

This is the peer reviewed version of the following article:

Radonjic Aleksandar, "Integer codes correcting single asymmetric errors" *Annals of Telecommunications*, 76, no. 1-2 (2021):109-113, <https://doi.org/10.1007/s12243-020-00816-w>



I. This work is licensed under a [Attribution-NonCommercial 4.0 International \(CC BY-NC 4.0\)](https://creativecommons.org/licenses/by-nc/4.0/)

Integer Codes Correcting Single Asymmetric Errors

Aleksandar Radonjic

Institute of Technical Sciences of the Serbian Academy of Sciences and Arts, Belgrade, Serbia

E-mail: sasa_radonjic@yahoo.com

Abstract: This paper presents a class of integer codes capable of correcting single asymmetric errors. The presented codes are defined over the ring of integers modulo $2^b - 1$ and are constructed with the help of a computer. The results of an exhaustive search have shown that, for practical lengths up to 4096 bits, the proposed codes use the same number of check-bits as the best systematic single asymmetric error correcting codes (SAECCs). Besides this, it is found that for some lengths the presented codes are perfect. Finally, the paper shows that the encoding/decoding complexity of the proposed codes is notably lower than that of the best systematic SAECCs.

Keywords: Integer codes, single asymmetric errors, error correction, perfect codes.

1. Introduction

Conventional coding theory is mainly focused on constructing codes for use over channels in which $1 \rightarrow 0$ and $0 \rightarrow 1$ errors occur with equal probability. However, it is known that some channels display only $1 \rightarrow 0$ errors. For example, in optical communications, photons may fade or fail to be detected ($1 \rightarrow 0$ errors), but the creation of spurious photons ($0 \rightarrow 1$ errors) is not possible [1]. Likewise, in some VLSI circuits and memories charges may leak with time ($1 \rightarrow 0$ errors), but new charges cannot be spontaneously created ($0 \rightarrow 1$ errors) [2].

Motivated by these and similar examples, researchers began constructing codes that correct asymmetric ($1 \rightarrow 0$) errors. Among them, special attention has been paid to the construction of single asymmetric error correcting codes (SAECCs). The reason for this was an attempt to design codes that would have higher rates than Hamming codes [3]. Although some successes have been achieved in the case of non-systematic codes [4]-[12], to date none systematic SAECC has been constructed that outperforms Hamming codes. This is not surprising given that Bose and Al-Bassam [13] showed that the best systematic SAECCs have the same parameters as Hamming codes, except possibly for the lengths $n = 2^u$ and $n = 2^u + 1$, where $u \geq 4$. In these two cases, as they stated, there may exist systematic SAECCs that are better than Hamming codes. However, such codes were never reported in the literature. The only known systematic SAECCs are those designed by Abdel-Ghaffar and Ferreira [14]. These codes are obtained by modifying group-theoretic (GT) codes [2], which means that they have the same parameters as Hamming codes.

In this paper, we will present a class of systematic SAECs that are significantly different from the codes proposed in [14]. The main difference is that the presented codes are not binary oriented, but are defined over the ring of integers modulo $2^b - 1$. In addition, unlike [14], they are constructed with the help of a computer. One consequence of these differences is that our codes are perfect only for certain lengths. However, as we will see, for all practical lengths up to 4096 bits, they use the same number of check-bits as the codes from [14].

The organization of this paper is as follows: Section 2 deals with the construction of integer codes capable of correcting single asymmetric errors. In Section 3, the proposed codes are evaluated and compared with the best systematic SAECs, while Section 4 concludes the paper.

2. Integer SAEC Codes

A. Codes Construction

As stated previously, the only known systematic SAECs are those obtained by modifying GT codes. According to [14], a modified GT (MGT) code can be defined as

$$C(n, d) = \left\{ u \in \{0, 1\}^n : \sum_{i=1}^K d_i \cdot u_i \equiv d \right\} \quad (1)$$

where $u = (u_1, \dots, u_K, u_{K+1}, \dots, u_n) \in \{0, 1\}^n$ is the codeword vector, d_i is the element of the Abelian group G of the order $K + 1$ and $d = \sum_{i=K+1}^n u_i \cdot 2^{i-K+1}$ is a fixed integer in G . Unlike MGT codes, the presented ones are defined over the ring of integers modulo $2^b - 1$. This is formally described by the following definitions.

Definition 1. [15] Let $Z_{2^b-1} = \{0, 1, \dots, 2^b - 2\}$ be the ring of integers modulo $2^b - 1$ and let $B_i = \sum_{n=0}^{b-1} a_n \cdot 2^n$ be the integer representation of a b -bit byte, where $a_n \in \{0, 1\}$ and $1 \leq i \leq k$. Then, the code $C(b, k, c)$, defined as

$$C(b, k, c) = \left\{ x \in Z_{2^b-1}^{k+1} : \sum_{i=1}^k C_i \cdot B_i \equiv B_{k+1} \pmod{2^b - 1} \right\} \quad (2)$$

is an $(kb + b, kb)$ integer code, where $x = (B_1, B_2, \dots, B_k, B_{k+1}) \in Z_{2^b-1}^{k+1}$ is the codeword vector, $c = (C_1, C_2, \dots, C_k, 1) \in Z_{2^b-1}^{k+1}$ is the coefficient vector and $B_{k+1} \in Z_{2^b-1}$ is an integer.

Definition 2. [16] Let $x = (B_1, B_2, \dots, B_k, B_{k+1}) \in Z_{2^b-1}^{k+1}$, $y = (\underline{B}_1, \underline{B}_2, \dots, \underline{B}_k, \underline{B}_{k+1}) \in Z_{2^b-1}^{k+1}$ and $e = (\underline{B}_1 - B_1, \underline{B}_2 - B_2, \dots, \underline{B}_k - B_k, B_{k+1} - \underline{B}_{k+1}) = (e_1, e_2, \dots, e_k, e_{k+1}) \in Z_{2^b-1}^{k+1}$ be respectively, the sent codeword, the received codeword and the error vector. Then, the syndrome S of the received codeword is defined as

$$S = \sum_{i=1}^k C_i \cdot \underline{B}_i - \underline{B}_{k+1} \pmod{2^b - 1} = \sum_{i=1}^{k+1} e_i \cdot C_i \pmod{2^b - 1} \quad (3)$$

Definition 3. An $(kb + b, kb)$ integer code is called SAEC if it can correct error vectors from the set $\varepsilon = \{(-2^r, 0, \dots, 0, 0), \dots, (0, 0, \dots, -2^r, 0), (0, 0, \dots, 0, 2^r)\}$, where $1 \leq r \leq b - 1$.

Definition 4. The error set for $(kb + b, kb)$ integer SAECCs is defined by

$$\zeta_{b,k} = s_1 \cup s_2 \quad (4)$$

where

$$s_1 = \left\{ -2^r \cdot C_i \pmod{2^b-1} : 0 \leq r \leq b-1, 1 \leq i \leq k \right\} \quad (5)$$

$$s_2 = \left\{ 2^r : 0 \leq r \leq b-1 \right\} \quad (6)$$

From the above it is obvious that integer SAECCs cannot be constructed without knowing the values of the C_i 's. This fact, however, does not prevent us to state the following theorems.

Theorem 1. An $(kb + b, kb)$ integer SAECC exists only if

$$|\zeta_{b,k}| = b \cdot (k+1),$$

where $|\zeta_{b,k}|$ denotes the cardinality of $\zeta_{b,k}$.

Proof. Observe that the set $\zeta_{b,k}$ can be expressed as

$$\zeta_{b,k} = \bigcup_{i=1}^{k+1} m_i$$

where

$$m_1 = \left\{ -2^r \cdot C_1 \pmod{2^b-1} : 0 \leq r \leq b-1 \right\},$$

M

$$m_k = \left\{ -2^r \cdot C_k \pmod{2^b-1} : 0 \leq r \leq b-1 \right\},$$

$$m_{k+1} = \left\{ 2^r : 0 \leq r \leq b-1 \right\}.$$

The elements of the above subsets will be nonzero and mutually different only if the coefficients C_i have values such that

$$m_1 \cap \dots \cap m_k \cap m_{k+1} = \emptyset,$$

$$|m_1| = L = |m_k| = |m_{k+1}|.$$

As a result, it follows that

$$|\zeta_{b,k}| = |m_1| + L + |m_k| + |m_{k+1}| = |m_{k+1}| \cdot (k+1) = b \cdot (k+1). \quad \square$$

Theorem 2. For any $(kb + b, kb)$ integer SAECC it holds that

$$k \leq \left\lfloor \frac{2^b - b - 2}{b} \right\rfloor.$$

Proof. From Theorem 1 we know that the set $\zeta_{b,k}$ has $b \cdot (k+1)$ nonzero elements. On the other hand, Definition 1 says that the total number of nonzero syndromes is equal to $2^b - 2$. Obviously, we have the inequality

$$b \cdot (k+1) \leq 2^b - 2$$

wherefrom it follows that

$$k \leq \left\lfloor \frac{2^b - b - 2}{b} \right\rfloor. \quad \square$$

Theorem 3. Any perfect $(kb+b, kb)$ integer SAECC, if exists, has a rate of $(2^b-b-2)/(2^b-2)$.

Proof. This theorem follows directly from Theorem 2.

Table 1. Number of Coefficients for Integer SAECCs with Parameter $b \leq 12$.

	$b=3$	$b=4$	$b=5$	$b=6$	$b=7$	$b=8$	$b=9$	$b=10$	$b=11$	$b=12$
Bound	1	2	5	9	17	30	55	101	185	340
Experiment	1	2	5	8	17	29	55	98	185	334

Table 2. Coefficients for Integer SAECCs with Parameter $b \leq 12$.

$b=3$																			
2																			
$b=4$																			
2	3																		
$b=5$																			
2	3	5	7	11															
$b=6$																			
2	3	5	7	11	13	15	23												
$b=7$																			
2	3	5	7	9	11	13	15	19	21	23	27	29	31	43	47	55			
$b=8$																			
2	3	5	7	9	11	13	15	19	21	23	25	27	29	31	37	39	43	45	47
53	55	59	61	63	87	91	95	111											
$b=9$																			
2	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	35	37	39	41
43	45	47	51	53	55	57	59	61	63	75	77	79	83	85	87	91	93	95	103
107	109	111	117	119	123	125	127	171	175	183	187	191	223	239					
$b=10$																			
2	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	35	37	39	41
43	45	47	49	51	53	55	57	59	61	63	69	71	73	75	77	79	83	85	87
89	91	93	95	101	103	105	107	109	111	115	117	119	121	123	125	127	147	149	151
155	157	159	167	171	173	175	179	181	183	187	189	191	205	207	213	215	219	221	223
235	237	239	245	247	251	253	255	343	347	351	367	375	379	383	439	447	479		
$b=11$																			
2	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39
41	43	45	47	49	51	53	55	57	59	61	63	67	69	71	73	75	77	79	81
83	85	87	89	91	93	95	99	101	103	105	107	109	111	113	115	117	119	121	123
125	127	137	139	141	143	147	149	151	153	155	157	159	163	165	167	169	171	173	175
179	181	183	185	187	189	191	199	201	203	205	207	211	213	215	217	219	221	223	229
231	233	235	237	239	243	245	247	249	251	253	255	293	295	299	301	303	307	309	311
315	317	319	331	333	335	339	341	343	347	349	351	359	363	365	367	371	373	375	379
381	383	411	413	415	423	427	429	431	437	439	443	445	447	463	469	471	475	477	479
491	493	495	501	503	507	509	511	683	687	695	699	703	727	731	735	751	759	763	767
879	887	895	959	991															
$b=12$																			
2	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39
41	43	45	47	49	51	53	55	57	59	61	63	67	69	71	73	75	77	79	81
83	85	87	89	91	93	95	97	99	101	103	105	107	109	111	113	115	117	119	121
123	125	127	133	135	137	139	141	143	145	147	149	151	153	155	157	159	163	165	167
169	171	173	175	177	179	181	183	185	187	189	191	197	199	201	203	205	207	209	211
213	215	217	219	221	223	227	229	231	233	235	237	239	241	243	245	247	249	251	253
255	275	277	279	281	283	285	287	291	293	295	297	299	301	303	307	309	311	313	315
317	319	327	329	331	333	335	339	341	343	345	347	349	351	355	357	359	361	363	365
367	371	373	375	377	379	381	383	397	399	403	405	407	409	411	413	415	421	423	425
427	429	431	435	437	439	441	443	445	447	457	459	461	463	467	469	471	473	475	477
479	485	487	489	491	493	495	499	501	503	505	507	509	511	587	589	591	595	597	599
603	605	607	613	615	619	621	623	627	629	631	635	637	639	661	663	667	669	671	679
683	685	687	691	693	695	699	701	703	717	719	723	725	727	731	733	735	743	747	749
751	755	757	759	763	765	767	821	823	827	829	831	847	853	855	859	861	863	871	875
877	879	885	887	891	893	895	925	927	939	941	943	949	951	955	957	959	981	983	987
989	991	1003	1005	1007	1013	1015	1019	1021	1023	1367	1371	1375	1387	1391	1399	1403	1407	1455	1463
1467	1471	1499	1503	1519	1527	1531	1535	1759	1775	1783	1791	1919	1983						

The last step in constructing integer SAECCs is to find the C_i 's that satisfy the condition of Theorem 1. For that purpose it is necessary to perform an exhaustive search on all possible candidates from the set $Z_{2^{b-1}} \setminus \{0,1\}$. In this paper, we have restricted ourselves to values of b less than or equal to 12. The reason for this is twofold: first, the number of the C_i 's roughly doubles with the increase of b (Tables 1 and 2), and second, for the mentioned values of b the proposed codes are fully comparable with those presented in [15].

B. Error Correction Procedure

The error correction procedure for the presented codes is very similar to those described in [15], [16]. In short, if $S \neq 0$, the decoder will lookup the syndrome table (ST) to find the entry with the error correction data. After that, in the next step, it will execute the operation

$$B_i = \underline{B}_i + \underline{E} \pmod{2^b - 1} \quad (7)$$

where $\underline{E} \in \{2^r: 0 \leq r \leq b-1\}$. To generate the ST it is necessary to substitute the values of b and C_i into (5)-(6). In this way, exactly $|\zeta_{b,k}|$ (Theorem 1) relationships (Fig. 1) between the nonzero syndrome (element of the set $\zeta_{b,k}$), error location (i) and error vector (\underline{E}) will be established. So, when $S \neq 0$, the decoder's task will be to find the entry with the first b bits as that of the syndrome S .

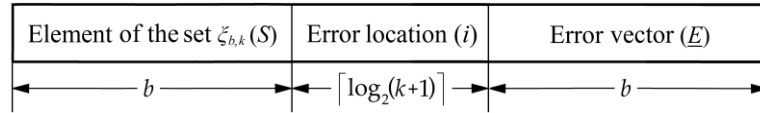


Fig. 1. Bit-width of one syndrome table entry.

Example 1. Let $b = 5$, $k = 5$, $C_1 = 2$, $C_2 = 3$, $C_3 = 5$, $C_4 = 7$ and $C_5 = 11$. According to Theorem 1, the ST will have $|\zeta_{5,5}| = 25$ entries (Table 3). Now, suppose that the encoder needs to encode 25 data bits, $D = 10101\ 11001\ 10010\ 00110\ 01010$. From (3) we know that the value of the last (sixth) byte will be equal to

$$B_{k+1} = B_6 = 2 \cdot 21 + 3 \cdot 25 + 5 \cdot 18 + 7 \cdot 6 + 11 \cdot 10 \pmod{31} = 18 = 10010_2$$

the codeword will have the form $x = (B_1, B_2, B_3, B_4, B_5, B_6) = (10101_2, 11001_2, 10010_2, 00110_2, 01010_2, 10010_2) = (21, 25, 18, 6, 10, 18)$. Assume now that the 5th bit is flipped. In that case, the codeword will have the form $y = (\underline{B}_1, \underline{B}_2, \underline{B}_3, \underline{B}_4, \underline{B}_5, \underline{B}_6) = (10100_2, 11001_2, 10010_2, 00110_2, 01010_2, 10010_2) = (20, 25, 18, 6, 10, 18)$. As explained previously, the decoder will perform the operation

$$S = 2 \cdot 20 + 3 \cdot 25 + 5 \cdot 18 + 7 \cdot 6 + 11 \cdot 10 - 18 \pmod{31} = 29$$

after which it will conclude that the first byte is in error (Table 3). As a result, it will execute the operation

$$B_1 = 20 + 1 \pmod{31} = 21.$$

Table 3. The ST for the Perfect (30, 25) Integer SAEC Code.

	S	i	\underline{E}		S	i	\underline{E}		S	i	\underline{E}		S	i	\underline{E}		S	i	\underline{E}				
1	1	6	1		7	7	2	8		13	13	3	16		19	19	2	4		25	25	2	2
2	2	6	2		8	8	6	8		14	14	2	16		20	20	5	1		26	26	3	1
3	3	4	4		9	9	5	2		15	15	1	8		21	21	3	2		27	27	1	2
4	4	6	4		10	10	5	16		16	16	6	16		22	22	3	8		28	28	2	1
5	5	5	8		11	11	3	4		17	17	4	2		23	23	1	4		29	29	1	1
6	6	4	8		12	12	4	16		18	18	5	4		24	24	4	1		30	30	1	16

3. Evaluation and Comparison

To evaluate the rate efficiency of the proposed codes, it is necessary to analyze data shown in Table 1. The first thing we notice from this table is an excellent agreement between the theory and experiments. More precisely, we see that for byte lengths $b = 3, 4, 5, 7, 9$ and 11 bits, we can construct six codes reaching the bound given in Theorem 2. These codes are either perfect ((30, 25), (126, 119) and (2046, 2035)), or optimal ((6, 3), (12, 8) and (504, 495)) in the sense of maximum rate. On the other hand, we also see that for byte lengths $b = 6, 8, 10$ and 12 bits we cannot construct perfect or optimal codes.

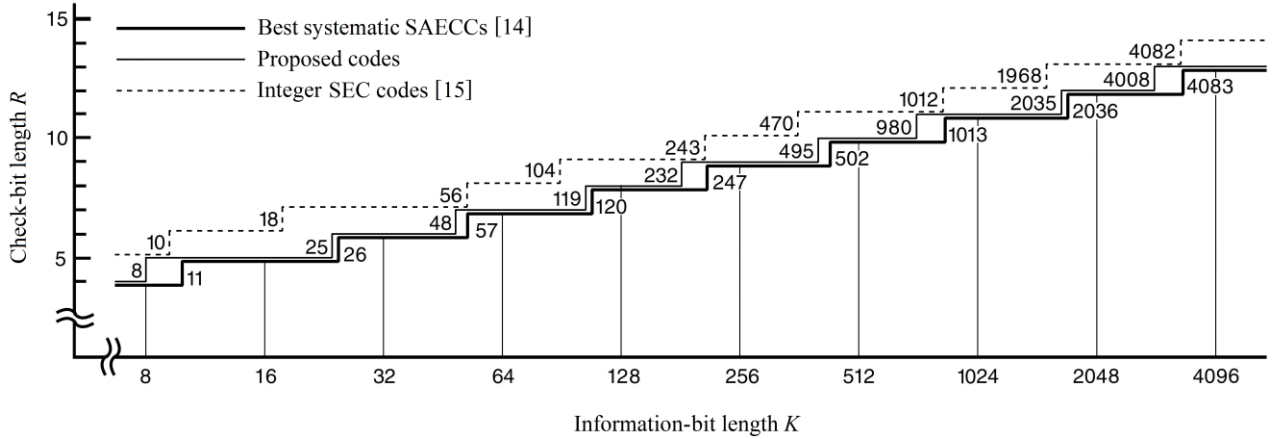


Fig. 2. Comparison of information-bit lengths and check-bit lengths of the best systematic SAECs [14], the proposed codes and integer SEC codes [15].

Despite this shortcoming, the presented codes are very efficient in terms of redundancy. To illustrate this, in Fig. 2, they are compared with codes from [14] and [15]. As we can see, for practical data lengths up to 4096 bits, the proposed codes require the same number of check-bits as the best systematic SAECs [14] and one check-bit less than integer single error correcting (SEC) codes [15]. Besides this, from Fig. 2, it can be observed that perfect integer SAECs have slightly lower rates than the codes from [14]. The reason for this is that the proposed codes are defined over an alphabet $\{0, 1, \dots, 2^b - 2\}$, which is a subset of the set $\{0, 1, \dots, 2^b - 1\}$.

On the other hand, the main advantage of the proposed codes over the best systematic SAECs lies in the ability to faster encode/decode data bits. Namely, from [16] we know that any integer encoder/decoder must perform approximately $b \cdot K$ operations per K -bit data word. In

contrast to this, from (1) we observe that the MGT encoder/decoder executes two operations at the bit level: one multiplication between d_i and u_i ($\lceil \log_2(K+1) \rceil$ operations) and one addition between two $\lceil \log_2(K+1) \rceil$ -bit integers ($\lceil \log_2(K+1) \rceil$ operations). Considering that there exist K data bits, we easily come to the conclusion that the MGT encoder/decoder must perform approximately $K \cdot \log_2 K$ operations per K -bit data word. This means that the encoding/decoding complexity grows linearithmic with the data length, while in the case of proposed codes it increases linearly.

4. Conclusion

This paper proposed a class of integer codes capable of correcting single asymmetric errors. The proposed codes are constructed with the help of a computer and are very close to being optimal in terms of redundancy. The results of an exhaustive search have shown that, for practical data lengths up to 4096 bits, the proposed codes use the same number of check-bits as the best systematic single asymmetric error correcting codes. In addition, it has been shown that, for some lengths the proposed codes are perfect. The parameters of these codes are $(2^b - 2, 2^b - b - 2)$, which makes them one of the most rate-efficient codes in the literature.

References

- [1] J. M. Borden, "Optimal Asymmetric Error Detecting Codes," *Inf. Control*, vol. 53, nos. 1-2, pp. 66-73, Apr.-May. 1982.
- [2] S. D. Constantin and T. R. N. Rao, "On the Theory of Binary Asymmetric Error Correcting Codes," *Inf. Control*, vol. 40, no. 1, pp. 20-26, Jan. 1979.
- [3] R. W. Hamming, "Error Detecting and Error Correcting Codes," *Bell Syst. Tech. J.*, vol. 29, no. 2, pp. 147-150, Apr. 1950.
- [4] R. R. Varshamov and G. M. Tenengol'ts, "Correction Code for Single Asymmetric Errors," *Automat. Telemekh.*, vol. 26, no. 2, pp. 288-292, Feb. 1965.
- [5] P. Delsarte and P. Piret, "Bounds and Constructions for Binary Asymmetric Error-Correcting Codes," *IEEE Trans. Inform. Theory*, vol. 27, no. 1, pp. 125-128, Jan 1981.
- [6] A. Shiozaki, "Single Asymmetric Error-Correcting Cyclic AN Codes," *IEEE Trans. Comput.*, vol. 31, no. 6, pp. 554-555, June 1982.
- [7] J. Weber, C. DeVroedt and D. Boeke, "Bounds and Construction for Binary Codes of Length Less than 24 and Asymmetric Distance Less than 6," *IEEE Trans. Inform. Theory*, vol. 34, no. 5, pp. 1321-1331, Sept. 1988.
- [8] Z. Zhang and X. Xia, "New Lower Bounds for Binary Codes of Asymmetric Distance Two," *IEEE Trans. Inform. Theory*, vol. 38, no. 5, pp. 1592-1597, Sept. 1992.
- [9] S. Al-Bassam, R. Venkatesan and S. Al-Muhammadi, "New Single Asymmetric Error Correcting Codes," *IEEE Trans. Inform. Theory*, vol. 43, no. 5, pp. 1619-1623, Sept. 1997.
- [10] S. Al-Bassam and S. Al-Muhammadi, "A Single Asymmetric Error-Correcting Code with 2^{13} Codewords of Dimension 17," *IEEE Trans. Inform. Theory*, vol. 46, no. 1, pp. 269-271, Jan. 2000.
- [11] F. Fu, S. Ling and C. Xing, "New Lower Bounds and Constructions for Binary Codes Correcting Asymmetric Errors," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3294-3299, Dec. 2003.

- [12] M. Grassl, P. Shor, G. Smith, J. Smolin and B. Zeng, "New Constructions of Codes for Asymmetric Channels Via Concatenation", *IEEE Trans. Inform. Theory*, vol. 61, no. 4, pp. 1879-1886, Apr. 2015.
- [13] B. Bose and S. Al-Bassam, "On Systematic Single Asymmetric Error Correcting Codes," *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 669-672, Mar. 2000.
- [14] K. Abdel-Ghaffar and H. Ferreira, "Systematic Encoding of the Varshamov-Tenengol'ts Codes and the Constantin-Rao Codes," *IEEE Trans. Inform. Theory*, vol. 43, no. 1, pp. 340-354, Jan. 1997.
- [15] A. Radonjic, "(Perfect) Integer Codes Correcting Single Errors," *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 17-20, Jan. 2018.
- [16] A. Radonjic and V. Vujicic, "Integer Codes Correcting Burst Errors within a Byte," *IEEE Trans. Comput.*, vol. 62, no. 2, pp. 411-415, Feb. 2013.