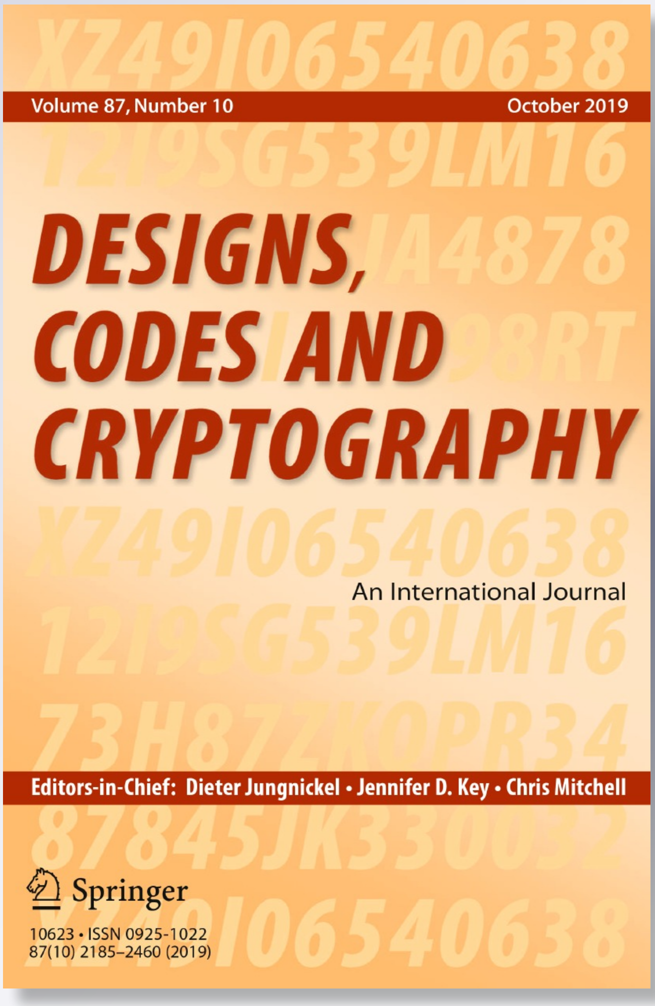
A note on good permutation codes from Reed–Solomon codes

R. Sobhani, A. Abdollahi, J. Bagherian & M. Khatami

Designs, Codes and Cryptography
An International Journal

ISSN 0925-1022
Volume 87
Number 10

Des. Codes Cryptogr. (2019)
87:2335-2340
DOI 10.1007/s10623-019-00621-0



Volume 87, Number 10 October 2019

DESIGNS, CODES AND CRYPTOGRAPHY

An International Journal

Editors-in-Chief: Dieter Jungnickel • Jennifer D. Key • Chris Mitchell

Springer

10623 • ISSN 0925-1022
87(10) 2185–2460 (2019)

Springer

Designs, Codes and Cryptography (2019) 87:2335–2340
https://doi.org/10.1007/s10623-019-00621-0

A note on good permutation codes from Reed–Solomon codes

R. Sobhani[1,2] · A. Abdollahi[1,2] · J. Bagherian[1] · M. Khatami[1]

Received: 9 March 2018 / Revised: 14 November 2018 / Accepted: 8 February 2019 /
Published online: 21 February 2019

Abstract
Let $M(n, d)$ be the maximum size of a permutation code of length n and distance d. In this note, the permutation codewords of a classical code C are considered. These are the codewords with all different entries in C. Using these codewords for Reed–Solomon codes, we present some good permutation codes in this class of codes. As a consequence, since these codes are subsets of Reed–Solomon codes, decoding algorithms known for Reed–Solomon codes can also be used as a decoding algorithm for them.

Keywords Permutation codes · Reed–Solomon codes · Automorphism groups

Mathematics Subject Classification 05A05 · 94B25 · 05E18

1 Introduction

Permutation codes are defined as subsets of the symmetric group S_n consisting of all permutations on n letters $\{1, 2, \dots, n\}$. The length of a permutation code in S_n is n. Permutation codes have been proposed for application in the transmission of data over powerlines [11,24,30] and in the design of block ciphers [7]. When a permutation code is used in a powerline communication, the capability of its error correction depends on its minimum Hamming distance. For reliable and efficient communication it is necessary to find codes, for a given length and

Communicated by C. J. Colbourn.

✉ R. Sobhani
r.sobhani@sci.ui.ac.ir

A. Abdollahi
a.abdollahi@sci.ui.ac.ir

J. Bagherian
bagherian@sci.ui.ac.ir

M. Khatami
m.khatami@sci.ui.ac.ir

[1] Department of Mathematics, University of Isfahan, 81746-73441 Isfahan, Iran

[2] School of Mathematics, Institute for Research in Fundamental Sciences (IPM), 19395-5746 Tehran, Iran

minimum distance, with size as large as possible. Let $M(n, d)$ denote this maximum size. In recent works, numerous techniques have been developed to derive lower and upper bounds on $M(n, d)$, [1,5,6,8,11,12,15–17,22,24,27]. Also, in [2,3], some techniques for obtaining new permutation codes from old ones have been presented.

In this paper, we find good permutation codes by considering all codewords of a Reed–Solomon code, say C, that are permutations, denoted by $P(C)$. In fact, we compute value vectors of all permutation polynomials of degree at most $k-1$ as a subset of a Reed–Solomon code of dimension k over $\mathbb{F}_q$. An advantage of the method is that we work on codewords of a linear code over $\mathbb{F}_q$ instead of computing permutation polynomials and their value vectors. Another advantage is that, since these codes are subsets of Reed–Solomon codes, decoding algorithms known for Reed–Solomon codes can also be used as a decoding algorithm for them. We also develop a theory on the structure of $P(C)$ and present an algorithm for determining $|P(C)|$. Precisely, we prove that $P(C)$ is a union of some cosets of $Perm(C)$, the permutation group of the code C, in the symmetric group S_q. The technique of considering unions of cosets of some permutation groups in S_n is also used in [1,27] for constructing good permutation codes.

2 Main result

A permutation code of length n is a subset of the symmetric group S_n. The Hamming distance between two permutations σ and τ is defined to be the number of moved points of the permutation $\sigma\tau^{-1}$. Note that we say the permutation α moves i if $\alpha(i) \neq i$. The minimum distance of a permutation code is the minimum of distances between all two distinct permutations in it.

A code C of length n over the finite field $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$. The code C is said to be linear if it is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$. The weight of an element of $\mathbb{F}_q^n$ is defined to be the number of its nonzero entries. The Hamming distance between two elements x, y of $\mathbb{F}_q^n$ is defined to be the weight of $x - y$. The minimum distance of a code C is the minimum of distances between all two distinct elements of C. By an $(n, M, d)_q$ code we mean a code of length n, cardinality M and minimum of distances between all pairs of distinct d over $\mathbb{F}_q$. When the code is linear, we use the notation $[n, k, d]_q$ where k is the dimension of C over $\mathbb{F}_q$ instead of its cardinality. The maximum size of a code of length n and distance d over $\mathbb{F}_q$ is denoted by $A_q(n, d)$. The Singleton bound states that $A_q(n, d) \leq q^{n-d+1}$. Codes achieving this bound are called Maximum Distance Separable (MDS) codes.

The following definition is a key for the main result of this paper.

Definition 1 Let C be a code of length q over $\mathbb{F}_q$. A codeword $c = (c_1, c_2, \ldots, c_q)$ in C is said to be a permutation codeword if all of its components are distinct. The set of all permutation codewords of C is denoted by $P(C)$.

It is clear that $P(C)$ can be viewed as a subset of the symmetric group S_q. Our strategy is to consider $P(C)$ as a permutation code, where C is a suitably chosen code of length q over $\mathbb{F}_q$. In this case $P(C)$ has minimum distance at least as large as the minimum distance of the corresponding code C, and hence we are interested in good codes C with large $P(C)$.

The permutation group of a code C of length n is the maximal subgroup Γ of S_n with the property that for any $\gamma \in \Gamma$ we have $\gamma(C) = C$, where $\gamma(C)$ is the code obtained by permuting the coordinates of C according to the permutation γ. We denote the permutation group of a code C, by $Perm(C)$. The following proposition deals with the relation between $P(C)$ and $Perm(C)$.

Proposition 1 *For any code of length q over $\mathbb{F}_q$, $P(C)$ is a union of some right cosets of $Perm(C)$ in S_q and hence $|Perm(C)| \mid |P(C)|$.*

Proof First note that, for any $\sigma \in Perm(C)$ and $c \in P(C)$ we have $\sigma(c) \in P(C)$. Equivalently, we have $Perm(C) \subseteq Perm(P(C))$ (in general, for codes C and D with $D \subseteq C$, it is not true that $Perm(C) \subseteq Perm(D)$). Now, $Perm(C)$ acts faithfully on the set $P(C)$ and hence $Perm(C)P(C) = P(C)$. Therefore $P(C)$ is a union of some right cosets of $Perm(C)$ in S_q. This completes the proof. □

Reed–Solomon (RS) codes are famous examples of linear MDS codes [14,25]. Write $\mathbb{F}_q = \{0, w, w^2, \ldots, w^{q-1}\}$, where w is a primitive element of $\mathbb{F}_q$ and let $\mathbb{F}_q[x]$ be the set of all polynomials with coefficients in $\mathbb{F}_q$. The Reed–Solomon code of distance d over $\mathbb{F}_q$, denoted by $RS(q, d)$, is the linear space

$$RS(q, d) := \{(P(0), P(w), \ldots, P(w^{q-1})) \mid P(x) \in \mathbb{F}_q[x],\ \deg(P(x)) \leq q - d\}.$$

It is known that $RS(q, d)$ is a $[q, q - d + 1, d]_q$ MDS code.

It has been proved in [10] (see also [4]) that the permutation group of the code $C = RS(q, d)$ with dimension $2 \leq k = q - d + 1 \leq q - 2$ is the group of affine permutations and has size $q(q-1)$. On the other hand, when $C = RS(q, d)$ and $3 \leq d \leq q - 1$, $P(C)$ contains

$$\{(Q(0), Q(w), \ldots, Q(w^{q-1})) \mid Q(x) = ax + b \in \mathbb{F}_q[x],\ a, b \in \mathbb{F}_q,\ a \neq 0\},$$

which is the set of affine permutations and has size $q(q-1)$. Hence $P(C)$ is not empty.

Corollary 1 *Let q be a prime power. Then $P(RS(q, q-1))$ is a $(q, q(q-1), q-1)_q$ optimal permutation code.*

Proof It is known that $M(n, d) \leq \frac{n!}{(d-1)!}$ and hence $M(q, q-1) \leq q(q-1)$. But $P(RS(q, q-1))$ has size at least $q(q-1)$. Therefore we have $|P(RS(q, q-1))| = q(q-1)$ and $P(RS(q, q-1))$ is an optimal permutation code. □

Corollary 2 *Let q be a prime power and $3 \leq d \leq q - 1$. Then*

$$q(q-1) \mid |P(RS(q, d))|.$$

Proof It follows from Proposition 1 and the fact that $P(RS(q, d))$ is not empty. □

Remark 1 A permutation polynomial over $\mathbb{F}_q$ is a polynomial in $\mathbb{F}_q[x]$ that permutes the elements of $\mathbb{F}_q$. When $C = RS(q, d)$, then $P(C)$ is in fact the set of value vectors of all permutation polynomials of degree at most $q-d$ and hence when we compute $P(C)$ we are in fact computing the value vectors of all permutation polynomials of degree at most $q-d$. There is a large body of knowledge related to the problem of finding all permutation polynomials of a given degree, see for example [9,19,20,23]. However, there are some advantages in computing $P(C)$ instead of computing the value vectors of permutation polynomials. First is that computing permutation polynomials and their value vectors is not always straightforward. Second is that, since we look at the permutation code as a subset of a Reed–Solomon code, decoding algorithms for Reed–Solomon codes presented in the literature (for example those in [13,21,29]), can also be used as a decoding algorithm for them.

To obtain permutation codes from permutation codewords of a classical code C, we need to calculate $P(C)$. A computational problem now is how to compute $P(C)$ or how to find

$|P(C)|$. More precisely, for large values of q and small values of d (large dimensions), the problem of finding $P(C)$ or $|P(C)|$ becomes complicated. For example, the CPU time for calculation of $P(C)$ where C is the $[32, 6, 27]_{32}$ Reed–Solomon code is about 32 hours on a 2 GHz CPU.

Here the complexity of finding $|P(C)|$, is reduced a little for some classes of codes including $RS(q, d)$. Let C be a $[q, k, d]_q$ code and $G = (g_{ij})_{k\times q}$, a generator matrix for C. Set $A := \{(i, j) \mid 1 \le i < j \le q\}$ and write $A := \{u_1, \ldots, u_s\}$, where $s = q(q-1)/2$ and $u_t = (a_t, b_t)$ for $1 \le t \le s$. Assume that $L = (l_{ij})_{k\times s}$ is a $k \times s$ matrix over $\mathbb{F}_q$ with $l_{ij} = g_{ia_j} - g_{ib_j}$. Let D be the linear code generated by L, k' be its dimension, and $FW(D)$ be the set of those codewords in D whose weights equals s. We have the following proposition now.

Proposition 2 *With notation as above, we have* $|P(C)| = q^{k-k'}|FW(D)|$.

Proof It can simply be verified that $c = [\alpha_1, \ldots, \alpha_k]G$ lies in $P(C)$ if and only if $d = [\alpha_1, \ldots, \alpha_k]L$ lies in $FW(D)$. Now we can assume that the first $k - k'$ rows of L are zero and hence $\alpha_1, \ldots, \alpha_{k-k'}$ can freely be chosen in $\mathbb{F}_q$. The proof is now completed. □

Now, if C contains the all-one vector then we can choose G such that its first row is the all-one vector. In this way, the first row of L becomes the zero vector and hence the dimension of D reduces at least by 1. Note that the codes $RS(q, d)$ contain the all-one vector and hence we have $k' \le k - 1$ for them. In fact, one can see that for MDS codes containing the all-one vector, we have $k' = k - 1$.

In what follows, we now list the size of $P(C)$ for some Reed–Solomon codes over $\mathbb{F}_q$ with different q which lead to some good permutation codes. As mentioned in Remark 1, codewords of these codes are in fact value vectors of all permutation polynomials of degree at most $q - d$. All of the codes we construct can also be constructed from the known results on permutation polynomials of small degree (see [9,18,23,26]). The text file of these codes (except the last) can be found in [28]. In that files, each code has been presented as a collection of representatives of some cosets of $AGL(1, q)$ in S_q.

(1) Let $q = 16$, $d = 10$ and C be the Reed–Solomon code of length 16 and dimension 7 over $\mathbb{F}_{16}$. Then $|P(C)| = 222{,}720$ and hence $M(16, 10) \ge 222{,}720$. The previous known lower bound for $M(16, 10)$ was 164,880 [1]. We should note that one of the referees, based on the method described in [16], kindly provided us with an unpublished permutation code of length 16, size 362880 and distance 10, in his (her) comments. Also the code can be obtained from permutation polynomials of degree at most 6 over $\mathbb{F}_{16}$.
(2) Let $q = 25$, $d = 20$ and C be the Reed–Solomon code of length 25 and dimension 6 over $\mathbb{F}_{25}$. Then $|P(C)| = 192{,}000$ and hence $M(25, 20) \ge 192{,}000$. The previous known lower bound for $M(25, 20)$ was 15600 [1]. The code can also be obtained from permutation polynomials of degree at most 5 over $\mathbb{F}_{25}$.
(3) Let $q = 27$, $d = 22$ and C be the Reed–Solomon code of length 27 and dimension 6 over $\mathbb{F}_{27}$. Then $|P(C)| = 522{,}288$ and hence $M(27, 22) \ge 522{,}288$. The previous known lower bound for $M(28, 22)$ was 275,184 [22]. The code can also be obtained from permutation polynomials of degree at most 5 over $\mathbb{F}_{27}$.
(4) Let $q = 32$, $d = 27$ and C be the Reed–Solomon code of length 32 and dimension 6 over $\mathbb{F}_{32}$. Then $|P(C)| = 1{,}388{,}800$ and hence $M(32, 27) \ge 1{,}388{,}800$. The previous known lower bound for $M(33, 27)$ was 327,360 [22]. The code can also be obtained from permutation polynomials of degree at most 5 over $\mathbb{F}_{32}$ (see [9,23]).
(5) Let $q = 32$, $d = 25$ and C be the Reed–Solomon code of length 32 and dimension 8 over $\mathbb{F}_{32}$. Then we have $|P(C)| = 32 * |FW(D)| = 3{,}420{,}416$, where D is the linear

$[496, 7]_{32}$-code obtained from the method described in Proposition 2 from the code C. Hence we have $M(32, 27) \geq 3{,}420{,}416$. The previous known lower bound for $M(32, 25)$ was 1,309,440 [22]. In this case, we could not find $P(C)$ and we just know $|P(C)|$. The code can also be obtained from permutation polynomials of degree at most 7 over $\mathbb{F}_{32}$.

Acknowledgements The authors would like to thank anonymous referees whose comments greatly improved the results and presentation of the paper. The first author was supported in part by Grant No. 95050080 from School of Mathematics, Institute for Research in Fundamental Sciences (IPM). The second author was supported in part by Grant No. 96050219 from School of Mathematics, Institute for Research in Fundamental Sciences (IPM). The second author was additionally financially supported by the Center of Excellence for Mathematics at the University of Isfahan.

References

1. Bereg S., Levy A., Sudborough I.H.: Constructing permutation arrays from groups. Des. Codes Cryptogr. **86**(5), 1095–1111 (2018).
2. Bereg S., Mojica L.G., Morales L., Sudborough H.: Parallel partition and extension: Better permutation arrays for hamming distances. In: Conference on Information Science and Systems (CISS), pp. 1–6. IEEE (2017).
3. Bereg S., Morales L., Sudborough I.H.: Extending permutation arrays: improving MOLS bounds. Des. Codes Cryptogr. **83**(3), 661–683 (2017).
4. Berger T.P.: A direct proof for the automorphism group of Reed–Solomon codes. In: Cohen G., Charpin P. (eds.) Proc. Eurocode 90. Lecture Notes in Computer Science, vol. 514, pp. 21–29. Springer, Berlin (1991).
5. Chu W., Colbourn C.J., Dukes P.: Constructions for permutation codes in powerline communications. Des. Codes Cryptogr. **32**(1–3), 51–64 (2004).
6. Colbourn C.J., Kløve T., Ling A.C.H.: Permutation arrays for powerline communication and mutually orthogonal latin squares. IEEE Trans. Inf. Theory **50**(6), 1289–1291 (2004).
7. de la Torre D.R., Colbourn C.J., Ling A.C.H.: An application of permutation arrays to block ciphers. Cong. Numer. **145**, 5–7 (2000).
8. Deza M., Vanstone S.A.: Bounds for permutation arrays. J. Stat. Plan. Inference **2**, 197–209 (1978).
9. Dickson L.E.: Linear Groups with an Exposition of the Galois Field Theory. Dover, New York (1958).
10. Dür A.: The automorphism groups of Reed–Solomon codes. J. Comb. Theory Ser. A **44**(1), 69–82 (1987).
11. Ferreira H.C., Vinck A.J.H.: Inference cancellation with permutation trellis arrays. In: Proceedings of IEEE Vehicular Technology Conference, Boston, pp. 2401–2407 (2000).
12. Frankl P., Deza M.: On the maximum number of permutations with given maximal or minimal distance. J. Comb. Theory Ser. A **22**(3), 352–360 (1977).
13. Gao S.: A new algorithm for decoding Reed–Solomon codes. In: Bhargava V.K., Poor H.V., Tarokh V., Yoon S. (eds.) Communications, Information and Network Security, vol. 712. The Springer International Series in Engineering and Computer Science (Communications and Information Theory)Springer, Boston (2003).
14. Gorenstein D., Zierler N.: A class of error correcting codes in p^m symbols. J. Soc. Ind. Appl. Math. **9**(2), 207–214 (1961).
15. Gao F., Yang Y., Ge G.: An improvement on the Gilbert–Varshamov bound for permutation codes. IEEE Trans. Inf. Theory **59**(5), 3059–3063 (2013).
16. Janiszczak I., Lempken W., Östergård P.R.J., Staszewski R.: Permutation codes invariant under isometries. Des. Codes Cryptogr. **75**(3), 497–507 (2015).
17. Janiszczak I., Staszewski R.: An improved bound for permutation arrays of length 10. Technical Report 4, Institute for Experimental Mathematics, University Duisburg-Essen (2008).
18. Li J., Chandler D.B., Xiang Q.: Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2. Finite Fields Appl. **16**, 406–419 (2010).
19. Lidl R., Mullen G.L.: When does a polynomial over a finite field permute the elements of the field? Am. Math. Mon. **95**(3), 243–246 (1988).
20. Lidl R., Mullen G.L.: When does a polynomial over a finite field permute the elements of the field? II. Am. Math. Mon. **100**(1), 71–74 (1993).
21. Massey J.L.: Shift-register synthesis and BCH decoding. IEEE Trans. Inf. Theory **IT–15**, 122–127 (1969).
22. Mojica L.G.: Permutation arrays with large Hamming distance, Ph.D. Thesis, University of Texas (2017).

23. Mullen G.L., Panario D.: Handbook of Finite Fields. CRC Press, Hoboken (2013). Chapter 8.
24. Pavlidou N., Vinck A.J.H., Yazdani J., Honary B.: Power line communications: state of the art and future trends. IEEE Commun. Mag. **41**, 34–40 (2003).
25. Reed I.S., Solomon G.: Polynomial codes over certain finite fields. J. Soc. Ind. Appl. Math. **8**(2), 300–304 (1960).
26. Shallue C.J., Wanless I.M.: Permutation polynomials and orthomorphism polynomials of degree six. Finite Fields Appl. **20**, 84–92 (2013).
27. Smith D.H., Montemanni R.: A new table of permutation codes. Des. Codes Cryptogr. **63**(2), 241–253 (2012).
28. Source files of the codes: http://sciold.ui.ac.ir/~r.sobhani/NPA. Last accessed 21 July 2018.
29. Sudan M.: Decoding of Reed Solomon codes beyond the error-correction bound. J. Complex. **13**(1), 180–193 (1997).
30. Vinck A.J.H.: Coded modulation for powerline communications. AEÜ Int. J. Electron. Commun. **54**(1), 45–49 (2000).

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