(x, y) \in X \times Y$ such that $g = xy$. We say that X and Y *divide* G. Such a subset Y is called a *code* with respect to X (it is of course a perfect code in the case where $\lambda = 1$). Such codes have attracted quite a bit of attention (see for example [1,2]), particularly in the case where the subset X is closed under conjugation. Some representation theory is developed in [1,4] to study this case, but there is something of a lack of examples in the literature. In this paper we present some families of examples of codes in symmetric and linear groups in which X is closed under conjugation and Y is a subgroup. These codes are not perfect, and indeed have rather large values of λ, but they exhibit some attractive features, and we make some conjectures about the existence of many further families.

* Corresponding author.
E-mail addresses: h.green.19@ucl.ac.uk (H.M. Green), m.liebeck@imperial.ac.uk (M.W. Liebeck).

https://doi.org/10.1016/j.disc.2019.111719
0012-365X/© 2019 Elsevier B.V. All rights reserved.

Our first result concerns the symmetric groups S_n. For $1 \le k \le \frac{1}{2}n$, let Y_k denote the subgroup $S_k \times S_{n-k}$ of S_n, where the factor S_k permutes the subset $\{1, \ldots, k\}$ and the factor S_{n-k} permutes the subset $\{k+1, \ldots, n\}$. We address the question: for which conjugacy classes X of S_n is it the case that

$$\lambda S_n = XY_k$$

for some λ? We answer this for $k \le 3$:

Theorem 1. *Let $k \le 3$ and $n > 2k$. Suppose $X = x^{S_n}$ is a conjugacy class in S_n.*

(i) *For $k = 1$ we have $\lambda S_n = XY_1$ if and only if x has exactly one fixed point.*
(ii) *For $k = 2$ we have $\lambda S_n = XY_2$ if and only if the cycle-type of x has exactly one fixed point and exactly one 2-cycle.*
(iii) *For $k = 3$ we have $\lambda S_n = XY_3$ if and only if the cycle-type of x has exactly one fixed point, exactly one 2-cycle, and no 3-cycles.*

In each case $\lambda = |x^{Y_k}|$, the size of the Y_k-conjugacy class of x (where x is taken to lie in Y_k).

Note that the equation $\lambda S_n = XY_k$ tells us that every left coset of Y_k contains precisely λ members of X (see Lemma 2.1(i)).

We have not been able to solve the problem for general k, but we propose a conjecture for the general case in Section 2 (see Conjecture 2.3).

Our other family of examples is for the special linear groups $SL_2(q)$. For q even, [4, Theorem 6] restricts the conjugation-closed subsets X that can possibly divide $SL_2(q)$. One possibility is that X is a conjugacy class of transvections (that is, conjugates of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$). Our next result shows that this class does indeed divide $SL_2(q)$ (for both even and odd q). Denote by B the Borel subgroup consisting of all upper triangular matrices.

Theorem 2. *Let $G = SL_2(q)$, let X be a conjugacy class of transvections in G and let B be a Borel subgroup. Then*

$$\lambda G = XB,$$

where $\lambda = (q-1)/(2, q-1)$.

At the end of Section 3 we conjecture some further examples for $SL_2(q)$.

2. Symmetric groups

In this section we prove two preliminary lemmas and then proceed to prove Theorem 1.

Lemma 2.1. *Let G be a finite group with a subgroup H.*

(i) *Let $\lambda \in \mathbb{N}$ and $X \subseteq G$. Then $\lambda G = XH$ if and only if $|gH \cap X| = \lambda$ for all $g \in G$.*
(ii) *Suppose $X = x^G$ is a conjugacy class of G with $x \in H$, and $\lambda G = XH$. Then*
  (a) *$x^G \cap H = x^H$,*
  (b) *$C_G(x) = C_H(x)$, and*
  (c) *$\lambda = |x^H|$.*

Proof. (i) Let $g \in G$. There are precisely λ pairs $(x, h) \in X \times H$ such that $xh = g$, and these pairs correspond bijectively with the elements $x = gh^{-1}$ of $gH \cap X$.

(ii) Suppose $X = x^G$ with $x \in H$ and $\lambda G = XH$. By (i) with $g = 1$, we have $\lambda = |H \cap X|$. On the other hand we have

$$\lambda = \frac{|H|\,|X|}{|G|} = \frac{|H|}{|C_G(x)|} \le \frac{|H|}{|C_H(x)|} = |x^H|.$$

Since $|H \cap X| \ge |x^H|$, equality must hold in the above, and all parts of (ii) follow. □

In the proof of Theorem 1 we will use the following elementary result about cosets and conjugacy class sizes.

Lemma 2.2. (i) *If $x \in S_n$ has cycle-type $(d_1^{k_1}, d_2^{k_2}, \ldots, d_t^{k_t})$, where the d_i are distinct, then*

$$|x^{S_n}| = \frac{n!}{k_1! \cdots k_t! d_1^{k_1} d_2^{k_2} \cdots d_t^{k_t}}.$$

(ii) *Let $Y_k = S_k \times S_{n-k}$ be the stabilizer in S_n of $\{1, \ldots .k\}$. Then for $g \in S_n$ the left coset*

$$gY_k = \{y \in S_n \mid y : \{1, \ldots, k\} \longrightarrow \{g(1), \ldots, g(k)\}\}.$$

Please cite this article as: H.M. Green and M.W. Liebeck, Some codes in symmetric and linear groups, Discrete Mathematics (2019) 111719, https://doi.org/10.1016/j.disc.2019.111719.

Proof of Theorem 1. (i) Suppose $k = 1$, so that $Y_1 = S_{n-1} < S_n$. Assume that $x \in S_n$ satisfies $\lambda S_n = XY_1$, where $X = x^{S_n}$, and let l be the number of fixed points of x. By Lemma 2.1(i) we have $\lambda = |X \cap Y_1|$, so $l \geq 1$ and we may take $x \in Y_1$. Also $C_{Y_1}(x) = C_{S_n}(x)$ by Lemma 2.1(ii), which implies that $l = 1$.

Conversely, assume that $x \in Y_1$ has a unique fixed point (namely, the point 1), and let $X = x^{S_n}$. Then x has cycle-type $(d_1^{k_1}, d_2^{k_2}, \ldots, d_s^{k_s}, 1)$, where the d_i are distinct and $d_i \geq 2$ for each i. By Lemma 2.1(i), to prove that $\lambda S_n = XY_1$ it suffices to show that $|gY_1 \cap X| = \lambda$ for all $g \in S_n$, where $\lambda = |x^{Y_1}|$. This is certainly the case if $g \in Y_1$, so suppose that $g(1) \neq 1$; without loss of generality we can take $g(1) = 2$. Then elements of $gY_1 \cap X$ have $(1, 2, \ldots)$ as a d_i-cycle for some i, and upon fixing an i there are $(n-2)\cdots(n-d_i+1)$ such cycles. It remains to count the number of elements of cycle-type $(d_1^{k_1}, \ldots, d_i^{k_i-1}, \ldots, d_s^{k_s}, 1)$ in S_{n-d_i} which is given by Lemma 2.2. Multiplying these contributions together and summing over i, we see that

$$|gY_1 \cap X| = \sum_{i=1}^{s}(n-2)\cdots(n-d_i+1)\frac{(n-d_i)!k_i d_i}{k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s} 1} = \frac{(n-1)!}{k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}} = |x^{Y_1}|,$$

as required.

(ii) Suppose $k = 2$, so that $Y_2 = S_2 \times S_{n-2} < S_n$. Assume that $x \in S_n$ satisfies $\lambda S_n = XY_2$, where $X = x^{S_n}$, and let the cycle-type of x be $(d_1^{k_1}, d_2^{k_2}, \ldots, d_s^{k_s}, 2^l, 1^m)$ with $d_i \geq 3$ for all i. We need to show that $(l, m) = (1, 1)$. As above we can take $x \in Y_2$. By Lemma 2.1(ii) we have $x^{S_n} \cap Y_2 = x^{Y_2}$ and $C_{S_n}(x) = C_{Y_2}(x)$. These facts force (l, m) to be one of $(1, 1)$, $(1, 0)$ and $(0, 2)$. We need to exclude the latter two possibilities.

Suppose that $(l, m) = (0, 2)$. We count elements of x^{S_n} in the coset gY_2, where $\{g(1), g(2)\} = \{1, 3\}$. Such elements either send $1 \mapsto 1, 2 \mapsto 3$ or $2 \mapsto 1 \mapsto 3$. The following table displays the number of elements in x^{S_n} mapping 1 and 2 as specified:

$1 \mapsto 1, 2 \mapsto 3$	$2 \mapsto 1 \mapsto 3$
$(2\,3\,\cdots)$ a d_i-cycle	$(2\,1\,3\,\cdots)$ a d_i-cycle
$\frac{(n-3)!k_i d_i}{k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}}$	$\frac{(n-3)!k_i d_i}{2k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}}$

Hence we see that

$$|gY_2 \cap x^{S_n}| = \frac{3}{2}\frac{\sum_1^s (n-3)!k_i d_i}{k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}} = \frac{3}{2}|x^{Y_2}|,$$

which contradicts Lemma 2.1(ii)(c).

Now suppose that $(l, m) = (1, 0)$. Again we count elements of x^{S_n} in the coset gY_2, where $\{g(1), g(2)\} = \{1, 3\}$. This time, such elements must send $2 \mapsto 1 \mapsto 3$, and we count as above to see that $|gY_2 \cap x^{S_n}| = \frac{1}{2}|x^{Y_2}|$, again contradicting Lemma 2.1(ii)(c). This completes the proof of the left to right implication in Theorem 1(ii).

For the converse, let $x \in Y_2$ have cycle-type $(d_1^{k_1}, d_2^{k_2}, \ldots, d_s^{k_s}, 2, 1)$, where $d_i \geq 3$ for each i, and let $X = x^{S_n}$. We need to show that $|gY_2 \cap X| = |x^{Y_2}|$ for all $g \in S_n$. There are three types of cosets gY_2 which will be considered separately.

Case 1. Let $\{g(1), g(2)\} = \{1, 2\}$. Here $g \in Y_2$ and $|gY_2 \cap X| = |Y_2 \cap X| = |x^{Y_2}|$, as required.

Case 2. Let $\{g(1), g(2)\} = \{1, 3\}$, so either $1 \mapsto 1$ and $2 \mapsto 3$ or $2 \mapsto 1 \mapsto 3$. In each case we consider in which cycles these elements could lie and count the number of such elements in X using Lemma 2.2. The details are displayed below.

$1 \mapsto 1, 2 \mapsto 3$		$2 \mapsto 1 \mapsto 3$
$(2\,3)$ a 2-cycle	$(2\,3\,\cdots)$ a d_i-cycle	$(2\,1\,3\,\cdots)$ a d_i-cycle
$\frac{(n-3)!}{k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}}$	$\frac{(n-3)!k_i d_i}{k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}}$	$\frac{(n-3)!k_i d_i}{2k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}}$

Summing over the relevant indices we obtain,

$$|gY_2 \cap X| = \frac{(n-3)!}{k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}} + 2\frac{(n-3)!\sum_{i=1}^s k_i d_i}{2k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}} = \frac{(n-2)!}{k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}} = |x^{Y_2}|.$$

Case 3. Finally, let $\{g(1), g(2)\} = \{3, 4\}$. The two mappings $\{1, 2\} \to \{g(1), g(2)\}$ give rise to identical arguments so assume that $1 \mapsto 3$ and $2 \mapsto 4$. Four possibilities occur according to which cycles contain 1, 3 and 2, 4; the results are contained in the table below.

A 2-cycle and a d_i-cycle	The same d_i-cycle	Different d_i-cycles	A d_i-cycle and a d_j-cycle, $i \neq j$
$\frac{2(n-4)!k_i d_i}{k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}}$	$\frac{(n-4)!k_i d_i(d_i-3)}{2k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}}$	$\frac{(n-4)!k_i(k_i-1)d_i^2}{2k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}}$	$\frac{(n-4)!k_i d_i k_j d_j}{2k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}}$

Summing over the relevant indices, and scaling by 2 to account for the mapping $1 \mapsto 4$ and $2 \mapsto 3$, we get the following desired expression

$$|gY_2 \cap X| = 2\left\{\frac{2(n-4)!\sum_{i=1}^{s} k_i d_i}{k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}} + \frac{(n-4)!\sum_{i=1}^{s} k_i d_i(d_i-3)}{2k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}} + \frac{(n-4)!\sum_{i=1}^{s} k_i(k_i-1)d_i^2}{2k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}} + \frac{(n-4)!\sum_{i\neq j} k_i d_i k_j d_j}{2k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}}\right\} = \frac{(n-2)!}{k_1!\cdots k_s! d_1^{k_1}\cdots d_s^{k_s}}.$$

This completes the proof of part (ii) of Theorem 1.

(iii) The proof of this follows exactly the same strategy as (ii). We leave the details to the reader.

This completes the proof of Theorem 1. □

We conclude this section with a conjecture for the general case of factorizations $\lambda S_n = XY_k$, where $Y_k = S_k \times S_{n-k}$ and $X = x^{S_n}$. Let x have cycle-type $(d_1^{k_1}, \ldots, d_t^{k_t})$. Lemma 2.1 tells us that if $\lambda S_n = XY_k$ then we must have $C_{S_n}(x) = C_{Y_k}(x)$ and also $x^{S_n} \cap Y_k = x^{Y_k}$. This means that there is a unique subset $I \subseteq \{1, \ldots, t\}$ such that $\sum_{i\in I} n_i d_i = k$ for some $1 \le n_i \le k_i$. We have amassed some computational data for various small values of n and k, and based on this, we conjecture that this subset I must be precisely the subset arising from the 2-adic expansion of k, as follows.

Conjecture 2.3. *Let $n > 2k$ and let j be such that $2^j \le k < 2^{j+1}$. Suppose $X = x^{S_n}$ is a conjugacy class in S_n. Then $\lambda S_n = XY_k$ if and only if the cycle-type of x has exactly one cycle of length 2^i for $0 \le i \le j$ and all other cycles have length at least $k+1$.*

3. Special linear groups $SL_2(q)$

In this section we prove Theorem 2 and then conjecture some further families of factorizations for $SL_2(q)$.

Let $G = SL_2(q)$, and let B be the Borel subgroup consisting of upper triangular matrices in G. Then $B = \mathrm{Stab}_G(\langle v\rangle)$ where $v = (1, 0)^T$. Hence we can describe the left cosets of B as follows.

Lemma 3.1. *If $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(q)$, then*

$$xB = \left\{\begin{pmatrix} \lambda a & u \\ \lambda c & v \end{pmatrix} \in SL_2(q) \mid \lambda \in \mathbb{F}_q^\times\right\}.$$

Proof of Theorem 2. An arbitrary conjugate of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ looks like $\begin{pmatrix} 1-\alpha\beta & \alpha^2 \\ -\beta^2 & 1+\alpha\beta \end{pmatrix}$ for $\alpha, \beta \in \mathbb{F}_q$ not both zero. For fixed $a, c \in \mathbb{F}_q$ not both zero, we shall count how many such matrices are of the form $\begin{pmatrix} \lambda a & u \\ \lambda c & v \end{pmatrix}$ where $\lambda \in \mathbb{F}_q^\times$. We shall show that this number is always $(q-1)/(2, q-1)$, so that Lemmas 3.1 and 2.1(i) imply the conclusion of Theorem 2.

Case I. Suppose that $c = 0$. So, $\beta = 0$ and $\alpha \neq 0 \Rightarrow v = 1$ and $\lambda = a^{-1}$. Conjugates of this form are therefore determined by $u = \alpha^2$. When q is even there are $q-1$ such choices for u and when q is odd there are $(q-1)/2$.

Case II. Suppose that $c \neq 0$. So, $\lambda = -\beta^2/c \neq 0$ for which there are $q-1$ or $(q-1)/2$ choices, dependent on q being even or odd. Now for each square root β of β^2, the equation $\lambda a = 1 - \alpha\beta$ determines α and hence both u and v too. Note that both square roots of β^2 give the same values for u and v, concluding the proof. □

When q is even, the work of Terada in [4] shows that

$$X := \{x \in SL_2(q) : x^{q+1} = 1,\ x \neq 1\}$$

is another candidate for a union of conjugacy classes dividing $SL_2(q)$. If this were to have a code given by a subgroup Y (i.e. if $\lambda G = XY$), then [4, Theorem 6] together with the classification of finite subgroups of $SL_2(q)$ (see [3, Theorem 6.25]), shows that Y would have to be either C_{q+1} or $D_{2(q+1)}$.

Immediately it can be seen that $Y = C_{q+1}$ does not work, since $|X \cap C_{q+1}| = q$, whereas λ would have to be $q/2$ for such a code. Hence the only possibility is $Y = D_{2(q+1)}$. In this case, computations in GAP verify that we do have a factorization $qSL_2(q) = XY$ for even $q \le 256$. Computation also suggests a similar factorization of $PGL_2(q)$ for odd q. Hence we propose (noting that for even q we have $SL_2(q) = PGL_2(q)$):

Conjecture 3.2. *Let $G = PGL_2(q)$, and define*

$$X = \{x \in G : x^{q+1} = 1,\ x^2 \neq 1\}.$$

Then $\lambda G = XD_{2(q+1)}$, where $\lambda = q$ if q is even, and $\lambda = q-1$ if q is odd.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] G. Etienne, Perfect codes and regular partitions in graphs and groups, European J. Combin. 8 (1987) 139–144.
[2] H. Huang, B. Xia, S. Zhou, Perfect codes in Cayley graphs, SIAM J. Discrete Math. 32 (2018) 548–559.
[3] M. Suzuki, Group Theory I, in: Grundlehren der Mathematischen Wissenschaften, vol. 247, Springer-Verlag, Berlin-New York, 1982.
[4] S. Terada, Perfect codes in $SL(2, 2^f)$, European J. Combin. 25 (2004) 1077–1085.

Please cite this article as: H.M. Green and M.W. Liebeck, Some codes in symmetric and linear groups, Discrete Mathematics (2019) 111719, https://doi.org/10.1016/j.disc.2019.111719.