Constructions of Binary Linear Block Codes with Largest Minimum Distance and Smallest Error Coefficient

Murad Abdullah[1,2], *Student Member, IEEE* and Wai Ho Mow[1], *Senior Member, IEEE*
[1]Department of Electronic and Computer Engineering
[2]Internet of Things Thrust Area, Information Hub, HKUST (GZ)
The Hong Kong University of Science and Technology
Email: mabdullah@connect.ust.hk, eewhmow@ust.hk

***Abstract*—In this paper, we present some new constructions of the binary linear block codes (BLBCs) that achieve the largest possible minimum Hamming distance and the lowest possible number of codewords of this Hamming weight (also known as error coefficient), and they are said to be $[d, A_d]$-optimal (n, k) linear codes. These (n, k) BLBCs give the best possible frame error rate (FER) in the asymptotic regime under maximum-likelihood decoding over the additive white Gaussian noise channel. Specifically, for all positive integers k and m, and $0 \leq l \leq k-1$, we give the constructions of $((2^k-1)m+l, k)$, $((2^k-1)+k, k+1)$, $(15m+4, 4)$, $(15m+6, 4)$, $(12, 5)$, and $(33, 5)$ BLBCs. Many of these BLBCs have $A_d = 1$, and some achieve the lower bound on A_d, which asserts their optimality. Our constructions show the asymptotic E_b/N_o gain of up to 1.24 dB over their d-optimal counterpart at a FER of 10^{-7}.**

***Index Terms*—Binary linear block codes, optimal error coefficients, Griesmer bound.**

I. Introduction

In coding theory, finding the code with the optimal FER performance under maximum-likelihood (ML) decoding is a very challenging task. The following parameters are very important when describing a linear block code: block length n, message length k, minimum Hamming distance d, and the error coefficient A_d. The asymptotic FER performance of a BLBC over the additive white Gaussian noise (AWGN) channel under ML decoding depends on d and A_d. The database in [1] maintains the best-record for the bounding values on the minimum distance and constructions of BLBCs for all block lengths of up to 256.

Internet of Things (IoT) devices generally need to communicate at a low-rate due to the power constraints in the applications (e.g., a low-cost sensor installed in a remote area) offered under massive machine-type communications (mMTC) [2]. It is necessary to design codes with optimal FER performance to save energy for these sensors. Consequently, it is necessary to both maximize the minimum distance and minimize the corresponding error coefficient while constructing a BLBC.

There are many BLBCs for which the optimal values of the minimum distance are not known. However, the BLBCs for which the optimal values of d are known, the constructions are not optimal for the minimal values of A_d. If an (n, k) BLBC has the largest possible value of the minimum distance, we call this a d-optimal (n, k) linear code. A BLBC with optimal values of d and A_d gives the best possible asymptotic FER performance under ML decoding, e.g., guessing random additive noise decoding (GRAND) [3], which can efficiently decode high rate codes. Any BLBC can be transformed to the polar coding framework with dynamic frozen bits, and computationally efficient decoding can be performed using successive cancellation list (SCL) decoding [4]. However, it is necessary to mention here that the required list size for the SCL could be very large to achieve the ML performance.

Moreover, the performance of the BLBC for which the optimal value of d is known can only be further improved by finding the construction which gives a lower value of A_d. If a d-optimal (n, k) linear code has a minimum possible value of A_d, we call this a $[d, A_d]$-optimal (n, k) linear code. Solé *et al.* [5] used linear programming (LP) to derive lower and upper bounds on the values of A_d for any linear code over a finite field $GF(q)$. These bounds are very useful to benchmark the constructions of the linear codes. If a d-optimal linear code achieves the lower bound on A_d, this code is $[d, A_d]$-optimal (n, k) linear code. A comprehensive survey on the error coefficient of linear codes can be found in [6], where authors also pointed out the significance of designing the linear codes with optimal error coefficients. However, it is essential to mention here that our motivation to study these $[d, A_d]$-optimal (n, k) linear codes is independent of the work of [5], [6]. We designed an algorithm to search for the largest minimum distance BLBCs with a smaller error coefficient[1].

The work was supported by the Hong Kong Research Grants Council under project no. GRF 16233816.

This work was submitted to the 2022 IEEE International Symposium on Information Theory on Feburary 6, 2022, but unfortunately, it has not been accepted.

[1]The poster was presented in the recent results session at *IEEE International Symposium on Information Theory (ISIT), Melbourne, Australia, July 2021*. The poster is available at github.com/Murad1997/ISIT_2021_Poster/blob/main/Poster_ISIT_2021.pdf

Here we only give the general structures of the generator matrices of most of the codes that appeared in our search.

As mentioned previously, the constructions of the BLBCs given in [1] are optimal for the maximum values of d, not for the minimal values of A_d. Our objective is to give general constructions of $[d, Ad]$-optimal linear codes.

The rest of this paper is organized as follows. Section II gives the optimality criteria for the code construction followed by a review of simplex codes, and we conclude this section by presenting the LP bounds on the error coefficient. Section III is devoted to constructing the $[d, A_d]$-optimal codes. Section IV compares new constructions with the previous best-known constructions. Section V concludes the paper.

II. Preliminaries

We denote by $GF(2)$ the binary field. An (n, k) BLBC over $GF(2)$ is a k-dimensional $GF(2)$ vector subspace of $GF(2)^n$. The Hamming weight of a vector $y = (y_1, \ldots, y_n)$ is the number of nonzero elements. We denote this as $wt(y)$. The Hamming distance between two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, we define as the number of positions where they differ, i.e., $d_H(x, y) = wt(x - y)$. Given an (n, k) linear code, say C, the minimum Hamming distance of C is $d = min\{d_H(x, y) \mid x, y \in C\}$. If A_i denotes the number of codewords of weight i in an (n, k) code. Then the polynomial

$$W(y) = \sum_{i=0}^{n} A_i y^i, \tag{1}$$

is called the *weight enumerating function* (WEF) of the (n, k) code. If the code is a binary linear code, then $\sum_{i=0}^{n} A_i = 2^k$.

A. Optimality Criteria

The truncated union bound on the FER performance of a BLBC under ML decoding [7] is

$$P_e \approx A_d Q(\sqrt{2d(k/n)E_b/N_o}), \tag{2}$$

where $Q(x) \triangleq \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt$, d is the minimum distance, and A_d is the number of codewords of weight d. This suggests maximizing d and minimizing A_d for the given (n, k) BLBC to improve its asymptotic FER performance. It can be easily seen that of two codes having exactly the same values of d, the code with a smaller value of A_d performs better. The bounds on the minimum distance of linear codes can be found in [1]. The constructions given there are optimized for maximizing d, not for minimizing A_d. Minimizing A_d is crucial for improving the performance of the d-optimal code. Here, we give the construction of the codes with the best possible value of A_d. However, it is important to mention that Equation 2 is neither an upper nor a lower bound on the FER; it is tight only in the high E_b/N_o regime, as shown in Fig. 1. Given two (n, k) BLBCs of the same minimum distance d, let $A_d^{(1)}$ and $A_d^{(2)}$ denote the error coefficients of these two codes. Then the estimated E_b/N_o gain at the target FER = P_e is

$$(Q^{-1}(P_e/A_d^{(1)}) - Q^{-1}(P_e/A_d^{(2)}))/(2dk/n) \tag{3}$$

where Q^{-1} is the inverse of Q-function.

B. Simplex Codes

A $(2^k - 1, k)$ simplex code of dimension k with $d = 2^{k-1}$ has a generator matrix S_k, where the columns of S_k consist of all $2^k - 1$ non-zero binary vectors of dimension k [8]. Without loss of generality, we will assume that the i-th column of S_k corresponds to the binary representation of the integer i. The WEF of a simplex code is $W(y) = 1 + (2^k - 1)y^{2^{k-1}}$. In an *equidistant* code, the distance between any two distinct codewords is equal to a constant. All codewords in simplex code are at a constant distance from each other, so this is an equidistant code. The simplex codes are the dual of the Hamming codes. For example the $(7, 3)$ simplex code has the following generator matrix

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

The WEF of this codes is $W(y) = 1 + 7y^4$.

C. Bounds on A_d

The authors in [5] used LP to derive lower and upper bounds on A_d for any (n, k) code over the finite field $GF(q)$ of the minimum distance d. We present the bounds here for the sake of completeness. For the detailed derivation, please refer to reference [5]. Moreover, we used the GAP [9] to compute the bounding values.

Theorem 1 (Lower Bound on A_d [5, Th. 1]): *For any (n, k) code over $GF(q)$ with minimum distance d, we have*

$$A_d \geq q^k - 1 - \lfloor L \rfloor \tag{4}$$

where L is the maximum of the function $\sum_{j=d+1}^{n} A_j$ subject to the $2n - d$ constraints

$$-P_i(0) - (q^k - 1)P_i(d) \leq \sum_{j=d+1}^{n} A_j(P_i(j) - P_i(d)) \tag{5}$$

where

$$P_t(x) = \sum_{j'=0}^{t} (-1)^{j'} (q-1)^{t-j'} \binom{x}{j'} \binom{n-x}{t-j'}, \; 0 \leq t \leq n$$

for $i = 1, 2, \ldots, n$, $A_j \geq 0$ for $j = d + 1, d + 2, \ldots, n$.

Theorem 2 (Upper Bound on A_d [5, Th. 2]): *For any (n, k) code over $GF(q)$ with minimum distance d, we have*

$$A_d \leq q^k - 1 - \lceil S \rceil \tag{6}$$

where S denotes the minimum of the function $\sum_{j=d+1}^{n} A_j$ subject to the constraints as in Theorem 1.

III. Construction of $[d, A_d]$-optimal linear codes

This section gives our new constructions of the $[d, A_d]$-optimal BLBCs.

Theorem 3: *For all positive integers k and m, the $((2^k - 1)m + k - 1, k)$ binary linear block code given by the generator matrix*

$$\Gamma = \left[\begin{array}{c:c} S_k^{\times m} & \begin{matrix} I_{k-1} \\ \mathbf{0}_{k-1} \end{matrix} \end{array} \right]$$

is $[d, A_d]$-optimal with $d = 2^{k-1}m$ and weight enumerating function $W(y) = 1 + y^{2^{k-1}m} + \sum_{i=1}^{k-1} 2\binom{k-1}{i} y^{2^{k-1}m+i}$. $S_k^{\times m}$ denotes m repetitions of S_k, I_{k-1} is the identity matrix of dimension $k-1$, and $\mathbf{0}_{k-1}$ is a row vector of length $k-1$.

Proof. The submatrix of Γ corresponding to the repetitions of simplex code forms an equidistant code with $d = 2^{k-1}m$. All codewords are at a distance of $2^{k-1}m$ from each other. To prove that there are $2\binom{k-1}{i}$ codewords of weight $2^{k-1}m + i$, for $1 \leq i \leq k-1$. We use the fact that the first $(2^k - 1)m$ coordinates of all codewords are at a distance of $2^{k-1}m$ from each other, so the weight is $2^{k-1}m$. The last $k-1$ coordinates, which are linear combinations of the rows of I_{k-1}, have $\binom{k-1}{i}$ of the weight i, for $1 \leq i \leq k-1$. The all-zero row vector in the last $k-1$ coordinate of the last row, when added to the linear combinations of I_{k-1}, results in $2\binom{k-1}{i}$ codewords of weight i, for $1 \leq i \leq k-1$. Hence, $W(y) = 1 + y^{2^{k-1}m} + \sum_{i=1}^{k-1} 2\binom{k-1}{i} y^{2^{k-1}m+i}$, with $d = 2^{k-1}m$, and $A_d = 1$.

It remains to prove that the code is $[d, A_d]$-optimal. Since $A_d = 1$ is the smallest possible, it suffices to show that $d = 2^{k-1}m$ is the largest possible for all $((2^k - 1)m + k - 1, k)$ BLBCs. Let us prove this by contradiction. Assume that there exists a $((2^k - 1)m + k - 1, k)$ code with $d = 2^{k-1}m + p$ for some positive integer p. The Griesmer bound [10] implies that

$$\begin{aligned}(2^k - 1)m + k - 1 &\geq \sum_{i=0}^{k-1} \left\lceil \frac{2^{k-1}m + p}{2^i} \right\rceil \\ &\geq \sum_{i=0}^{k-1} \left\lceil \frac{2^{k-1}m}{2^i} \right\rceil + \sum_{i=0}^{k-1} \left\lceil \frac{p}{2^i} \right\rceil \\ &\geq (2^k - 1)m + \sum_{i=0}^{k-1} \left\lceil \frac{p}{2^i} \right\rceil\end{aligned}$$

or equivalently, $p \leq 0$. This contradicts the fact that p is a positive integer. □

It is noteworthy that the code construction given in Theorem 1 is related to anticodes discussed in [8, Chapter 17]. We can construct good BLBCs of the higher minimum distance by deleting specific columns from m repetitions of the simplex code. The deleted columns form the generator matrix of an *anticode*.

Example 1: We put $k = m = 1$ in Theorem 3, we have a $(9, 3)$ code with $d = 4$ and the generator matrix is

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

The last row of this generator matrix has a weight of four corresponding to the minimum distance of the code. By listing all the codewords, we have WEF $W(y) = 1 + y^4 + 4y^5 + 2y^6$ as proved in Theorem 3.

Theorem 4: *For all positive integers k, the $((2^k - 1) + k, k + 1)$ binary linear block code given by the generator matrix*

$$\left[\begin{array}{cc:c} S_k & I_{k-1} & \mathbf{0}_k^T \\ & \mathbf{0}_{k-1} & \\ \hdashline \mathbf{1}_{2^{k-1}-1} & \mathbf{0}_{2^{k-1}+k-1} & 1 \end{array}\right]$$

has $d = 2^{k-1}$ and $A_d = 2$. $\mathbf{0}_i$ and $\mathbf{1}_i$ denote all-zero and all-one row vectors of length i, respectively, and $(.)^T$ denotes the transpose of a vector.

Proof. We obtain the above generator matrix by modifying the code given in Theorem 3 with $m = 1$. The weight of the last row is 2^{k-1}, of which $2^{k-1} - 1$ ones are at the first $2^{k-1} - 1$ coordinate. All the codewords for which the last row is selected and other rows are selected from the first k rows can have a weight of at least $2^{k-1} - 1$ but adding one in the last column will increase the weight. Hence, $d = 2^{k-1}$.

To prove that $A_d = 2$, we can see that the second last and the last rows of the generator matrix have a weight of 2^{k-1}, and all other codewords have a weight $> 2^{k-1}$.

To prove the d-optimality, we make use of the Griesmer bound. Let us prove this by contradiction as above. Before applying the bound, we replace $k' = k + 1$ and assume that there exists a $((2^{k'-1} - 1) + k' - 1, k')$ code with $d = 2^{k'-2} + p$ for some positive integer p. The Griesmer bound [10] implies that

$$\begin{aligned}(2^{k'-1} - 1) + k' - 1 &\geq \sum_{i=0}^{k'-1} \left\lceil \frac{2^{k'-2} + p}{2^i} \right\rceil \\ &\geq \sum_{i=0}^{k'-1} \left\lceil \frac{2^{k'-2}}{2^i} \right\rceil + \sum_{i=0}^{k'-1} \left\lceil \frac{p}{2^i} \right\rceil \\ &\geq 2^{k'-1} + \sum_{i=0}^{k'-1} \left\lceil \frac{p}{2^i} \right\rceil\end{aligned}$$

or equivalently, $p \leq 0$. This contradicts the fact that p is a positive integer. □

Example 2: We put $k = 3$ in Theorem 4, we have a $(10, 4)$ code with $d = 4$ and the generator matrix is

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

From the above generator matrix, we can see that the last two rows have weights corresponding to the minimum distance of the code. If we list all the codewords and we have the WEF $W(y) = 1 + 2y^4 + 8y^5 + 4y^6 + y^8$.

Corollary 5: *For all positive integers k and m, the $((2^k - 1)m + l, k)$ binary linear block code, for $0 \leq l \leq k - 1$ given by the generator matrix*

$$\Gamma = \left[\begin{array}{c:c} S_k^{\times m} & I_{:,l} \\ & \mathbf{0}_l \end{array}\right]$$

has $d = 2^{k-1}m$ *and* $A_d = \sum_{j=1}^{k-l}\binom{k-l}{j}$. $S_k^{\times m}$ *denotes* m *repetitions of* S_k, $I_{:,l}$ [2] *denotes the first* l *columns of the identity matrix of dimension* $k-1$, *and* $\mathbf{0}_l$ *is an all-zero row vector of length* l.

Proof. If $l = 0$ we have m repetitions of the simplex codes and $d = 2^{k-1}m$ and $A_d = \sum_{j=1}^{k}\binom{k}{j} = 2^k - 1$.

If $l = k-1$, it is the code proved in Theorem 1.

For $1 \le l < k-1$, the last l columns increase the weight of the codewords by at least l, and there are exactly $A_d = \sum_{j=1}^{k-l}\binom{k-l}{j}$. □

Corollary 6: *For all postive integers* m, *the* $(15m+4, 4)$ *binary linear block code given by the generator matrix*

$$\Gamma = \begin{bmatrix} S_4^{\times m} & I_4 \end{bmatrix}$$

has $d = 8m+1$ *and the weight enumerating function* $W(y) = 1 + \sum_{i=1}^{4}\binom{4}{i}y^{8m+i}$. *Namely,* $A_d = 4$. $S_4^{\times m}$ *denotes* m *repetitions of* S_4 *and* I_4 *is an identity matrix of dimension* 4.

Proof. The submatrix of Γ corresponding to $S_4^{\times m}$ has weight $8m$. I_4 matrix has $\binom{4}{i}$ weight i codewords, for $1 \le i \le 4$, which increase the weight of the codewords to $8m+i$. The d-optimality can be seen the Griesmer bound as done above. □

Corollary 7: *For all postive integers* m, *the* $(15m+6, 4)$ *binary linear block code given by the generator matrix*

$$\Gamma = \left[\begin{array}{c|cc} S_4^{\times m} & I_3 & I_3' \\ & \mathbf{0}_3 & \mathbf{1}_3 \end{array}\right]$$

has $d = 8m+2$ *and the weight enumerating function* $W(y) = 1 + 3y^{8m+2} + 8y^{8m+3} + 3y^{8m+4} + y^{8m+6}$. I_3 *denotes an identity matrix of dimension* 3 *and* I_3' *denotes the element-wise complement of* I_3.

Proof. The submatrix of Γ corresponding to $S_4^{\times m}$ has all codewords of weight-$8m$. We need only to show that there are 3 weight-2 codewords, 8 weight-3 codewords, 3 weight-4 codewords and 1 weight-6 codeword at the last 6 columns.

We can only obtain weight-6 in the last 6 coordinates if the codeword is the combination of all the rows of Γ.

The weight-3 codewords can be obtained by taking the combinations of the rows of Γ one and three at a time resulting in 8 weight-3 codewords.

The weight-4 codewords can be obtained by taking the two rows from the first three rows. While the weight-2 codewords can be obtained by fixing the last rows and selecting the other row from the above three.

The d-optimality can be seen by the Griesmer bound as done above. □

Theorem 8: *The* $(12, 5)$ *binary linear block code having the first row of the generator matrix* $(5160)_8$ *and the remaining rows are the cyclic shift of the first row, is a* $[d, A_d]$*-optimal code with* $d = 4$ *and the WEF* $W(y) = 1 + y^4 + 10y^5 + 10y^6 + 5y^7 + 4y^8 + y^{11}$.

[2]For the sake of convenience, we use the MATLAB notation.

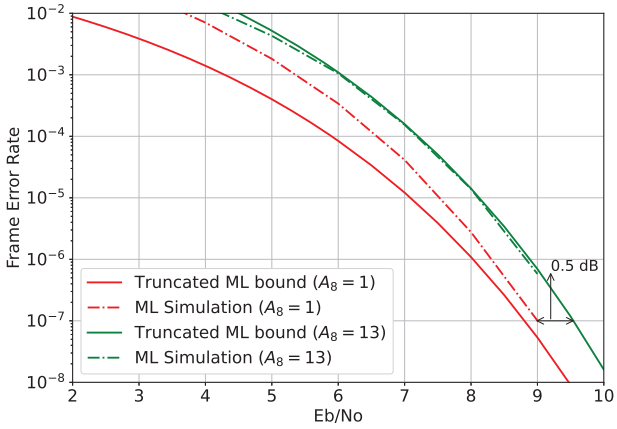

Fig. 1. Truncated ML bound for the comparison of our construction (red curves, constructed using Theorem 3) with best-known in [1] (green cruves) for the $(18, 4)$ BLBC. Our construction outperforms the best-known by 0.50 dB at the FER $= 10^{-7}$.

Proof. By listing all 32 codewords, we have the above WEF. The d-optimality can be seen by looking at the lower and upper bounds on the minimum distance given in [1], and $A_4 = 1$ proves the A_d-optimality. □

Theorem 9: *The* $(33, 5)$ *binary linear block code having the first row* $(76112546720)_8$ *and the remaining rows are the cyclic shift of the first row, is a* $[d, A_d]$*-optimal code with* $d = 16$ *and the WEF* $W(y) = 1 + 7y^{16} + 16y^{17} + 8y^{18}$.

Proof. The d-optimality can be seen by looking at the lower and upper bounds on the minimum distance given in [1]. By listing all 32 codewords, gives the above WEF. Then comparing A_{16} with the LP lower bound in Table I proves the A_d-optimality. □

IV. Numerical Results

Fig. 1 shows the simulation results of the ML decoding superimposed with the truncated ML bound for the $(18, 4)$ BLBC to compare our construction, which results in $A_8 = 1$, and the previously best-known construction having $A_8 = 13$ [1]. In Fig. 1, we can see that the estimated E_b/N_o gain is reasonably accurate at FER = 10^{-6}, and the accuracy gets better as the FER gets smaller. Our construction outperforms the best-known by 0.5 dB at a FER of 10^{-7}, as shown in Fig. 1. Table I compares the constructions of the BLBCs in [1] and presented in this work. Table I also includes the lower and upper bounds on the error coefficient A_d [5], computed using GAP [9]. In Table I, there are many codes for which our new constructions achieve the lower bounds on the error coefficient to assert the $[d, A_d]$-optimality. The WEF has an explicit expression for most of the codes presented here. The MacWilliams identity [8] can be applied straightforwardly to get the WEF of the dual codes.

An interesting observation can be made about the WEF of the $[d, A_d]$-optimal codes by looking at examples 1 & 2

TABLE I
COMPARISON OF OUR NEW CONSTRUCTIONS WITH PREVIOUSLY BEST-KNOWN CONSTRUCTIONS AND BOUNDS. THE ESTIMATED E_b/N_o GAIN IS CALCULATED BY (3) AT FER $= 10^{-7}$.

	Best-known [1], [5], [6]	**LP Bound [5], [6] (c.f. Section II-C)**		**New Constructions**		
$(\mathbf{n}, \mathbf{k}, \mathbf{d})$	$\mathbf{A_d}$	**Lower Bound**	**Upper Bound**	$\mathbf{A_d}$	**Estimated $\mathbf{E_b/N_o}$ Gain (dB)**	**Construction Method**
(8,3,4)	3	3	7	3	0	Corollary 5
(8,5,2)	15	1	15	1	0.771	Dual of the $(8, 3)$ code
(9,3,4)	1	1	7	1	0	Theorem 3
(9,6,2)	21	2	21	2	0.648	Dual of the $(9, 3)$ code
(10,4,4)	8	2	15	2	0.393	Theorem 4
(10,6,3)	8	7	11	8	0	Dual of the $(10, 4)$ code
(16,3,8)	6	1	7	1	0.524	Theorem 3
(16,13,2)	91	11	91	11	0.53	Dual of the $(16, 3)$ code
(18,4,8)	13	-1	15	1	0.63	Theorem 3
(18,14,2)	105	3	110	3	0.924	Dual of the $(18, 4)$ code
(19,5,8)	25	-1	31	2	0.692	Theorem 4
(19,14,3)	24	15	51	24	0	Dual of the $(19, 5)$ code
(21,4,10)	10	2	15	3	0.335	Corollary 7
(21,17,2)	153	5	159	6	0.815	Dual of the $(21, 4)$ code
(19,4,9)	4	-2	8	4	0	Corollary 4
(19,15,2)	120	3	125	4	0.873	Dual of the $(19, 4)$ code
(12,5,4)	12	-1	24	1	0.712	Theorem 8
(33,5,16)	30	7	31	7	0.381	Theorem 9
(33,4,16)	14	-1	15	1	0.753	Theorem 3
(33,29,2)	485	21	446	21	0.740	Dual of the $(33, 4)$ code
(36,4,18)	10	2	15	3	0.516	Corollary 7
(36,32,2)	528	26	540	27	0.694	Dual of the $(36, 4)$ code
(47,4,24)	14	3	15	3	0.424	Corollary 5
(47,43,2)	946	51	963	51	0.661	Dual of the $(47, 4)$ code
(66,5,32)	30	-9	31	1	0.948	Theorem 3
(133,7,64)	101	-63	127	1	1.243	Theorem 3
(158,5,80)	30	-1	31	3	0.619	Corollary 5

presented in Section III. The WEF has consecutive powers of the indeterminate y. This observation also holds for the $[d, A_d]$-optimal codes of theorems 8 & 9. However, we can explain this for the examples by looking at their generator matrices, a concatenation of the simplex code, and the identity matrix. The consecutive powers of the indeterminate are due to the identity matrix because simplex code has all codewords at the same distance. Nevertheless, for the codes in Theorems 8 & 9, we cannot explain this way. However, this observation holds for all $[d, A_d]$-optimal linear codes presented here.

V. CONCLUSION

In this article, we have constructed a class of $[d, A_d]$-optimal (n, k) linear codes of the maximum possible value of the minimum distance, and their error coefficients achieve the LP lower bound for most cases. In summary, for all positive integers m and k, and $0 \leq l \leq k-1$, we gave the constructions of $((2^k-1)m+l, k)$, $((2^k-1)+k, k+1)$, $(15m+4, 4)$, $(15m+6, 4)$, $(12, 5)$, and $(33, 5)$ BLBCs. Most of these codes are $[d, A_d]$-optimal linear codes. Hence, give the best possible FER performance under ML decoding in the asymptotic regime over the AWGN channel.

Our future work includes investigating the general structure of the generator matrices of the high-rate $[d, A_d]$-optimal linear codes.

REFERENCES

[1] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Online available at http://www.codetables.de, 2007, accessed on 2021-11-13.

[2] *3GPP TS 22.261 Service requirements for the 5G system; Stage 1 (Release 18)*, Sep. 2021.

[3] K. R. Duffy, J. Li, and M. Médard, "Capacity-achieving guessing random additive noise decoding," *IEEE Transactions on Information Theory*, vol. 65, no. 7, pp. 4023–4040, 2019.

[4] C.-Y. Lin, Y.-C. Huang, S.-L. Shieh, and P.-N. Chen, "Transformation of binary linear block codes to polar codes with dynamic frozen," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 333–341, 2020.

[5] P. Solé, Y. Liu, W. Cheng, S. Guilley, and O. Rioul, "Linear programming bounds on the kissing number of q-ary codes," in *2021 IEEE Information Theory Workshop (ITW2021)*, 2021.

[6] Y. Liu, W. Cheng, O. Rioul, S. Guilley, and P. Solé, "Kissing number of codes: A survey."

[7] T. K. Moon, *Error correction coding: mathematical methods and algorithms*. John Wiley & Sons, 2005.

[8] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*. Elsevier, 1977, vol. 16.

[9] *GAP – Groups, Algorithms, and Programming,Version 4.11.1*, The GAP Group, 2021. [Online]. Available: https://www.gap-system.org

[10] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, and A. Wassermann, *Error-correcting linear codes: Classification by isometry and applications*. Springer Science & Business Media, 2006, vol. 18.