designs by Mathon [13] and Jimbo [14]. Here, we use it to produce good larger DTS from smaller DTS.

An additive triangle of size n is a collection T of $n(n+1)/2$ integers s_j^k, $k = 1, 2, \cdots, n$; $j = 1, 2, \cdots, n+1-k$,

$$\begin{array}{ccccc} & & s_1^n & & \\ & s_1^{n-1} & & s_2^{n-1} & \\ & / & & \backslash & \\ s_1^2 & & \cdots & & s_{n-1}^2 \\ s_1^1 & s_2^1 & \cdots & & s_n^1 \end{array}$$

such that

$$s_j^k = \sum_{i=j}^{j+k-1} s_i^1, \tag{5}$$

where s_j^k is called the entry in the (k, j)-position of T.

From definitions above, we can show that an additive sequence of permutations of order $2r+1$ and length n is equivalent to $2r+1$ additive triangles of size n with entries from X^1 such that each integer of X^1 is the entry s_j^k, $k = 1, 2, \cdots, n$; $j = 1, 2, \cdots, n+1-k$, of exactly one of them [15]. Each triangle Δ_i of a DTS determines an additive triangle of size n whose entries are $s_j^k = a_{i,j+k} - a_{ij}$, $k = 1, 2, \cdots, n$; $j = 1, 2, \cdots, n+1-k$, called a difference triangle of Δ_i with $n = J$. Following the construction for perfect systems of difference sets with ASP, we describe a method to obtain DTS from known DTS and ASP. Let $U_1, \cdots, U_{2r+1}$ be the additive triangles corresponding to an additive sequence of permutations of order $2r+1$ and length $n = J$. For $i = 1, 2, \cdots, I$ and $j = 1, 2, \cdots, 2r+1$, define additive triangles $T_i + U_j$ as follows: for $k = 1, 2, \cdots, J$ and $p = 1, 2, \cdots, J+1-k$, the entry in the (k, p)-position of $T_i + U_j$ is $(2r+1)s_p^k + s_p^k$, where T_i has entry s_p^k and U_j has entry s_p^k in the (k, p)-position. The resulting mI additive triangles $T_i + U_j$ correspond to a new (tI, J)-DTS with $t = 2r+1$ and $m = tm_1 + r$, where m_1 is the maximum element of (I, J)-DTS. For a similar proof, see [12], [15].

Example 2: An ASP of order 5 and length 4 is as follows: $X^1 = (-2, -1, 0, 1, 2,$ $X^2 = (0, 1, 2, -2, -1)$, $X^3 = (2, -2, -1, 0, 1)$, and $X^4 = (-1, 0, 1, 2, -2)$. It is known that there are a $(3,4)$-DTS with $m_1 = 32$ and a $(4,4)$-DTS with $m_1 = 41$. Therefore, we have a $(15,4)$-DTS with $m = 162$ and a $(20,4)$-DTS with $m = 207$. New results on $M(I, J)$ obtained with this construction are also given in Table I. The best known results are included for comparison.

IV. Conclusion

With the disjoint difference sets formed from the lines of Euclidean geometries and difference families, and additive sequence of permutations, we present further results on the size of difference triangle sets. With these results, we can construct better convolutional self-orthogonal codes. DTS and related DDS have some applications. The results can be extended to apply to other applications [4], [6].

Acknowledgment

The author is grateful to Professor I. Ingemarsson for his support and discussion. The author is also grateful to the referees and the Associate Editor for their reviews and helpful suggestions.

References

[1] J. P. Robinson and A. J. Bernstein, "A class of recurrent codes with limited error propagation," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 106–113, 1967.
[2] E. J. Klieber, "Some difference triangles for constructing self-orthogonal codes," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 237–238, 1970.
[3] W. Wu, "New convolutional codes, Part II," *IEEE Trans. Commun.*, vol. COM-24, pp. 19–32, 1976.
[4] T. Kløve, "Bounds and construction for difference triangle sets," *IEEE Trans. Inform. Theory*, vol. 35, pp. 879–886, 1989.
[5] G. D. Martin, "Optimal convolutional self-orthogonal codes with an application to digital radio," *Proc. IEEE ICC*, pp. 1249–1253, 1987.
[6] Z. Chen, P. Z. Fan, and F. Jin, "Disjoint difference sets, difference triangle sets and related codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 518–522, 1992.
[7] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *AMS Trans.*, vol. 43, pp. 377–385, 1938.
[8] R. C. Bose, "An affine analogue of Singer's theorem," *Ind. Math. Soc.*, vol. 6, pp. 1–5, 1942.
[9] R. M. Wilson, "Cyclotomy and difference families in elementary abelian groups," *J. Number Theory*, vol. 4, pp. 17–47, 1972.
[10] R. C. Rao, "Cyclical generation of linear subspaces in finite geometries," in *Combinatorial Mathematics and its Applications*, R. C. Bose, ed. Place: Publisher, 1967, pp. 515–535.
[11] J. A. Salehi, F. K. Chung, and V. K. Wei, "Optical orthogonal codes: Designs, analysis, and applications," *IEEE Trans. Inform. Theory*, vol. 35, pp. 595–604, 1989.
[12] A. Kotzig and J. M. Turgeon, "Perfect systems of difference sets and additive sequence of permutations," *Congr. Numer. 24*, vol. II, pp. 629–636, 1979.
[13] R. Mathon, "Constructions for cyclic Steiner 2-designs," *Ann. Discrete Math.*, vol. 34, pp. 353–362, 1987.
[14] M. Jimbo, "Recursive construction for cyclic BIB designs and their generalizations," *Discrete Math.*, vol. 116, pp. 79–95, 1993.
[15] P. Wild, "Combining perfect systems of difference sets," *Bull. London Math. Soc.*, vol. 18, pp. 127–130, 1986.

Constructions, Families, and Tables of Binary Linear Covering Codes

Alexander A. Davydov
and Anna Yu. Drozhzhina-Labinskaya

Abstract—**We present constructions and infinite families of binary linear covering codes with covering radii $R = 2, 3, 4$. Using these codes, we obtain a table of constructive upper bounds on the length function $l(r, R)$ for $r \le 64$ and $R = 2, 3, 4$, where $l(r, R)$ is the smallest length of a binary linear code with given codimension r and covering radius R. We obtain also upper bounds on $l(r, R)$ for $r = 21, 28$, $R = 5$. Parameters of the constructed codes are better than parameters of previously known codes.**

Index Terms—**Covering radius, covering codes, binary linear codes.**

I. Introduction

Covering codes are being extensively studied, see, e.g., [1]–[17]. We consider *binary linear* covering codes.

Manuscript received September 10, 1991; revised August 20, 1993. This work was presented in part at the II International Workshop on Algebraic and Combinatorial Coding Theory, ACCT-2, Leningrad, USSR, September 1990, and at the International Workshop on Algebraic and Combinatorial Coding Theory, Voneshta Voda, Bulgaria, June 1992.

The authors are with the Institute for Problems of Cybernetics of the Russian Academy of Sciences, Vavilov Street 37, Moscow 117312, Russia.

IEEE Log Number 9403709.

Denote by E^n the space of n-dimensional vectors over the Galois field GF(2). Let an $[n, n-r]R$ code be a binary linear code of length n, codimension r, and covering radius R. An $[n, n-r]R$ code is an $(n-r)$-dimensional subspace of E^n. The *covering radius* of an $[n, n-r(C)]R$ code C is the least integer R such that the space E^n is covered by spheres of radius R whose centers are codewords. The *density* of this covering is denoted by $\mu(n, R, C)$ and is defined as follows:

$$\mu(n,R,C) \triangleq 2^{n-r(C)} \sum_{i=0}^{R} \binom{n}{i} \Big/ 2^n = \sum_{i=0}^{R} \binom{n}{i} \Big/ 2^{r(C)} \geq 1. \tag{1.1}$$

This parameter characterizes a quality of the covering.

Let U be an infinite family of codes with covering radius R, and let U_n be a code with length n of this family. For the family U, we consider the following asymptotic parameter [9]:

$$\overline{\mu}(R,U) \triangleq \liminf_{n\to\infty,\, U_n \in U} \mu(n,R,U_n). \tag{1.2}$$

Further, we use the notation $\overline{\mu}(R)$ instead of $\overline{\mu}(R,U)$ because the family U is defined by context.

The *length function* $l(r, R)$ [3] is the smallest length of a binary linear code with codimension r and covering radius R.

For the family of the $[2^r-1, 2^r-1-r]1$ Hamming codes with $R = 1$, we have $\overline{\mu}(1) = 1$. Infinite families of binary linear codes with $R \geq 2$ are considered, e.g., in [3], [5], [7], [9], [10], [16]. Tables of upper bounds on $l(r, R)$ are given in [1] and [3]. The constructions DS (direct sum) and ADS (amalgamated direct sum) for covering codes are described in [10]. Other constructions of covering codes are proposed in [7]. They use a starting code to generate an infinite code family.

In this work we modify a construction from [7] and generate infinite families of codes with covering radii $R = 2, 3, 4$ having better parameters than known families. Thus we improve upper bounds on $l(r, R)$. The constructed codes are normal as defined in [10].

In Section II, we give the general form of a covering code parity-check matrix proposed in [7]. We call this form "Construction A." In order to obtain a real matrix from the general form, one should design some submatrix and some set of field elements. In Sections III–V, for $R = 2, 3, 4$, we propose a number of techniques for design of this submatrix and this set and obtain code families. We constructed in Examples 3.1, 4.2, and 5.5 infinite families of $[n, n-r]R$ codes with parameters:

$$R = 2, \quad r = 2t, \quad t \geq 4, \quad n = 27 \times 2^{t-4} - 1, \quad \overline{\mu}(2) \approx 1.4238, \tag{1.3}$$

$$R = 3, \quad r = 3t-1, \quad t \geq 14, \quad n = 821 \times 2^{t-9} - 1, \quad \overline{\mu}(3) \approx 1.3744, \tag{1.4}$$

$$R = 4, \quad r = 4t-2, \quad t \geq 16, \quad n = 991 \times 2^{t-9} - 1, \quad \overline{\mu}(4) \approx 2.3392. \tag{1.5}$$

In Section VI we give in Table I the new upper bounds on $l(r, R)$ for $r \leq 64$, $R = 2, 3, 4$, and new upper bounds on $l(r, R)$ for $r = \overline{21, 28}$, $R = 5$.

II. Definition, Notations, and Construction A

Here all matrices and columns are binary. An upper index in the notation of a matrix (column) is the number of *binary* rows (components) in it, except for the symbol of transposition *tr*. An element h of GF(2^m) written as an element of a binary matrix (column) denotes the m-dimensional column vector that is the binary representation of h. For definiteness, $h = h_m\alpha^{m-1} + \cdots + h_2\alpha + h_1 = (h_m \cdots h_2\, h_1)^{tr}$, where $h_i \in$ GF(2), $i = \overline{1, m}$, and α is a primitive element of GF(2^m). We assume that formally the number of summands of a column sum may be equal to zero and then we treat this sum to be equal to the zero column.

TABLE I
Constructive Upper Bounds on the Length Function $l(r, R)$ for $R = 2, 3, 4$

codimension r	upper bound on $l(r,R)$ $R = 2$	$R = 3$	$R = 4$	codimension r	upper bound on $l(r,R)$ $R = 2$	$R = 3$	$R = 4$
				33	163839 [c]	4863	894
2	2 [a]			34	221183	6143	990
3	4 [a]	3 [a]		35	327679 [c]	6574	1246
4	5 [a]	5 [a]	4 [a]	36	442367	9727	1533
5	9 [a]	6 [a]	6 [a]	37	655359 [c]	12287	1790
6	13 [a]	7 [a]	7 [a]	38	884735	13150	1982
7	19 [a]	11 [a]	8 [a]	39	1310719 [c]	19455	2494
8	26 [b,c]	14 [a]	9 [a]	40	1769471	24575	3038
9	39 [c]	18 [b]	13 [a]	41	2621439 [c]	26271	3581
10	53 [d]	22 [a]	16 [a]	42	3538943	38911	3965
11	79 [c]	23 [a]	20 [a]	43	5242879 [c]	49151	4989
12	107	38 [b]	24 [a]	44	7077887	52543	6015
13	159 [c]	53 [c]	25 [a]	45	10485759 [c]	77823	7165
14	215	63 [d,e]	29 [a]	46	14155775	98303	7933
15	319 [c]	75	37 [a]	47	20971519 [c]	105087	9981
16	431	95	49 [e]	48	28311551	155647	12031
17	639 [c]	126	62 [d]	49	41943039 [c]	196607	14333
18	863	153	77 [c]	50	56623103	210175	15869
19	1279 [c]	205	84	51	83886079 [c]	311295	19965
20	1727	255 [d]	93	52	113246207	393215	24063
21	2559 [c]	308 [d]	125	53	167772159 [c]	420351	28669
22	3455	383	150	54	226492415	622591	31741
23	5119 [c]	511 [d]	174	55	335544319 [c]	786431	39933
24	6911	618	190	56	452984831	840703	48127
25	10239 [c]	767	238	57	671088639 [c]	1245183	57341
26	13823	820	301	58	905969663	1572863	63485
27	20479 [c]	1215	349	59	1342177279 [c]	1681407	79869
28	27647	1535	381	60	1811939327	2490367	96255
29	40959 [c]	1642	477	61	2684354559 [c]	3145727	114559
30	55295	2431	605	62	3623878655	3362815	126847
31	81919 [c]	3071	701	63	5368709119 [c]	4980735	159615
32	110591	3286	765	64	7247757311	6291455	192511

Key to Table I: Unmarked bounds are obtained in this work.
[a] Ref. [10].
[b] Ref. [1].
[c] Ref. [9].
[d] Ref. [7].
[e] Ref. [8].

Fact 2.1 [5]: The covering radius of a binary linear code of codimension r with a parity check matrix H is the least integer R such that any binary column of length r is a sum of at most R columns of H.

Definition 2.1: Let C be a binary linear $[Q, Q-s]R$ code of length Q, codimension s, covering radius R, with a parity-check matrix Φ^S. Let l be an integer, $R \geq l \geq 0$. Let l have the following properties: for any binary column π of length s (including the zero column), there exists an integer $z(\pi)$ such that $R \geq z(\pi) \geq l$, and the column π can be represented by a sum of $z(\pi)$ distinct columns of the matrix Φ^S. By definition, a sum of 0 columns is treated as the zero column. Then this code C is called an R, l-object of the space E^Q and is denoted by a $[Q, Q-s]R, l$ code. A $[Q, Q-s]R, l$ code with $l > 0$ is also a $[Q, Q-s]R, l_1$ code with $l_1 = 0, 1, \cdots, l-1$.

Remark 2.1: The R, l-objects are a subclass of the R, l-subsets introduced in [7, p. 321].

Clearly, a $[Q, Q-s]R$ code is always a $[Q, Q-s]R, 0$ code. But if $l > 0$, then the structure of the code parity-check matrix answers the question: can the $[Q, Q-s]R$ code be treated as a $[Q, Q-s]R, l$ code?

Example 2.1: We consider the following parity-check matrices:

$$\Phi_1^4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \tag{2.1}$$

$$\Phi_2^4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} = [\varphi_1 \cdots \varphi_5],$$

$$\varphi_i \in \mathrm{GF}(2^4), \quad i = \overline{1,5}, \tag{2.2}$$

$$\Phi^5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} = [\varphi_1 \cdots \varphi_7],$$

$$\varphi_i \in \mathrm{GF}(2^5), \quad i = \overline{1,7}. \tag{2.3}$$

The matrix Φ_1^4 defines the $[5,1]2,0$ repetition code. It cannot be treated as a $[5,1]2,1$ or a $[5,1]2,2$ code since the column $(0000)^{tr}$ is not equal to a sum of one or two columns of Φ_1^4. The matrix Φ_2^4 defines a $[5,1]3$ code C. We have $(0000)^{tr} = \varphi_3 + \varphi_4 + \varphi_5$. Hence C is a $[5,1]3,0$ and a $[5,1]3,1$ code. It cannot be treated as a $[5,1]3,2$ or a $[5,1]3,3$ code since the column $(1000)^{tr}$ cannot be represented by a sum of two or three columns of Φ_2^4 and for $l = 2,3$ the representation $(1000)^{tr} = \varphi_1$ cannot be used. The matrix Φ^5 defines a code with $R = 3$. It is a $[7,2]3,2$ code, since $(00000)^{tr} = \varphi_1 + \varphi_2 + \varphi_7$, $\varphi_1 = \varphi_2 + \varphi_7$, $\varphi_3 = \varphi_4 + \varphi_5 + \varphi_6, \cdots$.

An addition of columns to a parity-check matrix of a code can increase l for fixed covering radius R.

Example 2.2: A $[Q, Q-s]4$ code with minimum distance 3 is a $[Q, Q-s]4,2$ code (see this example below). If we add to a parity-check matrix Φ^s of a $[Q, Q-s]4,0$ code a column which is a sum of two columns of Φ^s, we construct a $[Q+1, Q+1-s]4,2$ code. From the $[8,1]4,0$ repetition code, we obtain a $[9,2]4,2$ code with the parity-check matrix

$$\Phi^7 = \left[\begin{array}{cccccccc:c} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{array}\right] = [\varphi_1 \cdots \varphi_9],$$

$$\varphi_i \in \mathrm{GF}(2^7), \quad i = \overline{1,9}. \tag{2.4}$$

Here $(0000000)^{tr} = \varphi_1 + \varphi_2 + \varphi_9$, $\varphi_1 = \varphi_2 + \varphi_9$, $\varphi_2 = \varphi_1 + \varphi_9$, $\varphi_9 = \varphi_1 + \varphi_2$, $\varphi_i = \varphi_i + \varphi_1 + \varphi_2 + \varphi_9$, $i = \overline{3,8}$.

Definition 2.2: Let Φ^s be a parity-check matrix of a binary linear $[Q, Q-s]R, l$ code of length Q, codimension s, covering radius R. A *partition* K of the column set of the matrix Φ^s into nonempty subsets is called (R, l)-sufficient if for any binary column π of length s, there exists an integer $z(\pi)$ such that $R \geq z(\pi) \geq l$ and the column π can be represented by a sum of $z(\pi)$ columns of Φ^s from *distinct* subsets. No two columns from the same subset should occur in this sum.

We denote by $h(\Phi^s, l; K)$ the number of subsets in an (R, l)-sufficient partition K for a matrix Φ^s. The value of R is defined by context. Obviously, $R \leq h(\Phi^s, l; K) \leq Q$. If $h(\Phi^s, l; K) = Q$, i.e., every subset contains one column, then the partition K is called *trivial*.

We consider also the following minimum over all partitions:

$$h(\Phi^s, l) \triangleq \min_K h(\Phi^s, l; K). \tag{2.5}$$

Example 2.3: The $[4,1]2,0$ repetition code parity-check matrix is

$$\Phi^3 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} = [\varphi_1\, \varphi_2\, \varphi_3\, \varphi_4],$$

$$\varphi_i \in \mathrm{GF}(2^3), \quad i = \overline{1,4}. \tag{2.6}$$

The partition $\{\varphi_1, \varphi_2, \varphi_3\}, \{\varphi_4\}$ is $(2,0)$-sufficient. $h(\Phi^3, 0) = 2 < Q$.

Remark 2.2: Assume that we treat the same code with a parity-check matrix Φ^s as an R, l_1-object and R, l_2-object with $l_1 > l_2 \geq 0$. Let K_1 be an (R, l_1)-sufficient partition of Φ^s. Then there exists an (R, l_2)-sufficient partition K_2 such that $h(\Phi^s, l_2; K_2) \leq h(\Phi^s, l_1; K_1)$; in any case, we can take $K_2 = K_1$. So,

$$h(\Phi^s, l_2) \leq h(\Phi^s, l_1) \quad \text{for } l_2 < l_1,$$

$$\forall l, K \quad h(\Phi^s, 0) \leq h(\Phi^s, l; K). \tag{2.7}$$

Example 2.4: For the matrix Φ_2^4 of (2.2), the trivial partition K_1 gives $h(\Phi_2^4, 1; K_1) = 5$. The following partition K_2 is $(3,0)$-sufficient: $\{\varphi_1\}, \{\varphi_2\}, \{\varphi_3, \varphi_4, \varphi_5\}$. We have $h(\Phi_2^4, 0; K_2) = 3 < 5$.

For the matrix Φ^5 of (2.3), the trivial partition K_1 gives $h(\Phi^5, 2; K_1) = 7$. The following partition K_2 is $(3,1)$-sufficient: $\{\varphi_i\}$, $i = 1,2,6,7$, $\{\varphi_3, \varphi_4, \varphi_5\}$. Here $h(\Phi^5, 1; K_2) = 5 < 7$.

Remark 2.3: The number of subsets $h(\Phi^s, l; K)$ is equal to the chromatic number $h(J)$ of graph $\Gamma(J)$ considered in [7, Section 3, Remark 1].

Let 0^s be a zero matrix with s rows. The number of columns in 0^s is determined by context. We introduce matrices $B^{mR}(b)$ with $b \in \mathrm{GF}(2^m) \cup \{*\}$:

$$B^{mR}(b) \triangleq \begin{bmatrix} e_1 & \cdots & e_M \\ e_1 b & \cdots & e_M b \\ e_1 b^2 & \cdots & e_M b^2 \\ \vdots & \ddots & \vdots \\ e_1 b^{R-1} & \cdots & e_M b^{R-1} \end{bmatrix}, \quad \text{if } b \in \mathrm{GF}(2^m),$$

$$B^{mR}(*) \triangleq \left[\begin{array}{c} 0^{m(R-1)} \\ \hdashline e_1 \cdots e_M \end{array}\right], \tag{2.8}$$

where $M = 2^m$; $e_j \in \mathrm{GF}(2^m)$, $e_j b^u \in \mathrm{GF}(2^m)$, $j = \overline{1,M}$, $u = \overline{1, R-1}$; b^i is the ith power of b; $0^{m(R-1)}$ is the zero $m(R-1) \times M$ matrix; $e_i \neq e_j$ if $i \neq j$, $i, j \in \{\overline{1,M}\}$ (i.e., $\{e_1, \cdots, e_M\} = \mathrm{GF}(2^m)$). The element b is called an *indicator* of matrix $B^{mR}(b)$.

We consider the general form of a covering code parity-check matrix construction proposed in [7]. Here we call it "Construction A."

Construction A: Let a *starting code* V_0 be a binary linear $[Q, Q-s]R, l_0$ code of covering radius R with a parity-check matrix

$$\Phi^s = [\varphi_1\, \varphi_2 \cdots \varphi_Q], \qquad \varphi_i \in \mathrm{GF}(2^s), \quad i = \overline{1,Q}. \tag{2.9}$$

Let K be an (R, l_0)-sufficient partition of the column set of Φ^s into $h(\Phi^s, l_0; K)$ subsets. A *new code* V is an $[n, n-r]R_V, l$

code of covering radius R_V with a parity-check matrix $H_\epsilon^r(K)$ which has the following construction:

$$H_\epsilon^r(K) \triangleq \left[\begin{array}{c|c} 0^s & P^s(\varphi_1)\cdots P^s(\varphi_Q) \\ \hline D_\epsilon^{mR} & B^{mR}(b_1)\cdots B^{mR}(b_Q) \end{array}\right], \qquad r = s + mR, \tag{2.10}$$

where $m \geq 1$ is an integer; ϵ is an index of matrices D_ϵ^{mR} and $H_\epsilon^r(K)$; D_ϵ^{mR} is an $mR \times N(m)$ matrix (its structure and the number of columns $N(m)$ are defined separately); 0^s is the zero $s \times N(m)$ matrix; and $P^s(\varphi_i)$ is an $s \times 2^m$ matrix with equal columns φ_i, i.e., $P^s(\varphi_i) = [\varphi_i \cdots \varphi_i]$. The assignment of indicators b_i depends on the partition K in the following way: if columns φ_i and φ_j from Φ^s belong to distinct subsets of the partition K, then the inequality $b_i \neq b_j$ should be true; if columns φ_u and φ_t belong to the same subset of K, then we are free to assign the equality $b_u = b_t$ or the inequality $b_u \neq b_t$.

Note that for the trivial partition K, all indicators b_i should be distinct, i.e., $b_i \neq b_j$ if $i \neq j$. Note also that the index ϵ is useful to distinguish variants of matrices D_ϵ^{mR} and $H_\epsilon^r(K)$.

Denote by β the set of indicators of the matrices $B^{mR}(b_i)$ in (2.10):

$$\beta \triangleq \bigcup_{i=1}^{Q} \{b_i\}. \tag{2.11}$$

Construction A defines the *general form* of the parity-check matrix of a new code V. To obtain a concrete matrix from the general form in (2.10), we should construct submatrix D_ϵ^{mR} and give the set of indicators β and the value of parameter m. These problems are considered in detail in Sections III–V for codes with $R = 2, 3, 4$.

Directly from the construction in (2.10) it follows that the new $[n, n-r]R_V, l$ code V has codimenison $r = s + mR$, length $n = 2^m Q + N(m)$, where $N(m)$ is the number of columns in submatrix D_ϵ^{mR}, and covering radius $R_V \geq R$. In Sections III–V, we design submatrix D_ϵ^{mR} and set β such that the equality $R_V = R$ holds.

Without going into detail, note that indicator set β and bounds for the m value will be designed by one of the following ways:

Case A1:

$$\beta \subseteq \mathrm{GF}(2^m) \cup \{*\} \setminus T, \qquad 2^m + 1 - |T| \geq h(\Phi^s, l_0; K). \tag{2.12}$$

Case A2:

$$\beta = \mathrm{GF}(2^m) \cup \{*\} \setminus T, \qquad Q \geq 2^m + 1 - |T| \geq h(\Phi^s, l_0; K). \tag{2.13}$$

Here T is some set, and $|T|$ is the cardinality of T. We will give T for every concrete situation (see Theorems 3.1–5.1). For Case A2, we *must* use *all* elements of the set $\mathrm{GF}(2^m) \cup \{*\} \setminus T$ as indicators b.

We use Construction A iteratively. We can use a parity-check matrix $H_\epsilon^r(K)$ of a code V obtained on the ith step as a parity-check matrix Φ^r of a starting code V_0 for the $(i+1)$th step. In this process, we may consider the same starting code V_0 with distinct values of l_0 to use both Case A1 and Case A2 and different variants of these cases. (See, (2.7), Remark 2.2, and Examples 4.2, 5.1, 5.6.) Estimates of l and $h(H_\epsilon^r(K), l)$ for new codes V are important for the remarked iterative process. We give these estimates in Theorem 3.1–5.1. (In [7], such estimates are not described.)

We introduce notations for submatrices of matrix $H_\epsilon^r(K)$ in (2.10):

$$L_i^r \triangleq \left[\begin{array}{c} P^s(\varphi_i) \\ \hline B^{mR}(b_i) \end{array}\right], \qquad i = \overline{1, Q}; \qquad \Psi_\epsilon^r \triangleq \left[\begin{array}{c} 0^s \\ \hline D_\epsilon^{mR} \end{array}\right]. \tag{2.14}$$

We denote by $L(f)$ the union of columns of all submatrices L_i^r having the same indicator $b_i = f$, where $i \in \overline{\{1, Q\}}$, $f \in \beta$. Let W^m be a parity-check matrix of the $[2^m - 1, 2^m - 1 - m]1$ Hamming code containing all nonzero columns of length m. Let $\gamma, w, d \in \mathrm{GF}(2^m)$ be columns of this matrix. Denote by W_γ^m the matrix W^m with column γ omitted.

Example 2.5: The matrix D^6 is obtained by ADS of two Hamming codes:

$$D^6 = \left[\begin{array}{cccccc|c|cccccc} 0&0&1&1&1&1&0&0&0&0&0&0&0 \\ 1&1&0&0&1&1&0&0&0&0&0&0&0 \\ 0&1&0&1&0&1&1&0&0&0&0&0&0 \\ \hline 0&0&0&0&0&0&0&0&0&1&1&1&1 \\ 0&0&0&0&0&0&0&1&1&0&0&1&1 \\ 0&0&0&0&0&0&1&0&1&0&1&0&1 \end{array}\right]$$

$$= \left[\begin{array}{c|c|c} W_\gamma^3 & \gamma & 0^3 \\ \hline 0^3 & \gamma & W_\gamma^3 \end{array}\right], \qquad \gamma = (001)^{tr}. \tag{2.15}$$

Let $U \triangleq (\pi, u_1, \cdots, u_R)^{tr}$, $\pi \in \mathrm{GF}(2^s)$, $u_i \in \mathrm{GF}(2^m)$, $i = \overline{1, R}$, i.e., U is a column of $\mathrm{GF}(2^r)$, $r = s + mR$. Proofs of the equality $R_V = R$ in Theorem 3.1–5.1 are based on Fact 2.1. We should represent any column U as a sum of at most R columns of matrix $H_\epsilon^r(K)$. The basic idea of the proof lies in the following. Let $\pi = \varphi_{j_1} + \cdots + \varphi_{j_z}$, where $\varphi_{j_1}, \cdots, \varphi_{j_z}$ belong to distinct subsets of K and $R \geq z > 0$. Then by definition of matrix $H_\epsilon^r(K)$ (see (2.10)), *all indicators* $b_{j_1}, \cdots, b_{j_z}$ *are distinct*. This allows us to solve some system of z linear equations and to find z columns (one column of each submatrix $L_{j_1}^r, \cdots, L_{j_z}^r$) such that their sum S coincides with U in z elements $u_{\tau_1}, \cdots, u_{\tau_z}$. If $R > z$, we add $R - z$ columns of submatrix Ψ_ϵ^r to the sum S. The added columns contain zeros in positions corresponding to $u_{\tau_1}, \cdots, u_{\tau_z}$. If $l_0 = 0$, then for $\pi = 0$ we have $z = 0$. For Case A1 in the situation $l_0 = 0$, the submatrix D_ϵ^{mR} is a parity-check matrix of a code with covering radius R. For Case A2 when $\pi = 0$ (and in some other situations), we calculate some indicator b_ξ and use the sum of two columns of submatrix L_ξ^r. The indicator b_ξ always exists since $\beta = \mathrm{GF}(2^m) \cup \{*\} \setminus T$.

The new codes V are normal by Theorem 32 of [6], which shows that if a linear binary code has length $n \leq 12$, or minimal distance $d \leq 3$, or covering radius $R \leq 2$, then this code is normal. We show that codes V with $R = 3, 4$ have $d = 3$. We can use codes V in construction ADS [10].

For some examples in Sections III–V, we tested codes using a computer. For most of these examples there are proofs based on Fact 2.1. To save space we omit these proofs. For short we may write H_ϵ^r instead of $H_\epsilon^r(K)$. For $R = 2, 3, 4$, we write mR by $2m, 3m, 4m$. If in a column sum S representing a column U some summand is equal to the zero column, then this summand is treated to be absent. In summands of the form $(\varphi_f, 0, w)^{tr}$, $(0, 0, w, 0)^{tr}$, etc., the value of w is defined by context.

III. Codes with Covering Radius $R = 2$

Theorem 3.1: Let a starting code V_0 be a $[Q, Q - s]2, 0$ code with a parity-check matrix Φ^s of the form (2.9). Let K be a

(2, 0)-sufficient partition of Φ^s into $h(\Phi^s, 0; K)$ subsets. We define a new code V by a parity-check matrix $H_\epsilon^r(K)$ of the form (2.10), where indicator set β (see (2.11)), parameter m, and submatrix D_ϵ^{2m} are chosen by one of the following ways:

Case A1:

$$\beta \subseteq \mathrm{GF}(2^m) \cup \{*\}, \qquad 2^m + 1 \geq h(\Phi^s, 0; K),$$
$$D_1^{2m} \triangleq \begin{bmatrix} W^m & 0^m \\ 0^m & W^m \end{bmatrix}. \tag{3.1}$$

Case A2:

$$\beta = \mathrm{GF}(2^m), \qquad Q \geq 2^m \geq h(\Phi^s, 0; K), \qquad D_2^{2m} \triangleq \begin{bmatrix} 0^m \\ W^m \end{bmatrix}. \tag{3.2}$$

Then V is a normal $[n, n-r]2, 0$ code with $r = s + 2m$ and parameters:

Case A1:

$$n = 2^m(Q+2) - 2, \qquad h(H_1^r(K), 0) \leq h(\Phi^s, 0; K). \tag{3.3}$$

Case A2:

$$n = 2^m(Q+1) - 1, \qquad h(H_2^r(K), 0) \leq 2 \times 2^m + 1. \tag{3.4}$$

Proof: We prove Cases A1 and A2 considering examples of representation for columns $U = (\pi, u_1, u_2)^{tr} \in \mathrm{GF}(2^r)$, $\pi \in \mathrm{GF}(2^s)$, $u_1, u_2 \in \mathrm{GF}(2^m)$.

1) $\pi = \varphi_i + \varphi_j$; φ_i and φ_j belong to distinct subsets of K; $b_i \neq b_j$.

Cases A1 and A2: Let $b_i, b_j \neq *$. We find x and y solving the system $x b_i^{\delta-1} + y b_j^{\delta-1} = u_\delta$, $\delta = 1, 2$. Now $U = (\varphi_i, x, x b_i)^{tr} + (\varphi_j, y, y b_j)^{tr}$.

Case A1: $b_j = *$. $U = (\varphi_i, u_1, u_1 b_i)^{tr} + (\varphi_j, 0, w)^{tr}$, $w = u_1 b_i + u_2$.

2) $\pi = \varphi_i$.

Cases A1 and A2: If $b_i \neq *$, then $U = (\varphi_i, u_1, u_1 b_i)^{tr} + (0, 0, w)^{tr}$.

Case A1: $b_i = *$. $U = (\varphi_i, 0, u_2)^{tr} + (0, u_1, 0)^{tr}$.

3) $\pi = 0$.

Case A1: $U = (0, u_1, 0)^{tr} + (0, 0, u_2)^{tr}$.

Case A2: Let $u_1 \neq 0$. Since $\beta = \mathrm{GF}(2^m)$, indicator $b_\xi = u_2/u_1$ always exists and $U = (\varphi_\xi, 0, 0)^{tr} + (\varphi_\xi, u_1, u_1 b_\xi)^{tr}$. If $u_1 = 0$, $U = (0, 0, u_2)^{tr}$.

To estimate $h(H_1^r(K), 0)$, we partition columns of $H_1^r(K)$ (except submatrix Ψ_1^r) in accordance with the partition K of matrix Φ^s: if columns φ_i, φ_j of Φ^s belong to distinct subsets of K, then columns of submatrices L_i^r, L_j^r belong to distinct subsets of the partition of $H_1^r(K)$. For definiteness we assume that the first (resp., second) subset does not contain submatrices L_i^r with $b_i = 0$ (resp., $b_i = *$). Taking into account the case $\pi = \varphi_i$, we inscribe the columns of Ψ_1^r of the form $(0, 0, w)^{tr}$ (resp., $(0, w, 0)^{tr}$ in the first (resp., second) subset. To estimate $h(H_2^r(K), 0)$, we obtain 2×2^m subsets partitioning every union $L(f)$ in two subsets such that the first subset contains all columns of the form $(\varphi_i, 0, 0)^{tr}$ and the second subset contains the rest of the columns. The $(2 \times 2^m + 1)$th subset consists of columns of Ψ_2^r. From the considered representations of U, it follows that these partitions of $H_1^r(K)$ and $H_2^r(K)$ are (2, 0)-sufficient.

By Theorem 32 of [6], the code V is normal since it has $R = 2$. □

Note that Case A1 corresponds to condition 2 of Theorems 2 and 4 in [7].

Example 3.1: In the first step of an iterative process, the $[5, 1]2, 0$ code with the parity-check matrix Φ_1^4 of (2.1) is a starting code V_0 with $h(\Phi_1^4, 0) = 5$. We design three new codes V_1, V_2, V_3 for $m = 2, 3, 4$, respectively. Directly using Case A1 of (3.1) and (3.3) with $m = 2$, we design a $[26, 18]2, 0$ code V_1 with $h(H_1^8, 0) \leq 5$. For $m = 3, 4$, we construct the parity-check matrix $H_\epsilon^r(K)$ of the form (2.10) with special indicator sets β and submatrices D_ϵ^{2m}. For $m = 3$, we take $D_{11}^{2m} = D^6$ (see (2.15)) and $\beta = \{0, \alpha, \alpha+1, \alpha^2+1, \alpha^2+\alpha\}$, where α is a primitive element of $\mathrm{GF}(2^3)$. We obtain $[53, 43]2, 0$ code V_2 with $h(H_{11}^{10}, 0) \leq 9$. (The same code is described in Theorem 5 of [7].) For $m = 4$, we take $\beta = \{0, 1, \alpha, \alpha^2, *\}$, where α is a primitive element of $\mathrm{GF}(2^4)$, and

$$D_{12}^{2m} = \left[\begin{array}{ccccccc|c}
000 & 0000 & 1111 & 111 & 1111 & 0000 & 0000 & 1 \\
000 & 1111 & 0000 & 111 & 1111 & 0000 & 0000 & 1 \\
011 & 0011 & 0011 & 011 & 0011 & 0011 & 0000 & 1 \\
101 & 0101 & 0101 & 101 & 0101 & 0101 & 0000 & 1 \\
000 & 0000 & 0000 & 000 & 0000 & 1111 & 1111 & 0 \\
000 & 0000 & 0000 & 000 & 1111 & 0000 & 1111 & 0 \\
000 & 0000 & 0000 & 101 & 0011 & 0110 & 0011 & 0 \\
000 & 0000 & 0000 & 011 & 0110 & 0101 & 0101 & 0
\end{array}\right]. \tag{3.5}$$

This 8×27 matrix is a modified form of the parity-check matrix of the $[26, 18]2, 0$ code V_1 with the last additional column. We obtain a $[107, 95]2, 0$ code V_3 with $h(H_{12}^{12}, 0) \leq 32$. We tested the codes V_2 and V_3 and the estimates of $h(H_{11}^{10}, 0)$ and $h(H_{12}^{12}, 0)$ using a computer.

For $i \geq 2$ on the ith step of the iterative process, we directly use Case A2 of (3.2) and (3.4). Codes designed on the $(i-1)$th step are starting codes for the ith step. Let $f(r) \triangleq 27 \times 2^{t-4} - 1$ for $r = 2t$. The $[Q, Q-s]2, 0$ codes V_1, V_2, and V_3 have $Q = f(s)$. Hence (see (3.4)) all $[n, n-r]2, 0$ codes obtained by the iterative process have $n = f(r)$.

In the second step, the condition $Q \geq 2^m \geq h(\Phi^s, 0; K)$ holds for $m = 3, 4$, $m = 4, 5$, and $m = 5, 6$ if a starting code is V_1, V_2, and V_3, respectively. We obtain codes C_1, C_2 with $n = 215, 431$, $r = 14, 16$, $h(H_2^r, 0) \leq 17, 33$ (for starting code V_1 and $m = 3, 4$), codes C_3, C_4 with $n = 863, 1727$, $r = 18, 20$ (for starting code V_2 and $m = 4, 5$), and codes C_5, C_6 with $n = 3455, 6911$, $r = 22, 24$ (for starting code V_3 and $m = 5, 6$).

Take a $[f(s), f(s) - s]2, 0$ code with $s = 2k \geq 8$ as a starting code for Case A2 with $m = \mu$. We obtain a $[f(r), f(r) - r]2, 0$ code C with $r = 2t$, $t = \mu + k$, $h(H_2^r(K), 0) \leq 2 \times 2^\mu + 1$. We next use C as a starting code for Case A2 with $m = M$. The inequality in (3.2) has the form $27 \times 2^{t-4} - 1 \geq 2^M \geq 2 \times 2^\mu + 1$. It holds for $M = \overline{\mu + 2, t}$. Using these values of M, we construct $t - \mu - 1 = k - 1$ new $[f(\rho), f(\rho) - \rho]2, 0$ codes Y with $\rho = 2\tau$, $\tau = \overline{t + \mu + 2, 2t}$. Since $k \geq 4$, codes Y with $\tau = 2t - 1, 2t$ will always be obtained. So, if we have a series of codes C with $t = \overline{a, 2a-2}$, we can design a sequence of codes Y with $\tau = \overline{2a-1, 4a-4}$. Now we can take this sequence of codes Y as starting codes and obtain a series of new $[f(r), f(r) - r]2, 0$ codes with $r = 2t$, $t = \overline{4a-3, 8a-8}$, etc.

Codes $C_1, \cdots, C_6$ designed in the second step form a required series of codes C with $t = \overline{7, 12}$. So, we proved that the considered iterative process forms an infinite family of $[n, n-r]2, 0$ codes with $R = 2$, $r = 2t$, $t \geq 4$, $n = 27 \times 2^{t-4} - 1$, $\overline{\mu}(2) \approx 1.4238$ (see (1.3)).

Really we obtain also codes Y with $\tau \leq 2t - 2$ and can construct for the described family different codes with the same parameters.

Remark 3.1: Taking the $[4, 1]2, 0$ code of (2.6) as a starting code and directly using Case A2, we can design codes with $R = 2$, $r = 2t - 1 \geq 7$, $r \neq 9, 13, 17, 25, 33$, $n = 5 \times 2^{t-2} - 1$, that have the same parameters as the codes of [9]. But these codes and the codes of [9] differ in structure.

IV. Codes with Covering Radius $R = 3$

Denote by A^{2m} a parity-check matrix of a code with covering radius $R = 2$ and codimension $r = 2m$. Let λ_{2m} be the length of this code.

Theorem 4.1: Let a starting code V_0 be a $[Q, Q-s]3, l_0$ code with parity-check matrix Φ^s of the form (2.9). Let K be a $(3, l_0)$-sufficient partition of Φ^s into $h(\Phi^s, l_0; K)$ subsets. We define a new code V by a parity-check matrix $H^r_\epsilon(K)$ of the form (2.10), where indicator set β (see (2.11)), parameter m, and submatrix D^{3m}_ϵ are chosen by one of the following ways:

Case A1:

i) $l_0 = 0, \quad \beta \subseteq GF(2^m) \setminus \{0\}, \quad 2^m - 1 \ge h(\Phi^s, 0; K),$

$$D^{3m}_{10} \triangleq \begin{bmatrix} W^m & 0^m \\ 0^{2m} & A^{2m} \end{bmatrix}, \tag{4.1}$$

ii) $l_0 = 1, \quad \beta \subseteq GF(2^m), \quad 2^m \ge h(\Phi^s, 1; K),$

$$D^{3m}_{11} \triangleq \begin{bmatrix} 0^m & 0^m \\ W^m & 0^m \\ 0^m & W^m \end{bmatrix}, \tag{4.2}$$

iii) $l_0 = 2, \quad \beta \subseteq GF(2^m) \cup \{*\}, \quad 2^m + 1 \ge h(\Phi^s, 2; K),$

$$D^{3m}_{12} \triangleq \begin{bmatrix} 0^m \\ W^m \\ 0^m \end{bmatrix}. \tag{4.3}$$

Case A2:

$$\forall l_0, \quad \beta = GF(2^m) \cup \{*\}, \quad Q \ge 2^m + 1 \ge h(\Phi^s, l_0; K),$$
$$D^{3m}_2 \triangleq D^{3m}_{12}. \tag{4.4}$$

Then V is an $[n, n-r]3, l$ code with $r = s + 3m$ and parameters:

Case A1:

i) $$n = 2^m(Q+1) + \lambda_{2m} - 1, \quad l \ge 1, \tag{4.5}$$

ii) $$n = 2^m(Q+2) - 2, \quad l = 2,$$
$$h(H^r_{11}(K), 1) \le h(\Phi^s, 1; K) + 2, \tag{4.6}$$

iii) $$n = 2^m(Q+1) - 1, \quad l = 2,$$
$$h(H^r_{12}(K), 2) \le h(\Phi^s, 2; K) + 1. \tag{4.7}$$

Case A2:

$$n = 2^m(Q+1) - 1, \quad l = 2 \quad \text{for } m \ge 2,$$
$$h(H^r_2(K), l_0) \le 2(2^m + 1) + 1. \tag{4.8}$$

Besides, if $m \ge 2$ or $n \le 12$, then V is a normal $[n, n-r]3$ code.

Proof: We prove Cases A1 and A2 considering examples of representation for columns $U = (\pi, u_1, u_2, u_3)^{tr}$, $\pi \in GF(2^s)$, $u_1, u_2, u_3 \in GF(2^m)$.

1) $\pi = \varphi_i + \varphi_j + \varphi_k$; φ_i, φ_j, and φ_k belong to distinct subsets of K; b_i, b_j, and b_k are distinct.

Cases A1 i–A1iii, A2: Let $b_i, b_j, b_k \neq *$. We find x, y, z solving the system $xb_i^{\delta-1} + yb_j^{\delta-1} + zb_k^{\delta-1} = u_\delta$, $\delta = 1, 2, 3$. Now $U = (\varphi_i, x, xb_i, xb_i^2)^{tr} + (\varphi_j, y, y_j^b, yb_j^2)^{tr} + (\varphi_k, z, zb_k, zb_k^2)^{tr}$. If $b_k = *$, the system takes the form $xb_i^{\delta-1} + yb_j^{\delta-1} = u_\delta$, $\delta = 1, 2$, and the third summand is $(\varphi_k, 0, 0, w)^{tr}$.

2) $\pi = \varphi_i + \varphi_j$; φ_i and φ_j belong to distinct subsets of K; $b_i \neq b_j$. If $b_i, b_j \neq *$, then $U = (\varphi_i, x, xb_i, xb_i^2)^{tr} + (\varphi_j, y, yb_j, yb_j^2)^{tr} + F$, where x, y are a solution of the system $xb_i^{\delta-1} + yb_j^{\delta-1} = u_\delta$; $\delta = 2, 3$ and $F = (0, w, 0, 0)^{tr}$ for Case A1 i; $\delta = 1, 3$ and $F = (0, 0, w, 0)^{tr}$ for Cases A1ii, A1iii, and A2. Note that $\beta \cap \{0\} = \varnothing$ for Case A1i.

If $b_j = *$, then $U = (\varphi_i, u_1, u_1 b_i, u_1 b_i^2)^{tr} + (\varphi_j, 0, 0, \gamma)^{tr} + (0, 0, w, 0)^{tr}$.

3) $\pi = \varphi_i$. (Here we do not consider Case A1iii.)

Cases A1i and A1ii: $U = (\varphi_i, u_1, u_1 b_i, u_1 b_i^2)^{tr} + P$, where P is a sum of at most two columns of submatrix Ψ^r_ϵ (see the definition of A^{2m}).

Case A2: Let $b_i \neq *$, $u_2 \neq u_1 b_i$, $u_3 \neq u_1 b_i^2$. Take $b_\xi = (u_3 + u_2 b_i)/(u_2 + u_1 b_i) \neq b_i$, $x = (u_1 b_\xi + u_2)/(b_i + b_\xi)$, $y = (u_1 b_i + u_2)/(b_i + b_\xi)$. Then $U = (\varphi_i, x, xb_i, xb_i^2)^{tr} + (\varphi_\xi, 0, 0, 0)^{tr} + (\varphi_\xi, y, yb_\xi, yb_\xi^2)^{tr}$.

Let $b_i \neq *$, $u_2 = u_1 b_i$, $u_3 \neq u_1 b_i^2$. Take $b_\xi = *$, $w = u_3 + u_1 b_i^2$. Then $U = (\varphi_i, u_1, u_1 b_i, u_1 b_i^2)^{tr} + (\varphi_\xi, 0, 0, 0)^{tr} + (\varphi_\xi, 0, 0, w)^{tr}$.

Let $b_i = *$, $u_1 \neq 0$. Take $b_\xi = u_2/u_1$, $w = u_3 + u_1 b_\xi^2$. Then $U = (\varphi_i, 0, 0, w)^{tr} + (\varphi_\xi, u_1, u_1 b_\xi, u_1 b_\xi^2)^{tr} + (\varphi_\xi, 0, 0, 0)^{tr}$.

4) $\pi = 0$. (Here we do not consider Cases A1ii and A1iii.)

Case A1i: D^{3m}_{10} is a parity-check matrix of a code with $R = 3$.

Case A2: Let $u_1 \neq 0$, $u_2^2 \neq u_1 u_3$. Take $b_\xi^2 = u_3/u_1$, $w = u_2 + u_1 b_\xi$. Then $U = (\varphi_\xi, u_1, u_1 b_\xi, u_1 b_\xi^2)^{tr} + (\varphi_\xi, 0, 0, 0)^{tr} + (0, 0, w, 0)^{tr}$.

For $\pi = \varphi_i$, $\pi = 0$, the indicators b_ξ exist since $\beta = GF(2^m) \cup \{*\}$.

The estimate of $h(H^r_2(K), l_0)$ in (4.8) is obtained in perfect analogy to the estimate in (3.4). To estimate $h(H^r_{11}(K), 1)$ in (4.6), we partition columns of $H^r_{11}(K)$ (except submatrix Ψ^r_{11}) in accordance with partition K of matrix Φ^s, i.e., if columns φ_i and φ_j of Φ^s belong to distinct subsets of K, then columns of submatrices L^r_i and L^r_j belong to distinct subsets of the partition of $H^r_{11}(K)$. Also, we form two subsets from columns of Ψ^r_{11} having the form $(0, 0, w, 0)^{tr}$ and $(0, 0, 0, w)^{tr}$, respectively. The estimate of $h(H^r_{12}(K), 2)$ in (4.7) is similar. Since $h(\Phi^S, l_0) \ge R = 3$, we have $m \ge 2$ in Cases A1i and A1ii. Clearly, for $m \ge 2$ the zero column is a sum of three columns of W^m, every column of W^m is a sum of two columns of W^m, and every column of the submatrix L^r_i is a sum of three columns of it. Hence, we have $l \ge 1$ in (4.5) and $l = 2$ in (4.6) and (4.8). In (4.7) we have $l = 2$ since $l_0 = 2$. For $m \ge 2$, the new code V has minimal distance $d = 3$ (see W^m in (4.1)–(4.4)). By Theorem 32 of [6], an $[n, n-r]$ code is normal if $d \le 3$ or $n \le 12$. □

Cases A1i and A1ii correspond to conditions 4 and 5 of Theorems 2 and 4 in [7].

Example 4.1: V_0 is the $[7, 2]3, 2$ code of Examples 2.1 and 2.4. Case A1iii for $m \ge 3$ gives an infinite family of $[n, n-r]3, l$ codes with

$$R = 3, \quad l = 2, \quad r = 3t - 1, \quad t \ge 5,$$
$$n = 2^{t+1} - 1, \quad \overline{\mu}(3) \approx 2.6667. \tag{4.9}$$

Example 4.2: The $[23, 12]3, 0$ Golay code is a code V_0 for Case A1i. We take the parity-check matrices of codes in (1.3) obtained in Example 3.1 as A^{2m} and obtain a family of $[n, n-r]3, l$ codes with

$$R = 3, \quad l \ge 1, \quad r = 3t - 1, \quad t \ge 9,$$
$$n = 411 \times 2^{t-8} - 2, \quad \overline{\mu}(3) \approx 1.3794. \tag{4.10}$$

The first code of the family uses the parity-check matrix H^{10}_{11} of the $[53, 43]2, 0$ code obtained in Example 3.1 as matrix A^{2m}. We tested using a computer that this first code is an $[820, 794]3, 2$ code with $h(H^{26}_{10}, 2) \le 820$, $h(H^{26}_{10}, 0) \le 33$. We use it as V_0 for Case A2, $m = \overline{5, 9}$, and Case A1iii, $m \ge 10$. Thus we obtain a family of $[n, n-r]3, 2$ codes with $R = 3$, $r = 3t - 1$, $t \geq 14$, $n = 821 \times 2^{t-9} - 1$, $\overline{\mu}(3) \approx 1.3744$ (see (1.4)).

Example 4.3: V_0 is the $[5,1]3,1$ code with parity-check matrix Φ_2^4, $h(\Phi_2^4, 0) \leq 3$ (see Examples 2.1 and 2.4). We use Case A2, $m = 1, 2$, and obtain an $[11,4]3,1$ code with the parity-check matrix

$$H_2^7 = \left[\begin{array}{c|ccccc} 0 & 11 & 00 & 00 & 00 & 00 \\ 0 & 00 & 11 & 00 & 00 & 00 \\ 0 & 00 & 00 & 11 & 00 & 11 \\ 0 & 00 & 00 & 00 & 11 & 11 \\ 0 & 01 & 01 & 00 & 00 & 00 \\ 1 & 00 & 01 & 00 & 00 & 00 \\ 0 & 00 & 01 & 01 & 01 & 01 \end{array}\right] = [h_1 \cdots h_{11}],$$

$$h_i \in GF(2^7), \quad i = \overline{1,11}, \quad (4.11)$$

$h(H_2^7, 0) \leq 7$, and a $[23,13]3,2$ code with $h(H_2^{10}, 0) \leq 11$. Using the $[11,4]3,1$ code as V_0 for Case A2, $m = 3$, we obtain a $[95,79]3,2$ code. The designed $[23,13]3,2$ code has a larger length than the $[22,12]3,0$ shortened Golay code, but its parameters l and $h(H_2^{10}, 0)$ are better. Using the $[23,13]3,2$ code as V_0 for Case A2, $m = 4$, and Case A1iii, $m \geq 5$, we generate an infinite family of $[n, n-r]3, l$ codes with

$$R = 3, \quad l = 2, \quad r = 3t - 2, \quad t \geq 8,$$
$$n = 3 \times 2^{t-1} - 1, \quad \overline{\mu}(3) \approx 2.25. \quad (4.12)$$

Example 4.4: V_0 is the $[7,1]3,0$ repetition code. For Case A1i, $m \geq 4$, we take the parity-check matrices of codes in (1.3) as A^{2m} and generate an infinite family of $[n, n-r]3, l$ codes with parameters

$$R = 3, \quad l \geq 1, \quad r = 3t, \quad t \geq 6,$$
$$n = 155 \times 2^{t-6} - 2, \quad \overline{\mu}(3) \approx 2.3676. \quad (4.13)$$

Now we consider some special forms of submatrix D_ϵ^{3m} and β.

Example 4.5: V_0 is the $[7,1]3,0$ code, $m = 3$, $\beta = GF(2^3) \setminus \{0\}$, and D_ϵ^{3m} has the form

$$D_{13}^{3m} = \begin{bmatrix} W^3 & 0^3 \\ 0^6 & Y^6 \end{bmatrix}, \quad Y^6 = \left[\begin{array}{c|c} W_\gamma^3 & P^3(\gamma) \\ P^3(\gamma) & W_\gamma^3 \end{array}\right],$$

$$\gamma = (001)^{tr}. \quad (4.14)$$

$P^3(\gamma)$ is a matrix of six equal columns γ. We verified using a computer that a $[75,60]3,2$ code V_{31} with $h(H_{13}^{15}, 2) \leq 23$ is obtained. Now again V_0 is the $[7,1]3,0$ code, $m = 3$, $\beta = GF(2^3) \setminus \{1\}$, and D_ϵ^{3m} has the form

$$D_{14}^{3m} = \left[\begin{array}{c|c|c|c} W_\gamma^3 & 0^3 & 0^3 & \gamma \\ 0^3 & W_\gamma^3 & 0^3 & \gamma \\ 0^3 & 0^3 & W_\gamma^3 & \gamma \end{array}\right], \quad \gamma = (001)^{tr}. \quad (4.15)$$

We tested using a computer that a $[75,60]3,1$ code V_{32} with $h(H_{14}^{15}, 1) \leq 14$ is obtained. So, we have two distinct codes V_{31} and V_{32} with the same parameters n and r, but with distinct values of l and $h(H_\epsilon^{15}, l)$. We next use directly Theorem 4.1 in the following situations: Case A2, $m = 4$, V_0 is code V_{32}; Case A2, $m = 5, 6$, V_0 is code V_{31} or V_{32}; Case A1iii, $m \geq 7$, V_0 is code V_{31}. We obtain a family of $[n, n-r]3, l$ codes with

$$R = 3, \quad l = 2, \quad r = 3t, \quad t \geq 9,$$
$$n = 19 \times 2^{t-3} - 1, \quad \overline{\mu}(3) \approx 2.2327. \quad (4.16)$$

Example 4.6: V_0 is the $[11,4]3,1$ code of Example 4.3. We construct a $(3,1)$-sufficient partition for matrix H_2^7 as follows: $\{h_1\}, \cdots, \{h_6\}, \{h_8\}, \{h_7, h_9, h_{10}, h_{11}\}$. $h(H_2^7, 1) \leq 8$. We take $m = 4$, $\beta = \{0, \alpha, \alpha^2, \alpha^2 + \alpha, \alpha^3, \alpha^3 + \alpha, \alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + \alpha\}$, α is a primitive element of $GF(2^4)$,

$$D_{15}^{3m} = \left[\begin{array}{c|c|c} 0^4 & 0^4 & 0^4 \\ W_\gamma^4 & \gamma & 0^4 \\ 0^4 & \gamma & W_\gamma^4 \end{array}\right], \quad \gamma = (0001)^{tr} = \alpha^0. \quad (4.17)$$

We tested using a computer that a $[205,186]3,1$ code is obtained.

Example 4.7: Let $D_\epsilon^{3m} = D_{11}^{3m}$, $B^{3m}(\sharp) \triangleq D_{12}^{3m}$, $\beta = GF(2^m) \cup \{*, \sharp\}$, $m = 3$ (see (4.2) and (4.3)). V_0 is the $[14,6]3,0$ code [10] with the parity-check matrix

$$\Phi^8 = \begin{bmatrix} 100 & 000 & 00 & 00 & 11 & 01 \\ 010 & 000 & 00 & 00 & 11 & 10 \\ 001 & 000 & 00 & 01 & 01 & 01 \\ 000 & 100 & 00 & 01 & 01 & 10 \\ 000 & 010 & 00 & 10 & 01 & 01 \\ 000 & 001 & 00 & 10 & 01 & 10 \\ 000 & 000 & 10 & 11 & 10 & 01 \\ 000 & 000 & 01 & 11 & 10 & 10 \end{bmatrix} = [\varphi_1, \cdots, \varphi_{14}],$$

$$\varphi_i \in GF(2^8), \quad i = \overline{1,14}.$$

Let K be a partition of Φ^8 of the form $\{\varphi_i, \varphi_{i+1}\}$, $i = 1, 3, 5, 13$, $\{\varphi_j\}$, $j = \overline{7,12}$. We tested using a computer that K is $(3,0)$-sufficient. Take $b_1 = b_2 = 1$, $b_3 = b_4 = \alpha$, $b_5 = b_6 = \alpha^2$, $b_7 = \alpha^3$, $b_8 = \alpha^4$, $b_9 = \alpha^5$, $b_{10} = \alpha^6$, $b_{11} = *$, $b_{12} = \sharp$, $b_{13} = b_{14} = 0$, where α is a primitive element of $GF(2^3)$. We tested using a computer that $[126,109]3,2$ code is obtained.

V. Codes with Covering Radius $R = 4$

Theorem 5.1: Let a starting code V_0 be a $[Q, Q-s]4, l_0$ code with a parity-check matrix Φ^s of the form (2.9). Let K be a $(4, l_0)$-sufficient partition of Φ^s into $h(\Phi^s, l_0; K)$ subsets. We introduce the notation $h_0 \triangleq h(\Phi^s, l_0; K)$. We define a new code V by a parity-check matrix $H_\epsilon^r(K)$ of the form (2.10), where indicator set β (see (2.11)), parameter m, and submatrix D_ϵ^{4m} are chosen by one of the following ways:

Case A1:

i) $$l_0 = 2, \quad \beta \subseteq GF(2^m), \quad 2^m \geq h_0,$$

$$D_{11}^{4m} \triangleq \begin{bmatrix} 0^{2m} & 0^{2m} \\ W^m & 0^m \\ 0^m & W^m \end{bmatrix}, \quad (5.1)$$

ii) $$l_0 = 2, \quad \beta \subseteq GF(2^m) \cup \{*\}, \quad 2^m + 1 \geq h_0, \quad m \text{ is odd},$$

$$D_{12}^{4m} \triangleq \begin{bmatrix} 0^m & 0^m \\ W^m & 0^m \\ 0^m & W^m \\ 0^m & 0^m \end{bmatrix}, \quad (5.2)$$

iii) $$l_0 = 2, \quad \beta \subseteq \{1, \alpha, \alpha^2, \cdots, \alpha^c\}, \quad c = \lfloor (2^m + 2)/3 \rfloor,$$

$$c + 1 \geq h_0, \quad D_{13}^{4m} \triangleq \left[\begin{array}{c|c|c} W_\gamma^m & \gamma & 0^m \\ 0^{2m} & 0^{2m} & 0^{2m} \\ 0^m & \alpha & W_\alpha^m \end{array}\right],$$

$$\gamma = (0 \cdots 01)^{tr} = \alpha^0, \quad (5.3)$$

where $\alpha = (0 \cdots 010)^{tr}$ is a primitive element of GF(2^m);

iv) $l_0 = 3, \quad \beta \subseteq \mathrm{GF}(2^m), \quad 2^m \geq h_0,$

$$D_{14}^{4m} \triangleq \begin{bmatrix} 0^{3m} \\ W^m \end{bmatrix}. \tag{5.4}$$

Case A2:

j) $l_0 = 0, \quad \beta = \mathrm{GF}(2^m) \cup \{*\}, \quad Q \geq 2^m + 1 \geq h_0,$

$$D_{21}^{4m} \triangleq \begin{bmatrix} 0^m & 0^m & 0^m \\ W^m & 0^m & 0^m \\ 0^m & W^m & 0^m \\ 0^m & 0^m & W^m \end{bmatrix}, \tag{5.5}$$

jj) $l_0 = 0, \quad \beta = \mathrm{GF}(2^m),$

$$Q \geq 2^m \geq h_0, \quad D_{22}^{4m} \triangleq D_{21}^{4m}, \tag{5.6}$$

jjj) $l_0 = 0, \quad \beta = \mathrm{GF}(2^m), \quad Q \geq 2^m \geq h_0, \quad m$ is odd,

$$D_{23}^{4m} \triangleq \begin{bmatrix} 0^m & 0^m \\ A^{2m} & 0^{2m} \\ 0^m & W^m \end{bmatrix}, \tag{5.7}$$

where A^{2m} is a parity-check matrix of a $[\lambda_{2m}, \lambda_{2m} - 2m]2$ code. Then V is a normal $[n, n-r]4, l$ code with $r = s + 4m$ and parameters:

Case A1:

i) and ii)

$$n = 2^m(Q+2) - 2, \quad l = 3, \quad h(H_g^r(K), 2) \leq h_0 + 2,$$

$$h(H_g^r(K), 3) \leq 3h_0 + 2 \quad \text{for } m \geq 3, \quad g = 11, 12, \tag{5.8}$$

iii)
$$n = 2^m(Q+2) - 3, \quad l \geq 2; \tag{5.9}$$

iv)
$$n = 2^m(Q+1) - 1, \quad l = 3,$$

$$h(H_{14}^r(K), 3) \leq h_0 + 1. \tag{5.10}$$

Case A2:

j) and jj) $n = 2^m(Q+3) - 3, \quad l = 3 \quad \text{for } m \geq 3,$

$$h(H_f^r(K), 2) \leq 2Y_f + 5, \quad h(H_f^r(K), 3) \leq 4Y_f + 9,$$

$$f = 21, 22,$$

$$Y_{21} = 2^m + 1, \quad Y_{22} = 2^m; \tag{5.11}$$

jjj)
$$n = 2^m(Q+1) + \lambda_{2m} - 1, \quad l \geq 2. \tag{5.12}$$

Proof: We prove Cases A1 and A2 considering examples of representation for columns $U = (\pi, u_1, u_2, u_3, u_4)^{tr}$, $\pi \in \mathrm{GF}(2^s)$, $u_1, u_2, u_3, u_4 \in \mathrm{GF}(2^m)$.

1) $\pi = \varphi_i + \varphi_j + \varphi_k + \varphi_p$; φ_i, φ_j, φ_k, and φ_p belong to distinct subsets of K; b_i, b_j, b_k, and b_p are distinct.

Cases A1i–A1iv, A2j–A2jjj: Let $b_i, b_j, b_k, b_p \neq *$. We find x, y, z, and t solving the system $xb_i^{\delta-1} + yb_j^{\delta-1} + zb_k^{\delta-1} + tb_p^{\delta-1} = u_\delta$, $\delta = \overline{1,4}$. $U = (\varphi_i, x, xb_i, xb_i^2, xb_i^3)^{tr} + (\varphi_j, y, yb_j, yb_j^2, yb_j^3)^{tr} + (\varphi_k, z, zb_k, zb_k^2, zb_k^3)^{tr} + (\varphi_p, t, tb_p, tb_p^2, tb_p^3)^{tr}$. If $b_p = *$ (Cases A1ii and A2j), the system contains three equations. In the representation of U, the fourth summand is $(\varphi_p, 0, 0, 0, w)^{tr}$.

2) $\pi = \varphi_i + \varphi_j + \varphi_k$; φ_i, φ_j, and φ_k belong to distinct subsets of K; b_i, b_j and b_k are distinct.

Let $b_i, b_j, b_k \neq *$. We find x, y, and z solving the system T of three equations $xb_i^{\delta-1} + yb_j^{\delta-1} + zb_k^{\delta-1} = u_\delta$. Now $U = (\varphi_i, x, xb_i, xb_i^2, xb_i^3)^{tr} + (\varphi_j, y, yb_j, yb_j^2, yb_j^3)^{tr} + (\varphi_k, z, zb_k, zb_k^2, zb_k^3)^{tr} + f$; f is a column of Ψ_ϵ^r. We introduce notations: $S_1 = b_i + b_j$, $S_2 = b_i + b_k$, $S_3 = b_j + b_k$, $\Pi_1 = b_i b_j$, $\Pi_2 = b_i b_k$, $\Pi_3 = b_j b_k$, $\sigma_1 = b_i + b_j + b_k$, $\sigma_2 = \Pi_1 + \Pi_2 + \Pi_3$, $\sigma_3 = b_i b_j b_k$, $\Delta = S_1 S_2 S_3$, $\theta = u_3 \sigma_1 + u_2 \sigma_2 + u_1 \sigma_3$, $\Omega = (u_4 + u_3 \sigma_1 + u_2 \sigma_2)/\sigma_3$.

Cases A1i, A1iv, A2j–A2jjj: We take $\delta = 1, 2, 3$ and $f = (0, 0, 0, 0, w)^{tr}$.

Case A1ii: We solve two systems T with $\delta = 1, 2, 4$ and $\delta = 1, 3, 4$. We denote their determinants by Δ_1 and Δ_2. We can show that $\Delta_1 = \Delta\sigma_1$, $\Delta_2 = \Delta\sigma_2$. Clearly, $\Delta \neq 0$. Suppose, $\Delta_1 = \Delta_2 = 0$. Then $\sigma_1 = \sigma_2 = 0$ and $b_j^2 + b_j b_k + b_k^2 = 0$. Let $t = b_j b_k^{-1}$. Then $t^2 + t + 1 = 0$. The equation cannot be solved over GF(2^m) with odd m [14]. So, either $\Delta_1 \neq 0$ or $\Delta_2 \neq 0$. If $\Delta_1 \neq 0$, then $f = (0, 0, 0, w, 0)^{tr}$. If $\Delta_2 \neq 0$, then $f = (0, 0, w, 0, 0)^{tr}$.

Case A1iii: Solving the system T with $\delta = 1, 2, 3$, we obtain $x = (u_3 + u_2 S_3 + u_1 \Pi_3)/(S_1 S_2)$, $y = (u_3 + u_2 S_2 + u_1 \Pi_2)/(S_1 S_3)$, $z = (u_3 + u_2 S_1 + u_1 \Pi_1)/(S_2 S_3)$. For these values of x, y, z, we have $xb_i^3 + yb_j^3 + zb_k^3 = \theta$. If $\theta + u_4 \neq \alpha$, then (see (5.3)) the matrix Ψ_{13}^r contains the column $f = (0, 0, 0, 0, \theta + u_4)^{tr}$ and the representation of U is obtained.

If $\theta + u_4 = \alpha$ (i.e., $u_4 = \alpha + \theta$), then we solve the system T with $\delta = 2, 3, 4$ and obtain $x = (u_4 + u_3 S_3 + u_2 \Pi_3)/(S_1 S_2 b_i)$, $y = (u_4 + u_3 S_2 + u_2 \Pi_2)/(S_1 S_3 b_j)$, $z = (u_4 + u_3 S_1 + u_2 \Pi_1)/(S_2 S_3 b_k)$, where $b_i, b_j, b_k \neq 0$ (see (5.3)). For obtained values of x, y, and z, we have $x + y + z = \Omega$. We substitute $u_4 = \alpha + \theta$ into Ω and obtain $\Omega = u_1 + \alpha/\sigma_3$. Since $\beta \subseteq \{1, \alpha, \alpha^2, \cdots, \alpha^c\}$, we have $\sigma_3 = \alpha^p$, $3 \leq p \leq 3c - 3 \leq 2^m - 1$. Hence $\sigma_3 \neq \alpha$, $\Omega + u_1 \neq 1$. For the matrix D_{13}^{4m}, we have $\gamma = 1$. Therefore, Ψ_{13}^r contains the column $f = (0, \Omega + u_1, 0, 0, 0)^{tr}$. The representation of U is designed.

Let $b_k = *$ (Cases A1ii, A2j). We solve the system $xb_i^{\delta-1} + yb_j^{\delta-1} = u_\delta$, $\delta = 1, 2$. Now $U = (\varphi_i, x, xb_i, xb_i^2, xb_i^3)^{tr} + (\varphi_j, y, yb_j, yb_j^2, yb_j^3)^{tr} + (\varphi_k, 0, 0, 0, w)^{tr} + (0, 0, 0, g, 0)^{tr}$, $w = xb_i^3 + yb_j^3 + u_4$, $g = xb_i^2 + yb_j^2 + u_3$.

3) $\pi = \varphi_i + \varphi_j$; φ_i and φ_j belong to distinct subsets of K; $b_i \neq b_j$. Here we do not consider Case A1iv. Let $b_i, b_j \neq *$. We solve the system $xb_i^{\delta-1} + yb_j^{\delta-1} = u_\delta$, where $\delta = 1, 2$, for Cases A1i, A2j, A2jj; $\delta = 2, 3$ for Case A1iii; $\delta = 1, 4$ for Cases A1ii, A2jjj (if m is odd, then $b_i^3 \neq b_j^3$). Now $U = (\varphi_i, x, xb_i, xb_i^2, xb_i^3)^{tr} + (\varphi_j, y, yb_j, yb_j^2, yb_j^3)^{tr} + P$, where P is a sum of at most two columns of Ψ_ϵ^r. If $b_j = *$ (Cases A1ii, A2j), then $U = (\varphi_i, u_1, u_1 b_i, u_1 b_i^2, u_1 b_i^3)^{tr} + (\varphi_j, 0, 0, 0, w)^{tr} + (0, 0, g, 0, 0)^{tr} + (0, 0, 0, d, 0)^{tr}$.

4) $\pi = \varphi_i$. (Here we do not consider Cases A1i–A1iv.)

Cases A2j–A2jjj: Let $b_i \neq *$. Then $U = (\varphi_i, u_1, u_1 b_i, u_1 b_i^2, u_1 b_i^3)^{tr} + (0, 0, 0, 0, w)^{tr} + P$, where P is a sum of at most two columns of Ψ_ϵ^r.

Case A2j: Let $b_i = *$. If $u_1 \neq 0$, then we can always find $b_\xi = u_2/u_1$, since $\beta = \mathrm{GF}(2^m) \cup \{*\}$. Now $U = (\varphi_i, 0, 0, 0, w)^{tr} + (\varphi_\xi, 0, 0, 0, 0)^{tr} + (\varphi_\xi, u_1, u_2, u_1 b_\xi^2, u_1 b_\xi^3)^{tr} + (0, 0, 0, d, 0)^{tr}$. If $u_1 = 0$, then $U = (\varphi_i, 0, 0, 0, u_4)^{tr} + (0, 0, u_2, 0, 0)^{tr} + (0, 0, 0, u_3, 0)^{tr}$.

5) $\pi = 0$. (Here we do not consider Cases A1i–A1iv.).

Cases A2j–A2jjj: $u_1 = 0$. U is a sum of at most three columns of Ψ_ϵ^r.

Cases A2j, A2jj: $u_1 \neq 0$. We can always find $b_\xi = u_2/u_1$. Now $U = (\varphi_\xi, 0, 0, 0, 0)^{tr} + (\varphi_\xi, u_1, u_2, u_1 b_\xi^2, u_1 b_\xi^3)^{tr} + (0, 0, 0, d, 0)^{tr} + (0, 0, 0, 0, w)^{tr}$.

Case A2jjj: $u_1 \neq 0$. Since for odd m any element of GF(2^m) is a cube, we can always find b_ξ such that $b_\xi^3 = u_4/u_1$. Then $U = (\varphi_\xi, 0, 0, 0, 0)^{tr} + (\varphi_\xi, u_1, u_1 b_\xi, u_1 b_\xi^2, u_4)^{tr} + P$, where P is a sum of at most two columns of Ψ_{23}^r corresponding to submatrix A^{2m}.

Estimates of $h(H_g^r(K), 2)$ in (5.8) and $h(H_{14}^r(K), 3)$ in (5.10) are obtained in the same way as the estimate of $h(H_{11}^r(K), 1)$ in Theorem 4.1.

Since $h(\Phi^s, l_0) \geq R = 4$, we have $m \geq 2$ for all Cases A1 and A2. Moreover, for Cases A1ii and A2jjj, where m is odd, we have $m \geq 3$.

For $m \geq 3$, we consider partitions P_3 and P_4 of a union $L(f)$. For P_3, the first (resp., second) subset consists of columns $(\varphi_j, e_i, e_i f, e_i f^2, e_i f^3)^{tr}$ with $e_i = 0, 1$ (resp., $e_i = \alpha, \alpha^2$), and the third subset is the rest of the columns. Here $0, 1, \alpha \in GF(2^m)$, and α is a primitive element. The first and the second subsets of P_4 are the same as the first and the second subsets of P_3, the third subset contains columns with $e_i = \alpha + 1$, and the fourth subset is the rest of the columns. It can be verified directly that both partitions P_3 and P_4 allow us to represent any column of $L(f)$ by a sum of three columns of *distinct* subsets. Also, P_4 permits us to represent any column of the form $(0, e_i, e_i f, \cdots)^{tr}$ by a sum of four columns of *distinct* subsets. Now we introduce the partition P_W of the column set of the matrix W^m: the first (resp., second) subset consists of only the column $(0 \cdots 01)^{tr}$ (resp., $(0 \cdots 010)^{tr}$, and the third subset is the rest of the columns. Any column of W^m is a sum of two columns of distinct subsets. Besides, in W^m, we have three linearly dependent columns of distinct subsets.

We consider Case A1i (see (5.8)). Since $l_0 = 2 > 0$, columns of Ψ_{11}^r occur in representations of U together with columns of submatrices L_i^r. For $m \geq 2$, any column of L_i^r is a sum of three columns of this submatrix. Hence $l = 3$. Let $|\beta| = h_0$, $m \geq 3$. To estimate $h(H_{11}^r(K), 3)$, we use P_3 for every union $L(f)$ and obtain $3h_0$ subsets. In addition, every submatrix W^m in Ψ_{11}^r defines one subset. Properties of P_3 show that the described partition of $H_{11}^r(K)$ is (4, 3)-sufficient. The Case A1ii is similar.

For Case A2j (see (5.11)), columns of Ψ_{21}^r can occur in representations of U without columns of L_i^r. To estimate $h(H_{21}^r(K), 3)$, we use P_4 for unions $L(f)$ and P_W for every submatrix W^m in Ψ_{21}^r. We obtain $4(2^m + 1) + 9$ subsets. Properties of P_4, P_W show that $l = 3$, and this partition of $H_{21}^r(K)$ is (4, 3)-sufficient. If, e.g., $U = (0, u_1, u_1 b_\xi, u_1 b_\xi^2, u_1 b_\xi^3)^{tr}$, $u_1 \neq 0$, then we represent U by a sum of four columns of distinct subsets. Now we consider Case A2j for $l = 2$. We partition every union $L(f)$ into two subsets as in Theorem 3.1. We use P_W for one of the submatrices W^m in Ψ_{21}^r. Other submatrices W^m define two subsets. We obtained a (4, 2)-sufficient partition of $2(2^m + 1) + 5$ subsets. Case A2jj is similar.

Since D_ϵ^{4m} contains submatrix W^m, and we always have $m \geq 2$, the code V has minimal distance $d = 3$ and is normal by Theorem 32 of [6]. □

Cases A1i and A1iv correspond to condition 4 of Theorems 2 and 4 in [7].

Example 5.1: V_0 is the [9, 1]4, 0 repetition code. Case A2j, $m = 3$, gives a [93, 73]4, 3 code with $h(H_{21}^{20}, 2) \leq 23$, $h(H_{21}^{20}, 3) \leq 45$. Now we take this code as V_0 for Case A1i, $m = 5$, and Case A1iv, $m \geq 6$. This generates a [3038, 2998]4, 3 code and a family of $[n, n - r]4, l$ codes with

$$R = 4, \quad l = 3, \quad r = 4t, \quad t = 5, \quad t \geq 11,$$
$$n = 47 \times 2^{t-4} - 1, \quad \bar{\mu}(4) \approx 3.1024. \tag{5.13}$$

Example 5.2: Here we use Example 2.2. ADS of the [23, 12]3, 0 Golay code and Hamming codes gives a [25, 12]4, 0 code, a [29, 15]4, 2 code with $h(\Phi^{14}, 2) \leq 26$, and a [37, 22]4, 2 code with $h(\Phi^{15}, 2) \leq 26$. (The estimates of $h(\Phi^s, 2)$ are tested using a computer.) From the [9, 1]4, 0 repetition code and the [25, 12]4,0 code, we obtain a [10, 2]4, 2 code and a [26, 13]4, 2 code.

Example 5.3: V_0 is the [10, 2]4, 2 code of Example 5.2. With the help of Case A1i, $m = 4$, and Case A1iii, $m = 5, 6, 7$, we design [190, 166]4, 3, [381, 353]4, 3, [765, 733]4, 3, and [1533, 1497]4,3 codes. Now V_0 is the [9, 2]4, 2 code of Example 2.2. By Case A1i, $m = 4$, and Case A1iii, $m = 5, 6$, we design [174, 151]4, 3, [349, 322]4, 3, and [701, 670]4, 3 codes.

Example 5.4: V_0 is the [8, 1]4, 0 repetition code. Using Case A2jjj for $m = 3$ and the matrix in (2.15) as A^{2m}, we obtain an [84, 65]4, 3 code. Now V_0 is the [37, 22]4, 2 code of Example 5.2. Case A1i, $m = 5, 6$, and Case A1iii, $m = \overline{7, 11}$, give an [1246, 1211]4, 3 code Ω with $h(H_{11}^{35}, 3) \leq 80$, a [2494, 2455]4, 3 code, and $[n, n - r]4, 3$ codes with

$$R = 4, \quad l = 3, \quad r = 4t - 1, \quad t = \overline{11, 15},$$
$$n = 39 \times 2^{t-4} - 3. \tag{5.14}$$

Now V_0 is the code Ω. Case A1iv, $m \geq 7$, gives $[n, n - r]4, l$ codes with

$$R = 4, \quad l = 3, \quad r = 4t - 1, \quad t = 9, \quad t \geq 16,$$
$$n = 1247 \times 2^{t-9} - 1, \quad \bar{\mu}(4) \approx 2.9323. \tag{5.15}$$

Example 5.5: We consider codes with $r = 4t - 2$. ADS of the [14, 6]3 code [10] and the [3, 1]1 Hamming code gives a [16, 6]4, 0 code V_0. Using Case A2jj, $m = 4$, we obtain a [301, 275]4, 3 code. Let I^k be the identity $k \times k$ matrix. ADS of the [5, 1]2 code (see (2.1)) and the [7, 4]1 Hamming codes gives a [17, 7]4, 2 code V_0 with the parity-check matrix

$$\Phi^{10} \triangleq \left[\begin{array}{ccc|c} I^4 & 0^4 & 0^4 & \nu \\ 0^3 & W_\rho^3 & 0^3 & \rho \\ 0^3 & 0^3 & W_\rho^3 & \rho \end{array}\right] = [\varphi_1 \cdots \varphi_{17}], \quad \nu = (1111)^{tr},$$
$$\rho = (111)^{tr}. \tag{5.16}$$

It can be shown that the partition into nine subsets $\{\varphi_1\}, \cdots, \{\varphi_6\}, \{\varphi_7, \cdots, \varphi_{10}\}, \{\varphi_{11}, \cdots, \varphi_{16}\}, \{\varphi_{17}\}$ is (4, 2)-sufficient. Case A1ii, $m = 3$, and Case A1iii, $m = 5$, give an [150, 128]4, 3 code and a [605, 575]4, 3 code.

Now V_0 is the [29, 15]4, 2 code of Example 5.2. Using Case A1i, $m = 5, 6$, and Case A1iii, $m = \overline{7, 11}$, we design a [990, 956]4, 3 code with $h(H_{11}^{34}, 3) \leq 80$, an [1982, 1944]4, 3 code, and $[n, n - r]4, 3$ codes with

$$R = 4, \quad l = 3, \quad r = 4t - 2, \quad t = \overline{11, 15},$$
$$n = 31 \times 2^{t-4} - 3. \tag{5.17}$$

Finally, let V_0 be the [990, 956]4, 3 code. Using Case A1iv, $m \geq 7$, we obtain an infinite family of $[n, n - r]4, 3$ codes with parameters $R = 4$, $r = 4t - 2$, $t = 9$, $t \geq 16$, $n = 991 \times 2^{t-9} - 1$, $\bar{\mu}(4) \approx 2.3392$ (see (1.5)).

Example 5.6: Further $r = 4t - 3$. The 9×13 parity-check matrix

$$\Phi^{9} \triangleq \left[\begin{array}{cc|c} I^6 & 0^6 & \xi \\ 0^3 & W_\rho^3 & \rho \end{array}\right] = [\varphi_1 \cdots \varphi_{13}], \quad \xi = (111111)^{tr},$$
$$\rho = (111)^{tr}, \tag{5.18}$$

defines a [13, 4]4, 2 code V_0. The partition $\{\varphi_1\}, \cdots, \{\varphi_7\}, \{\varphi_8, \cdots, \varphi_{12}\}, \{\varphi_{13}\}$ into nine subsets is (4, 0)-sufficient. The partition $\{\varphi_1\}, \cdots, \{\varphi_8\}, \{\varphi_9, \cdots, \varphi_{12}\}, \{\varphi_{13}\}$ into 10 subsets is (4, 2)-sufficient. Case A2j, $m = 3$, Case A1i, $m = 4$, and Case A1iii, $m = 5$, design a [125, 104]4, 3 code, a [238, 213]4, 3 code, and a [477, 448]4, 3 code, respectively.

Now take the [26, 13]4, 2 code of Example 5.2 as V_0. Case A1i, $m = 5, 6$, and Case A1iii, $m = \overline{7, 11}$, give an [894, 861]4, 3 code with $h(H_{11}^{33}, 3) \leq 80$, an [1790, 1753]4, 3 code, and $[n, n - r]4, 3$

codes with

$$R = 4, \quad l = 3, \quad r = 4t - 3, \quad t = \overline{11, 15},$$
$$n = 14 \times 2^{t-3} - 3. \qquad (5.19)$$

Finally, let V_0 be the [894, 861]4, 3 code. Using Case A1iv for $m \geq 7$, we obtain an infinite family of $[n, n-r]4, 3$ codes with parameters

$$R = 4, \quad l = 3, \quad r = 4t - 3, \quad t \geq 16,$$
$$n = 895 \times 2^{t-9} - 1, \quad \overline{\mu}(4) \approx 3.1124. \qquad (5.20)$$

Remark 5.1: One of the referees noted the following useful facts. We can treat binary columns as points of a projective geometry and multiples of these points (see [3], [9], [13]). For example, matrix $B^{mR}(b)$ contains all multiples of the point $(1, b, b^2, \cdots, b^{R-1})$ or $(0, \cdots, 0, 1)$ in the geometry PG$(R-1, 2^m)$. In Theorem 3.1, matrix D_1^{2m} corresponds to two points of the line PG$(1, 2^m)$, matrix D_2^{2m} corresponds to one point of the line, the claim $\beta = \mathrm{GF}(2^m)$ means that we require availability of the rest of the points, and finally, in the proof we generate the line with the help of two points. In Theorem 4.1, three noncolinear points span a plane. Case A1iii uses the oval in PG$(2, 2^m)$ of $2^m + 2$ points [14], etc. A similar approach can be used for Theorem 5.1.

VI. Table of Upper Bounds on the Length Function $l(r,R)$

In Table I we give constructive upper bounds on $l(r, R)$ for $r \leq 64$, $R = 2, 3, 4$. Our bounds are new for the following values of R and r: $R = 2$, $r = 2t \geq 12$; $R = 3$, $r = 15, \cdots, 19, 22$, $r \geq 24$; $R = 4$, $r \geq 19$.

The following entries of Table I are taken from [1], [7]–[10]. In [1], the bounds $l(8,2) \leq 26$, $l(9,3) \leq 18$, and $l(12,3) \leq 38$ are quoted as private communications by Ashlock and Kibler. In [8], the bounds $l(14,3) \leq 63$ and $l(16,4) \leq 49$ are given. In [9], codes yielding $l(8,2) \leq 26$, $l(13,3) \leq 53$, and $l(18,4) \leq 77$ are obtained. In [7], codes yielding $l(10,2) \leq 53$, $l(14,3) \leq 63$, $l(20,3) \leq 255$, $l(21,3) \leq 308$, $l(23,3) \leq 511$, and $l(17,4) \leq 62$ are given. Entries for $R = 2$ with $r \leq 7$, $R = 3$ with $r \leq 8$, $r = 10, 11$, and $R = 4$ with $r \leq 15$ are taken from [10]. In [9], codes with $R = 2$, $r = 2t - 1 \geq 7$, $n = 5 \times 2^{t-2} - 1$ are obtained.

In this work we rederived the mentioned codes with $R = 2$, $r = 8, 10$ and $R = 3$, $r = 14, 20, 21, 23$. Besides, the techniques of Section III permit us to obtain codes with $R = 2$, $r = 2t - 1$, $n = 5 \times 2^{t-2} - 1$ (see Remark 3.1).

New bounds are constructive. They follow from the existence of corresponding codes constructed in Sections III–V, in Examples 3.1, 4.1–4.7, and 5.1–5.6. Parameters of codes are given directly in the examples or are calculated with the help of relations (1.3)–(1.5), (4.9), (4.10), (4.12), (4.13), (4.16), (5.13)–(5.15), (5.17), (5.19), and (5.20).

Using the [15, 11]1 and the [31, 26]1 Hamming codes, the [23, 12]3 Golay code, and [26, 18]2, [53, 43]2, [63, 49]3, [95, 79]3, [84, 65]4, [93, 73]4, and [174, 151]4 codes (see Table I) in ADS construction, we obtain new upper bounds on $l(r, R)$ for $r = \overline{21, 28}$, $R = 5$:

$$l(21,5) \leq 75, \quad l(22,5) \leq 88,$$
$$l(23,5) \leq 98, \quad l(24,5) \leq 107,$$
$$l(25,5) \leq 123, \quad l(26,5) \leq 147,$$
$$l(27,5) \leq 173, \quad l(28,5) \leq 204. \qquad (6.1)$$

VII. Conclusion

Using the constructions of [7] and new constructions obtained in this work, we designed a number of infinite families of binary linear covering codes with covering radii $R = 2, 3, 4$. The designed codes give new upper bounds on the length function $l(r, R)$. Ideas and approaches used in this work can be applied for construction of codes with $R \geq 5$.

Acknowledgment

The authors thank V. A. Zinoviev and an anonymous referee for very helpful and detailed comments and suggestions. The authors also thank H. Janwa, J. H. van Lint, and V. S. Pless for sending to them copies of their papers.

References

[1] R. A. Brualdi and V. S. Pless, "On the length of codes with a given covering radius," in *Coding Theory and Design Theory. Part I. Coding Theory.* New York: Springer-Verlag, 1990, pp. 9–15.

[2] ___, "On the covering radius of a code and its subcodes," *Discrete Math.*, vol. 83, no. 2–3, pp. 189–199, 1990.

[3] R. A. Brualdi, V. S. Pless, and R. M. Wilson, "Short codes with a given covering radius," *IEEE Trans. Inform. Theory*, vol. 35, pp. 99–109, Jan. 1989.

[4] A. R. Calderbank and N. J. A. Sloane, "Inequalities for covering codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1276–1280, Sept. 1988.

[5] G. D. Cohen, M. G. Karpovsky, H. F. Mattson, Jr., and J. R. Shatz, "Covering radius—Survey and recent results," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 328–343, May 1985.

[6] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, "Further results on the covering radius of codes," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 680–694, Sept. 1986.

[7] A. A. Davydov, "Construction of linear covering codes," *Probl. Peredach. Inform.*, vol. 26, no. 4, pp. 38–55, Oct.–Dec. 1990 (in Russian). Eng. transl., *Probl. Inf. Transm. (USSR)*, vol. 26, no. 4, pp. 317–331, Oct.–Dec. 1990.

[8] R. Dougherty and H. Janwa, "Covering radius computations for binary cyclic codes," *Math. Comput.*, vol. 57, pp. 415–434, July 1991.

[9] E. M. Gabidulin, A. A. Davydov, and L. M. Tombak, "Codes with covering radius 2 and other new covering codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 219–224, Jan. 1991.

[10] R. L. Graham and N. J. A. Sloane, "On the covering radius of codes," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 385–401, May 1985.

[11] I. S. Honkala, "Modified bounds for binary covering codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 351–365, Mar. 1991.

[12] G. A. Kabatyanskii and V. I. Panchenko, "Unit sphere packings and coverings of the Hamming space," *Probl. Peredach. Inform.*, vol. 24, no. 4, pp. 3–16, 1988 (in Russian). Engl. trans., *Probl. Inf. Transm. (USSR)*, vol. 24, no. 4, pp. 261–272, Oct.–Dec. 1988.

[13] J. H. van Lint, "Recent results on covering problems," in *Proc. 6th Int. Conf. on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-6*, (Rome, Italy), July 1988. (Also *Lecture Notes in Computer Science, no. 357.* New York: Springer-Verlag, 1989, pp. 7–21).

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam, The Netherlands: North-Holland, 1977.

[15] A. A. Tietäväinen, "An upper bound on the covering radius as a function of the dual distance," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1472–1474, Nov. 1990.

[16] S. G. Vlăduţ and A. N. Skorobogatov, "Covering radius for long BCH codes," *Probl. Peredach. Inform.*, vol. 25, no. 1, pp. 38–45, 1989 (in Russian). Engl. trans., *Probl. Inf. Transm. (USSR)*, vol. 25, no. 1, pp. 28–34, Jan.–Mar. 1989.

[17] G. J. M. van Wee, "Improved sphere bounds on the covering radius of codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 237–245, Mar. 1988.