This is the peer reviewed version of the following article:

Radonjic, A., Vujicic, V., 2019. Integer codes correcting sparse byte errors.
Cryptography and Communications. https://doi.org/10.1007/s12095-019-0350-9


This work is licensed under a Creative Commons Attribution Non Commercial No Derivatives 4.0 license

# Integer Codes Correcting Sparse Byte Errors 

Aleksandar Radonjic* and Vladimir Vujicic<br>Institute of Technical Sciences of the Serbian Academy of Sciences and Arts, Belgrade, Serbia E-mails: sasa_radonjic@yahoo.com, vujicicv@yahoo.com (*Corresponding author)


#### Abstract

In public optical networks, the data are scrambled with a $x^{u}+1$ self-synchronous scramblers (SSSs). The reason for this is to avoid long strings of ones or zeros, which might affect the receiver synchronization. Unfortunately, the use of SSSs is always related to the problem of duplication of channel errors. More precisely, each error occurring during the transmission will be duplicated $u$ bits later. In this paper, we present a low-cost solution to this problem based on integer codes capable of correcting sparse byte errors.


Keywords: Integer codes, sparse byte errors, error correction, public optical networks.

## 1. Introduction

In many communication networks the data are randomized before transmission. The reason for this is to avoid long strings of 1 s or 0 s , which might affect the receiver synchronization. In public optical networks (PONs), such as synchronous optical network (SONET) and high-level data link control (HDLC) [1], the process of randomization is performed using self-synchronous scramblers (SSSs). These devices modify the data by XORing two bits that are spaced $u$ bits apart ( $u=29$ or 43) [6]-[10]. Such sequence is then sent to the receiver, which performs the same operation to recover the original unscrambled data.

Although this procedure is simple to implement, it has a drawback of error duplication. In other words, each error occurring during the transmission will be duplicated $u$ bits later. In mentioned networks, where random errors dominate [2]-[5], this will cause the appearance of two errors which cannot be corrected by standard cyclic redundancy check (CRC) codes. In order to overcome this problem, the researchers proposed the use of modified CRC codes (mCRCCs) [6]-[10]. These codes were preferred over other codes (e.g. BCH codes) due to their lower decoding complexity. In practice, however, such a solution would be complex to implement, since it is also based on the modification of existing network hardware (SONET terminals, HDLC controllers, etc.).

Bearing this in mind, in this paper, we present a class of integer codes that are suitable for use in modern PONs. Compared to m-CRCCs, these codes have three advantages. First, they use integer and lookup table operations, which are supported by all processors [11]. As a result, they can be implemented "for free" (in software), i.e. without modifying the network hardware. The second advantage is that the proposed codes can correct three types of errors within a $b$-bit byte:
single errors, double errors and triple-adjacent errors. Hence, they are more powerful than the codes suggested in [6]-[10]. Finally, the proposed codes can be interleaved without delay and without using dedicated hardware. Thanks to this, it is possible to construct simple codes capable of correcting errors affecting several consecutive bytes.

The organization of this paper is as follows: Section 2 deals with the construction of integer codes capable of correcting sparse byte (SB) errors. The error control procedure and theoretical decoding throughputs for these codes are described and evaluated in Section 3. Finally, Section 4 concludes the paper.

## 2. Codes Construction

In this section, we start with four definitions that are related to the construction of integer codes capable of correcting SB errors.

Definition 1. An error is called a SB error if, within a b-bit byte, one, two random or three adjacent bits are in error.

Definition 2. Let $Z_{2^{b}-1}=\left\{0,1, \ldots, 2^{b}-2\right\}$ 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
$C(b, k, c)=\left\{\left(B_{1}, B_{2}, \ldots, B_{k}, B_{k+1}\right) \in Z_{2^{b}-1}^{k+1}: \sum_{i=1}^{k} C_{i} \cdot B_{i} \equiv B_{k+1}\left(\bmod 2^{b}-1\right)\right\}$
is an $(k b+b, k b)$ integer code, where $c=\left(C_{1}, C_{2}, \ldots, C_{k}, 1\right) \in Z_{2^{b}-1}^{k+1}$ is the coefficient vector and $B_{k+1} \in Z_{2^{b}-1}$ is an integer.

Definition 3. Let $x=\left(B_{1}, B_{2}, \ldots, B_{k}, B_{k+1}\right) \in Z_{2^{b}-1}^{k+1}, y=\left(\underline{B}_{1}, \underline{B}_{2}, \ldots, \underline{B}_{k}, \underline{B}_{k+1}\right) \in Z_{2^{b}-1}^{k+1}$ and $e=y-$ $x=\left(\underline{B}_{1}-B_{1}, \underline{B}_{2}-B_{2}, \ldots, \underline{B}_{k}-B_{k}, \underline{B}_{k+1}-B_{k+1}\right)=\left(e_{1}, e_{2}, \ldots, e_{k}, e_{k+1}\right) \in Z_{2^{b}-1}^{k+1}$ be respectively, the sent codeword, the received codeword and the error vector. Then, the syndrome $S$ of the received codeword is defined as

$$
\begin{equation*}
S=\sum_{i=1}^{k}\left(C_{i} \cdot \underline{B}_{i}-\underline{B}_{k+1}\right)\left(\bmod 2^{b}-1\right)=\sum_{i=1}^{k+1} e_{i} \cdot C_{i}\left(\bmod 2^{b}-1\right) \tag{2}
\end{equation*}
$$

Definition 4. An $(k b+b, k b)$ integer code is called SB error correcting (SBEC) if it can correct error vectors from the set $E=\left\{\left(e_{i}, 0, \ldots, 0,0\right), \ldots,\left(0,0, \ldots, e_{i}, 0\right),\left(0,0, \ldots, 0, e_{i}\right)\right\}$, where $e_{i} \in\left\{ \pm 2^{r}, \pm 2^{s} \pm 2^{t},\left( \pm 2^{2} \pm 2^{1} \pm 2^{0}\right) \cdot 2^{m}\right\}, 0 \leq r \leq b-1,0 \leq s<t \leq b-1$ and $0 \leq m \leq b-3$.

Definition 5. The error set for an $(k b+b, k b)$ integer SBEC code is defined by $\xi=s_{1} \cup s_{2} \cup s_{3}$
where
$s_{1}=\left\{\bigcup_{i=1}^{k+1}\left( \pm 2^{r} \cdot C_{i}\right)\left(\bmod 2^{b}-1\right): 0 \leq r \leq b-1\right\}$,

$$
\begin{align*}
& s_{2}=\left\{\bigcup_{i=1}^{k+1}\left[\left( \pm 2^{r} \pm 2^{s}\right) \cdot C_{i}\right]\left(\bmod 2^{b}-1\right): 0 \leq r<s \leq b-1\right\},  \tag{5}\\
& s_{3}=\left\{\bigcup_{i=1}^{k+1}\left[\left( \pm 2^{2} \pm 2^{1} \pm 2^{0}\right) \cdot 2^{m} \cdot C_{i}\right]\left(\bmod 2^{b}-1\right): 0 \leq m \leq b-3\right\} . \tag{6}
\end{align*}
$$

With these definitions, we are ready to state the following theorem.
Theorem 1. The sets $s_{1}$ and $s_{3}$ are subsets of $s_{2}$.
Proof. An element $\alpha$ of $s_{1}$ takes the form $\left( \pm 2^{r} \cdot C_{i}\right)\left(\bmod 2^{b}-1\right)$, where $0 \leq r \leq b-1$. The set $s_{2}$ contains elements $\beta$ taking the form $\left[\left( \pm 2^{r} \pm 2^{s}\right) \cdot C_{i}\right]\left(\bmod 2^{b}-1\right)$, where $0 \leq r<s \leq b-1$. Obviously, if $s=r+1, \beta$ will take two forms: $\beta_{1}=\left( \pm 2^{r} \cdot C_{i}\right)\left(\bmod 2^{b}-1\right)$ and $\beta_{2}=\left( \pm 3 \cdot 2^{r} \cdot C_{i}\right)$ $\left(\bmod 2^{b}-1\right)$, where $0 \leq r \leq b-2$. On the other hand, if $r=0$ and $s=b-1, \beta$ will take the form $\beta_{3}=\left[\left( \pm 1 \pm 2^{b-1}\right) \cdot C_{i}\right]\left(\bmod 2^{b}-1\right)=\left(\mp 2^{b-1} \cdot C_{i}\right)\left(\bmod 2^{b}-1\right)$. For this it is easy to conclude that $\alpha=\beta_{1} \cup \beta_{3}$, i.e. that $s_{1} \subseteq s_{2}$. Similarly, an element $\gamma$ of $s_{3}$ takes the form $\left[\left( \pm 2^{2} \pm 2^{1} \pm 2^{0}\right) \cdot 2^{m} \cdot C_{i}\right]$ $\left(\bmod 2^{b}-1\right)$, where $0 \leq m \leq b-3$. Note that this element is of the form $\left( \pm \delta \cdot 2^{m} \cdot C_{i}\right)\left(\bmod 2^{b}-\right.$ 1), where $\delta \in\{1,3,5,7\}$. Now, if $\delta=1$, then $\gamma_{1}=\left( \pm 2^{m} \cdot C_{i}\right)\left(\bmod 2^{b}-1\right) \in \alpha \subseteq \beta$. If $\delta=3$, then $\gamma_{2}=\left( \pm 3 \cdot 2^{m} \cdot C_{i}\right)\left(\bmod 2^{b}-1\right)=\left[ \pm\left(2^{m+1}+2^{m}\right) \cdot C_{i}\right]\left(\bmod 2^{b}-1\right) \in \beta$. If $\delta=5$, then $\gamma_{3}=\left( \pm 5 \cdot 2^{m}\right.$. $\left.C_{i}\right)\left(\bmod 2^{b}-1\right)=\left[ \pm\left(2^{m+2}+2^{m}\right) \cdot C_{i}\right]\left(\bmod 2^{b}-1\right) \in \beta$. Finally, if $\delta=7$, then $\gamma_{4}=\left( \pm 7 \cdot 2^{m} \cdot C_{i}\right)$ $\left(\bmod 2^{b}-1\right)=\left[ \pm\left(2^{m+3}-2^{m}\right) \cdot C_{i}\right]\left(\bmod 2^{b}-1\right) \in \beta$. In all cases, $\gamma \subseteq \beta$. Hence, $s_{3} \subseteq s_{2}$.
Now we can prove the main theorem of this section.
Theorem 2. The codes defined by (1) can correct all SB errors only if there exist $k$ mutually different coefficients $C_{i} \in Z_{2^{b_{-1}}} \backslash\{0,1\}$ such that

$$
|\xi|=\left|s_{2}\right|=\left[2 \cdot(b-1)^{2}-2\right] \cdot(k+1),
$$

where $|A|$ is the cardinality of $A$.
Proof. To prove the theorem, observe that the set $s_{2}$ can be express as the union
$s_{2}=\bigcup_{j=1}^{2 b-2} R_{j}$
where

$$
\begin{aligned}
& R_{1}=\left\{\left[ \pm\left(2^{1}-2^{0}\right) \cdot 2^{r} \cdot C_{i}\right]\left(\bmod 2^{b}-1\right): 0 \leq r \leq b-2,1 \leq i \leq k+1\right\} \\
& R_{2}=\left\{\left[ \pm\left(2^{1}+2^{0}\right) \cdot 2^{r} \cdot C_{i}\right]\left(\bmod 2^{b}-1\right): 0 \leq r \leq b-2,1 \leq i \leq k+1\right\} \\
& R_{3}=\left\{\left[ \pm\left(2^{2}-2^{0}\right) \cdot 2^{r} \cdot C_{i}\right]\left(\bmod 2^{b}-1\right): 0 \leq r \leq b-3,1 \leq i \leq k+1\right\} \\
& R_{4}=\left\{\left[ \pm\left(2^{2}+2^{0}\right) \cdot 2^{r} \cdot C_{i}\right]\left(\bmod 2^{b}-1\right): 0 \leq r \leq b-3,1 \leq i \leq k+1\right\} \\
& R_{5}=\left\{\left[ \pm\left(2^{3}-2^{0}\right) \cdot 2^{r} \cdot C_{i}\right]\left(\bmod 2^{b}-1\right): 0 \leq r \leq b-4,1 \leq i \leq k+1\right\} \\
& R_{6}=\left\{\left[ \pm\left(2^{3}+2^{0}\right) \cdot 2^{r} \cdot C_{i}\right]\left(\bmod 2^{b}-1\right): 0 \leq r \leq b-4,1 \leq i \leq k+1\right\}
\end{aligned}
$$

$$
\begin{aligned}
& R_{2 b-7}=\left\{\left[ \pm\left(2^{b-3}-2^{0}\right) \cdot 2^{r} \cdot C_{i}\right]\left(\bmod 2^{b}-1\right): 0 \leq r \leq 2,1 \leq i \leq k+1\right\} \\
& R_{2 b-6}=\left\{\left[ \pm\left(2^{b-3}+2^{0}\right) \cdot 2^{r} \cdot C_{i}\right]\left(\bmod 2^{b}-1\right): 0 \leq r \leq 2,1 \leq i \leq k+1\right\} \\
& R_{2 b-5}=\left\{\left[ \pm\left(2^{b-2}-2^{0}\right) \cdot 2^{r} \cdot C_{i}\right]\left(\bmod 2^{b}-1\right): 0 \leq r \leq 1,1 \leq i \leq k+1\right\} \\
& R_{2 b-4}=\left\{\left[ \pm\left(2^{b-2}+2^{0}\right) \cdot 2^{r} \cdot C_{i}\right]\left(\bmod 2^{b}-1\right): 0 \leq r \leq 1,1 \leq i \leq k+1\right\} \\
& R_{2 b-3}=\left\{\left[ \pm\left(2^{b-1}-2^{0}\right) \cdot 2^{r} \cdot C_{i}\right]\left(\bmod 2^{b}-1\right): r=0,1 \leq i \leq k+1\right\} \\
& R_{2 b-2}=\left\{\left[ \pm\left(2^{b-1}+2^{0}\right) \cdot 2^{r} \cdot C_{i}\right]\left(\bmod 2^{b}-1\right): r=0,1 \leq i \leq k+1\right\}
\end{aligned}
$$

The syndromes caused by SB errors will be nonzero and mutually different only if there exists $k$ different coefficients $C_{i} \in Z_{2^{b^{-1}}} \backslash\{0,1\}$ such that

$$
\begin{aligned}
& R_{1} \cap R_{2} \cap \cdots \cap R_{2 b-2}=\varnothing \\
& \left|R_{2 t-1}\right|=\left|R_{2 t}\right|=2 \cdot(b-t) \cdot(k+1), t=1,2, \ldots, b-1 .
\end{aligned}
$$

Further, if we compare the sets $R_{2}, R_{3}, R_{2 b-2}$ and $R_{2 b-5}$ we can note that $R_{2 b-5} \subseteq\left(R_{2 b-2} \cup R_{2}\right)$ and $R_{3} \subseteq R_{2}$. As a result, it follows that
$\left|s_{2}\right|=\sum_{j=1}^{2 b-2}\left|R_{j}\right|-\left|R_{3}\right|-\left|R_{2 b-5}\right|=\left[4 \cdot \sum_{j=1}^{b-1}(b-j)-(b-2)-2\right] \cdot(k+1)=\left[2 \cdot(b-1)^{2}-2\right] \cdot(k+1)$.
Conversely, if the codes satisfy the above condition, then we correct all SB errors. Therefore, these codes are $(k b+b, k b)$ integer SBEC codes.

Now, by knowing the cardinality of $s_{2}$, we can derive the upper bound on code length.
Theorem 3. For any $(k b+b, k b)$ integer SBEC code it holds that

$$
k \leq\left\lfloor\frac{2^{b-1}-(b-1)^{2}}{(b-1)^{2}-1}\right\rfloor
$$

Proof. From Definition 1 we know that the total number of nonzero syndromes is $2^{b}-2$. In addition, from Theorem 2 we know that the set $s_{2}$ has $\left[2 \cdot(b-1)^{2}-2\right] \cdot(k+1)$ nonzero elements. Consequently, we have the inequality
$\left[2 \cdot(b-1)^{2}-2\right] \cdot(k+1) \leq 2^{b}-2$
wherefrom it follows that
$k \leq\left\lfloor\frac{2^{b-1}-(b-1)^{2}}{(b-1)^{2}-1}\right\rfloor \cdot \square$
To illustrate the applicability of Theorems 2-3 we have conducted an exhaustive computer search. Our first goal was to compare the obtained results with the theoretical bounds (Table 1), while the second goal was finding the coefficients $C_{i}$ (Table 2) for 32-bit codes (these codes are perfectly suited for implementation on modern 32/64-bit processors [11]).

Table 1. Number of Coefficients for Some Integer SBEC Codes.

|  | $b=8$ | $b=9$ | $b=10$ | $b=11$ | $b=12$ | $b=13$ | $b=14$ | $b=15$ | $b=16$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| Theoretical bound | 1 | 3 | 5 | 9 | 16 | 27 | 47 | 83 | 145 |
| Computer-search result | 0 | 1 | 1 | 3 | 6 | 10 | 16 | 27 | 43 |

Table 2. First 128 Coefficients in [2, $\left.2^{32}-2\right]$ for 32-bit Integer SBEC Codes.

| 19 | 23 | 25 | 27 | 29 | 37 | 39 | 41 | 47 | 49 | 53 | 59 | 61 | 67 | 71 | 77 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 79 | 83 | 89 | 97 | 101 | 103 | 107 | 109 | 113 | 121 | 131 | 137 | 139 | 149 | 151 | 157 |
| 163 | 167 | 173 | 179 | 181 | 191 | 193 | 197 | 199 | 211 | 223 | 227 | 229 | 233 | 239 | 251 |
| 263 | 269 | 271 | 277 | 281 | 283 | 289 | 293 | 307 | 311 | 313 | 317 | 331 | 337 | 347 | 349 |
| 353 | 357 | 359 | 361 | 365 | 367 | 373 | 379 | 383 | 389 | 397 | 401 | 409 | 419 | 421 | 431 |
| 433 | 437 | 439 | 443 | 449 | 457 | 461 | 463 | 465 | 467 | 475 | 479 | 487 | 491 | 499 | 503 |
| 521 | 523 | 529 | 541 | 547 | 551 | 557 | 563 | 569 | 571 | 575 | 577 | 587 | 593 | 599 | 601 |
| 607 | 613 | 617 | 619 | 621 | 625 | 631 | 641 | 643 | 647 | 653 | 659 | 661 | 667 | 673 | 675 |

## 3. Error Control Procedure and Theoretical Decoding Throughputs

The error control procedure for the proposed codes is similar to that described in [12]-[18]. In short, it consists of two steps: obtaining the error correction data from the syndrome table and executing the operation

$$
\begin{equation*}
B_{i}=\underline{B}_{i}-e\left(\bmod 2^{b}-1\right) \tag{7}
\end{equation*}
$$

where $1 \leq i \leq k+1, e= \pm 2^{r} \pm 2^{s}$ and $0 \leq r<s \leq b-1$. To generate the syndome table it is necessary to substitute the values of $b$ and $C_{i}$ (Table 2) into (5). In this way, exactly $|\xi|$ (Theorem 2) relationships between the syndrome (element of the set $\xi$ ), error location (i) and error vector (e) are established (Fig. 1). Accordingly, when $S \neq 0$, the decoder's task is to find the entry with the first $b$ bits as that of the syndrome $S$. If the elements of $\xi$ are sorted in increasing order, this task will be completed after $n_{\mathrm{TL}}$ table lookups, where $1 \leq n_{\mathrm{TL}} \leq\left\lfloor\log _{2}|\xi|\right\rfloor+2$ [19].


Fig. 1. Bit-width of one syndrome table entry.
To illustrate the effectiveness of the above approach, suppose that the data packet has $K=$ $6 \cdot b \cdot k=192 \cdot k$ data bits $(k=32,64,96$ and 128$)$ and that each network node is equipped with the six-core processor (Fig. 2) having the following parameters [20]:

1) clock rate: $C_{R}=3.3 \cdot 10^{9} \mathrm{~Hz}$,
2) integer addition/subtraction latency: 1 cycle,
3) integer multiplication latency: 3 cycles,
4) modulo reduction operation: 1 cycle latency,
5) 32-bit comparison operation: 1 cycle latency,
6) 128-bit shift operation latency: 1 cycle,
7) L1 cache ( 32 KB per core) access latency: 4 cycles,
8) L2 cache ( 256 KB per core) access latency: 12 cycles,
9) L3 cache ( 15 MB shared) access latency: 34 cycles.


Fig. 2. Block diagram of a six-core processor.
In addition, let us assume that the coefficients $C_{i}$ (Table 2) are stored in each of the six L1 caches and that the syndrome table is placed into the L3 cache (Fig. 2). In that case, instead of one, the decoder (processor) will (in parallel) compute the values of six syndromes:

- Core 1

$$
\begin{equation*}
S_{1}=\sum_{i=1}^{k}\left(C_{i} \cdot \underline{B}_{6 \cdot(i-1)+1}-\underline{B}_{6 \cdot k+1}\right)\left(\bmod 2^{32}-1\right) \tag{8}
\end{equation*}
$$

- Core 2

$$
\begin{equation*}
S_{2}=\sum_{i=1}^{k}\left(C_{i} \cdot \underline{B}_{6 \cdot(i-1)+2}-\underline{B}_{6 \cdot k+2}\right)\left(\bmod 2^{32}-1\right) \tag{9}
\end{equation*}
$$

- Core 6

$$
\begin{equation*}
S_{6}=\sum_{i=1}^{k}\left(C_{i} \cdot \underline{B}_{6 \cdot(i-1)+6}-\underline{B}_{6 \cdot k+6}\right)\left(\bmod 2^{32}-1\right) \tag{10}
\end{equation*}
$$

If we add to this $K / 128=1.5 \cdot k$ shift operations, we see that each core requires $\mathrm{T}_{1}=9.5 \cdot k+1$ clock cycles ( $k$ accesses to the L1 cache, $k$ integer multiplications, $k-1$ integer additions, $1.5 \cdot k$ shift operations, 1 integer subtraction and 1 modulo reduction) to calculate the values of all syndromes. If one or more syndromes are non-zero, the decoder will additionally perform $n_{\text {TL }}$ table lookups, $n_{\mathrm{TL}}$ comparisons, 1 integer addition and 1 modulo reduction. In our case, six such operations can be executed in parallel in $\mathrm{T}_{2}=35 \cdot n_{\mathrm{TL}}+2$ clock cycles. So, if we sum up both processing times, we come to the conclusion that the decoder requires

$$
\begin{equation*}
\mathrm{T}_{\text {total }}=\mathrm{T}_{1}+\mathrm{T}_{2}=9.5 \cdot k+35 \cdot n_{\mathrm{TL}}+3 \tag{11}
\end{equation*}
$$

clock cycles to process $K$ data bits, i.e. one second to decode

$$
\begin{equation*}
G=\frac{C_{\mathrm{R}}}{\mathrm{~T}_{\text {total }} / K}=\frac{\left(3.3 \cdot 10^{9}\right) \cdot K}{9.5 \cdot k+35 \cdot n_{\mathrm{TL}}+3}=\frac{\left(3.3 \cdot 10^{9}\right) \cdot 192 \cdot k}{9.5 \cdot k+35 \cdot n_{\mathrm{TL}}+3} \tag{12}
\end{equation*}
$$

data bits. From (12) it is easy to calculate that the theoretical throughput of the decoder varies between 22.48 Gbps and 43.05 Gbps (Table 3). This means that all codes from Table 3 have the potential to be used in 10G networks (e.g. 10G SONET and HDLC network) [1]. Besides this, from Table 3 we see that the code with the code rate 4096/4128 has theoretical throughput above 40 Gbps. This fact makes it a good candidate for use in 40G networks (e.g. 40G SONET) [1]. Finally, from (8)-(10) we see that the analyzed codes are interleaved at the byte level. Thanks to this, they are able both to protect up to 24576 bits and to correct SB errors spanning up to 192 bits. Such solution is not only more reliable than [6]-[10], but also much simpler to implement (Table 4).

Table 3. Memory requirements and theoretical decoding throughputs for some six-byte interleaved integer SBEC codes.

| Code | $k$ | Memory <br> requirements <br> for storing the <br> coefficients $C_{i}$ | Memory <br> requirements <br> for storing the <br> syndrome table | Number <br> of table <br> lookups | Minimum <br> theoretical <br> decoding <br> throughput |
| :---: | :---: | :---: | :---: | :---: | :---: |
| $(1056,1024)$ | 32 | $6 \times 128 \mathrm{~B}$ | 0.55 MB | $1 \leq n_{\mathrm{TL}} \leq 17$ | 22.48 Gbps |
| $(2080,2048)$ | 64 | $6 \times 256 \mathrm{~B}$ | 1.11 MB | $1 \leq n_{\mathrm{TL}} \leq 18$ | 32.68 Gbps |
| $(3104,3072)$ | 96 | $6 \times 384 \mathrm{~B}$ | 1.65 MB | $1 \leq n_{\mathrm{TL}} \leq 19$ | 38.50 Gbps |
| $(4128,4096)$ | 128 | $6 \times 512 \mathrm{~B}$ | 2.23 MB | $1 \leq n_{\mathrm{TL}} \leq 19$ | 43.05 Gpbs |

Table 4. Comparison of codes used or proposed for use in modern PONs.

| Main <br> characteristics | CRC codes | Modified CRC Codes <br> [6]-[10] | Proposed codes <br> (interleaved version) |
| :---: | :---: | :---: | :---: |
| Error control <br> capabilities | Detection of single, double, <br> triple and burst errors of <br> lenght up to 16 bits | Correction of single and <br> duplicate errors, and detection <br> of double and triple errors | Correction of SB errors <br> affecting several <br> consecutive $b$-bit bytes |
| Equal error <br> protection | No <br> (packet header only) | No <br> (packet header only) | Yes |
| Processing <br> of data bits | Modulo-2 operations | Modulo-2 operations | Integer and lookup table <br> operations |
| Type of <br> implementation | Hardware | Hardware | Software |
| Universal <br> application | Yes <br> (any PON) | Nes <br> (specific PON) |  |

## 4. Conclusion

In this paper, we presented a new class of integer error control codes. We have shown that these codes have three characteristics: first, they can correct sparse byte errors, second, they operate under integer arithmetic, and third, they can be interleaved without delay and without using additional hardware. Thanks to these features, the presented codes are well suited to be used in practice, especially in optical networks such as SONET and HDLC.

## References

[1] R. Ramaswani, K. Sivarajan and G. Sasaki, Optical Networks: A Practical Perspective, 3rd ed., Elsevier, Inc., 2010.
[2] CCITT Study Group XVIII Contribution D21, "Observations of Error Characteristics of Fiber Optic Transmission Systems," Jan. 1989.
[3] W. Grover and D. Moore, "Design and Characterization of an Error-Correcting Code for the SONET STS-1 Tributary," IEEE Trans. Commun., vol. 38, pp. 467-476, Apr. 1990.
[4] W. Grover, "Effect of Error Correcting Code Using D-S3 Framing Bits on Measured Dribble Error Pattern of $565 \mathrm{Mb} / \mathrm{s}$ Fibre Optic Transmission System", Elect. Lett., vol. 28, no. 20, pp. 1869-1870, Sept. 1992.
[5] M. Cheung, W. Grover and W. Krzymien, "Combined Framing and Error Correction Coding for DS3 Signal Format," IEEE Trans. Commun., vol. 43, nos. 2-4, pp. 1365-1374, Feb-Apr. 1995.
[6] N. Figueira, "Networking Device and Method for Making Cyclic Redundancy Check (CRC) Immune to Scrambler Error Duplication," U.S. Patent 6,609,226, Aug. 19, 2003.
[7] S. Gorshe, "Cyclic Redundancy Check Circuit for Use with Self-Synchronous Scramblers," U.S. Patent 7,353,446, Nov. 17, 2005.
[8] S. Gorshe, "Analysis of the Interaction Between Linear Cyclic Error Correcting Codes and Self-Synchronous Payload Scramblers", IEEE Trans. Commun., vol. 56, no. 11, pp. 18001806, Nov. 2008.
[9] S. Gorshe, "Forward Error Correction with Self-Synchronous Scramblers," U.S. Patent 7,913,151, Mar. 22, 2011.
[10] D. Ferguson et al., "System, Apparatus, and Method for Increasing Resiliency in Communications," U.S. Patent 7,986,717, Jul. 26, 2011.
[11] R. Giladi, Network Processors: Architecture, Programming, and Implementation, Elsevier, Inc., 2008.
[12] 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.
[13] A. Radonjic et al.,"Integer Codes Correcting Double Asymmetric Errors," IET Commun., vol. 10, no. 14, pp. 1691-1696, Sep. 2016.
[14] A. Radonjic and V. Vujicic, "Integer Codes Correcting Spotty Byte Asymmetric Errors," IEEE Commun. Lett., vol. 20, no. 12, pp. 2338-2341, Dec. 2016.
[15] A. Radonjic and V. Vujicic, "Integer Codes Correcting High-Density Byte Asymmetric Errors," IEEE Commun. Lett., vol. 21, no. 4, pp. 694-697, Apr. 2017.
[16] A. Radonjic and V. Vujicic, "Integer Codes Correcting Single Errors and Burst Asymmetric Errors within a Byte," Inform. Process. Lett., vol. 121, pp. 45-50, May 2017.
[17] A. Radonjic, "(Perfect) Integer Codes Correcting Single Errors," IEEE Commun. Lett., vol. 22, no. 1, pp. 17-20, Jan. 2018.
[18] A. Radonjic and V. Vujicic, "Integer Codes Correcting Burst and Random Asymmetric Errors within a Byte," J. Franklin Inst., vol. 355, no. 2, pp. 981-996, Jan. 2018.
[19] K. Mehlhorn and P. Sanders, Algorithms and Data Structures: The Basic Toolbox, Springer, 2008.
[20] A. Fog, "The Microarchitecture of Intel, AMD and VIA CPUs," Tech. Univ. Denmark, Denmark, Jan. 2016.

