ISIT'2013 1569719053

On L_1 metric Asymmetric/Unidirectional error control codes, constrained weight codes and σ-codes

Luca G. Tallini* and Bella Bose†
*Dip. di Scienze della Comunicazione, Università degli Studi di Teramo, Teramo, Italy.
Email: ltallini@unite.it
†School of EECS, Oregon State University, Corvallis, OR, USA.
Email: bose@eecs.orst.edu

***Abstract*—The general theory on partially asymmetric (t_-,t_+)-EC/(d_-,d_+)-ED m-ary codes for the L_1 distance is developed. In this metric, such codes are capable of correcting t_- or less negative errors, detecting d_- or less negative errors, correcting t_+ or less positive errors, and simultaneously detecting d_+ or less positive errors. Based on the elementary symmetric function, a wide class of these codes with efficient decoding algorithms are given. Let $\mathcal{S}(m,n,w,D)$ be the set of all the m-ary words of length n with real sum of their components being equal to $w \mod D$. Any subset of $\mathcal{S}(m,n,w,D)$ is called m-ary constrained weight (CW) code of length n and is known to be a $(D-1)$-UED code. Given a field, K, of prime characteristic p, some m-ary CW codes of length $n \leq |K|-1$ are defined. Such codes are (t_-,t_+)-EC/(d_-,d_+)-ED and have a redundancy of $\rho(\mathcal{C}) = n - \log_m|\mathcal{C}| \leq \rho(\mathcal{S}(m,n,w,d+1)) + t\log_m|K|$, with $t = \min\{t_- + d_+, d_- + t_+\}$, $d = \max\{t_- + d_+, d_- + t_+\}$ and $w \in \mathbb{N}$. In particular, for $t \leq p-1$, a class of essentially linear and systematic (hence, easy to encode) m-ary (t_-,t_+)-EC/(d_-,d_+)-ED CW σ-codes with length $n \leq |K| + \lceil d/(m-1)\rceil - 1$, $k \leq |K| - t\log_m|K| - 1$ information digits and $n-k = t\log_m|K| + \lceil d/(m-1)\rceil$ check digits are given. Also, some new hybrid partially asymmetric/unidirectional/symmetric error control codes are given and shown to be equivalent to the partially asymmetric (t_-,t_+)-EC/(d_-,d_+)-ED m-ary codes.**

***Index Terms*—m-ary alphabet, error control codes, symmetric errors, unidirectional errors, asymmetric errors, flash memories, insertion and deletion errors, repetition errors, L_1 distance.**

I. Introduction

Let $\mathbb{Z}_m \stackrel{\text{def}}{=} \{0,1,\ldots,(m-1)\}$ be the m-ary alphabet, $m = 2,3,\ldots,+\infty$; where we let $\mathbb{Z}_{+\infty} \stackrel{\text{def}}{=} \mathbb{N} = \{0,1,2,\ldots\}$. The L_1 distance between two m-ary words of length $n \in \mathbb{N}$, $X = x_1x_2\ldots x_n \in \mathbb{Z}_m^n$ and $Y = y_1y_2\ldots y_n \in \mathbb{Z}_m^n$, is equal to

$$d_{L_1}(X,Y) \stackrel{\text{def}}{=} \sum_{i=1}^{n} |x_i - y_i| \qquad (1)$$

where X and Y are regarded as n component vectors over the real field $\mathbb{R}$, and $|d|$ indicates the absolute value of $d \in \mathbb{R}$. For example, if $m=5$, $n=6$, $X=012314$ and $Y=443101$ then $d_{L_1}(X,Y) = |0-4| + |1-4| + |2-3| + |3-1| + |1-0| + |4-1| = 4+3+1+2+1+3 = 14$. Error control (EC) codes for the L_1 metric are fundamental whenever the transmission channel is characterized by an error probability of $Pr(\text{symbol } y \text{ is received} \mid \text{symbol } x \text{ is sent}) \simeq c_{x,y} \cdot \epsilon^{|x-y|}$, for all $x,y \in \{0,1,\ldots,m-1\} \subseteq \mathbb{R}$ and $x \neq y$, where the $c_{x,y} \in \mathbb{N}$ and $\epsilon \in [0,1] \subseteq \mathbb{R}^+$ is a small constant. Note that such channel can model any physical channel with a (partial) asymmetric and/or symmetric behavior whose error probability is exponential in the real distance between the sent and received symbol. For example, if $m=3$, $c_{0,1} = c_{0,2} = c_{1,2} = 1$ and $c_{1,0} = c_{2,0} = c_{2,1} = 2$ the model represents a partially asymmetric channel where the probability of positive symbol errors are double than the probability of negative symbol errors with the same magnitude. Note that, if we allow $c_{x,y} : \Omega \rightarrow \mathbb{N}$ to be natural random variables, for all $x,y \in \{0,1,\ldots,m-1\} \subseteq \mathbb{R}$ and $x \neq y$, then the above model captures the model of (partial) unidirectional channel [1], [14], [3], [13], [4]. Practical examples of physical channel modeled as above are the multi-level flash memories [2], [9], [10] and the repetition channels [11]. In Section II, based on a Theorem in [9], the general theory on partially asymmetric (t_-,t_+)-EC/(d_-,d_+)-ED m-ary codes for the L_1 distance is developed and a general (t_-,t_+)-EC/(d_-,d_+)-ED decoding algorithm is given. In Section III, it is shown how to combine some (t_-,t_+)-EC/(d_-,d_+)-ED algorithms to get some new hybrid partially asymmetric/unidirectional/symmetric error control algorithms. In Section IV the CW codes are introduced as a good solution to the (t_-,t_+)-EC/(d_-,d_+)-ED decoding problem. In Section V, efficient design of CW codes are given based on the σ-codes introduced in [12], [9], [10], [7], [8] and [6].

Let us recall some useful notation from [9]. If $X = x_1\ldots x_n \in \mathbb{Z}_m^n$ is any word of length n over the m-ary alphabet $\mathbb{Z}_m$ then let $supp(X) \stackrel{\text{def}}{=} supp_I(X)$ indicate a subset of the index set $I \stackrel{\text{def}}{=} [1,n] \stackrel{\text{def}}{=} \{1,2\ldots,n\}$ where every element $i \in [1,n]$ is counted with its multiplicity, $m_X(i) = x_i \in \mathbb{Z}_m \subseteq \mathbb{N}$, given by the i-th component of X. Namely, $X \equiv supp(X)$ is a multiset on $[1,n]$, and we simply let the weight of X to be $w(X) = |X| = |supp(X)| = \sum_{i\in[1,n]} x_i = \sum_{i\in[1,n]} m_X(i)$. For example, if $m=3$, $n=4$ and $X = 2012 \in \mathbb{Z}_3^4$ then $x_1 = m_X(1) = 2$, $x_2 = m_X(2) = 0$, $x_3 = m_X(3) = 1$, $x_4 = m_X(4) = 2$, $supp(X) = \{1,1,3,4,4\}$ and the weight of X is $w(X) = |supp(X)| = \sum_{i\in[1,n]} m_X(i) = 5$. Let $\partial X \stackrel{\text{def}}{=} \partial_I X \stackrel{\text{def}}{=} \{i \in I = [1,n] : \ x_i = m_X(i) \neq 0\} \in \mathbb{Z}_2^n$ be the set of indices where X is different from 0 and note that ∂X can be regarded as a **proper** subset of $[1,n]$. We refer to ∂X as the **index set** of X. Given $c \in \mathbb{N}$, let $c \cdot X = cx_1\, cx_2 \ldots cx_n \in \mathbb{Z}_{c(m-1)+1}^n \subseteq \mathbb{N}^n$. For example, if $X = 2012 \in \mathbb{Z}_3^4 \subseteq \mathbb{N}^4$ then $3 \cdot X = 6036 \in \mathbb{Z}_7^4 \subseteq \mathbb{N}^4$. Define the total order in $\mathbb{Z}_m$ as $0 \leq 1 \leq 2 \leq \ldots \leq (m-1)$ and, for all $x,y \in \mathbb{Z}_m$, let the minimum (maximum) operation $\min(x,y)$ $(\max(x,y))$ be defined as the minimum (maximum) between x and y, let the natural subtraction operation in $\mathbb{Z}_m$ be defined as $x \dot{-} y \stackrel{\text{def}}{=} \max\{0, x-y\}$, where "$-$" indicates the usual integer subtraction. Then given any two words/multisets $X,Y \in \mathbb{Z}_m^n$, the words/multiset operations $X \cap Y \in \mathbb{Z}_m^n$, $X \cup Y \in \mathbb{Z}_m^n$, $X + Y \in \mathbb{N}$, and $X \dot{-} Y \in \mathbb{Z}_m^n$ are defined as the digit by digit $\min$, $\max$, integer addition and $\dot{-}$ operation between X and Y, respectively. For example, if $m=3$, $n=8$, $X = 012012012$ and $Y = 000111222$ then $X \cap Y = 000011012$, $X \cup Y = 012112222$, $X + Y = 012123234$, $X \dot{-} Y = 012001000$ and $Y \dot{-} X = 000100210$. Given any

two word $X, Y \in \mathbb{Z}_m^n$, we say that X is contained in Y and write $X \subseteq Y$ iff $X = X \cap Y$. For example, $000011012 \equiv \{5,6,8,9,9\} \subseteq \{2,3,3,5,6,6,8,9,9\} \equiv 012012012$. Under this multiset interpretation, we give

Definition 1: Given $X, Y \in \mathbb{Z}_m^n$, let

$$\begin{aligned} d_S(X,Y) &\stackrel{\text{def}}{=} |Y \dot{-} X| + |X \dot{-} Y|, \\ d_A(X,Y) &\stackrel{\text{def}}{=} \max\{|Y \dot{-} X|, |X \dot{-} Y|\}, \\ \Delta(X,Y) &\stackrel{\text{def}}{=} |Y \dot{-} X| - |X \dot{-} Y|, \\ \delta(X,Y) &\stackrel{\text{def}}{=} \min\{|Y \dot{-} X|, |X \dot{-} Y|\} \end{aligned}$$

Note that d_S is nothing but the L_1 distance as defined in (1). So, we refer d_S and d_A as the symmetric and asymmetric L_1 distances, respectively. For example, if $X = 012012012 \equiv \{2,3,3,5,6,\ 6,8,9,9\}$ and $Y = 000111221 \equiv \{4,5,6,7,7,8,8,9\}$ then $X \dot{-} Y = 012001001 \equiv \{2,3,3,\ 6,9\}$, $Y \dot{-} X = 000100210 \equiv \{4,7,7,8\}$, $d_{L_1}(X,Y) = d_S(X,Y) = 9$, $d_A(X,Y) = 5$, $\Delta(X,Y) = 1$ and $\delta(X,Y) = 4$. In the above definitions there is nothing special in choosing $I = [1,n]$ as the index set. In fact, any other set can be chosen. For $n, w \in \mathbb{N}$, $m, d \in \mathbb{N} \cup \{+\infty\}$ let $\mathcal{S}(m,n,w,d) \stackrel{\text{def}}{=} \{X \in \mathbb{Z}_m^n : |X| = w \bmod d\}$ where we let $x \bmod +\infty = x$, for all $x \in \mathbb{N}$.

The asymmetric/unidirectional/symmetric error model for the L_1 metric is captured by the following definition.

Definition 2: Given $X, Y \in \mathbb{Z}_m^n$, we say that

D1) Y is obtained from X due to $t_- \in \mathbb{N}$ negative errors and $t_+ \in \mathbb{N}$ positive errors iff $|X \dot{-} Y| = t_-$ and $|Y \dot{-} X| = t_+$;

D2) Y is obtained from X due to $t \in \mathbb{N}$ (totally) asymmetric errors iff $|X \dot{-} Y| = t$ and $|Y \dot{-} X| = 0$ (if instead, $|\Delta(X,Y)| \geq 0$ is big compared to $|Y \dot{-} X| > 0$ we say that Y is obtained from X due to partially asymmetric errors);

D3) Y is obtained from X due to $t \in \mathbb{N}$ (totally) unidirectional errors iff $d_A(X,Y) = t$ and $\delta(X,Y) = 0$ (if instead, $|\Delta(X,Y)| = d_A(X,Y) - \delta(X,Y) \geq 0$ is big compared to $\delta(X,Y) > 0$ we say that Y is obtained from X due to partially unidirectional errors);

D4) Y is obtained from X due to $t \in \mathbb{N}$ symmetric errors iff $d_S(X,Y) = t$.

For example, if $m = 4$, $n = 3$, $X = 0123$, $Y = 2210$ and $Z = 0012$ then Y is obtained from X due to $|X \dot{-} Y| = t_- = 4$ negative errors and $|Y \dot{-} X| = t_+ = 3$ positive errors, Y is not obtained from X due to asymmetric or unidirectional errors because $\delta(X,Y) > 0$, Y (or Z) is obtained from X due to $t = t_- + t_+ = 4+3 = 7$ (or $t = 3$, respectively) symmetric errors, Z is obtained from X due to $t_- = 3$ asymmetric errors, Y is not obtained from Z due to asymmetric errors, and X (or Z) is obtained from Z (or X respectively) due to $t = 3$ unidirectional errors.

II. General (t_-, t_+)-EC/(d_-, d_+)-ED algorithms

First we give the following definition.

Definition 3 (of (t_-,t_+)-EC/(d_-,d_+)-ED codes): A code $\mathcal{C} \subseteq \mathbb{Z}_m^n$, $m, n \in \mathbb{N}$, is capable of correcting t_+ or less positive errors, detecting d_+ or less positive errors, correcting t_- or less negative errors, and simultaneously detecting d_- or less negative errors (i. e., $\mathcal{C}$ is a (t_-,t_+)-EC/(d_-,d_+)-ED code), with $t_-, t_+, d_-, d_+ \in \mathbb{N}$, $t_- \leq d_-$ and $t_+ \leq d_+$, iff there exists an algorithm, say $\mathcal{D}ec(\mathcal{C}, t_-, t_+, d_-, d_+)$, which, for all sent codeword $X \in \mathcal{C}$, takes the corresponding received word $Y \in \mathbb{Z}_m^n$ as the input and gives a word $X' \in \mathbb{Z}_m^n$ as the output with a correct signal $cor \in \{0,1\}$ such that

C1) if $|X \dot{-} Y| \leq d_-$, $|Y \dot{-} X| \leq d_+$ and $cor = 1$ then $X' = X \in \mathcal{C}$; and

C2) if $|X \dot{-} Y| \leq t_-$ ($\leq d_-$) and $|Y \dot{-} X| \leq t_+$ ($\leq d_+$) then $cor = 1$ (meaning that the errors are corrected).

We call any $\mathcal{D}ec(\mathcal{C}, t_-, t_+, d_-, d_+)$ satisfying the above properties a (well defined) decoding algorithm (for $\mathcal{C}$).

Now, assume $|X \dot{-} Y| \leq d_-$, $|Y \dot{-} X| \leq d_+$. In this case, note that if $|X \dot{-} Y| \leq t_-$ and $|Y \dot{-} X| \leq t_+$ then $cor = 1$ because of C2), and so, the errors in Y are corrected (and hence, detected) because of C1). Furthermore, from C2), if $cor = 0$ then either $|X \dot{-} Y| > t_-$ or $|Y \dot{-} X| > t_+$ and so errors have occurred during the transmission (and hence again, detected). Note that, if $cor = 0$ then either $X' \neq X$ or $X' = X \in \mathcal{C}$ (that is, errors may not or may have been corrected, respectively). Note that the above definition is equivalent to the usual definition given in terms of spheres. Note also that when $d_- = t_-$ and $d_+ = t_+$, if $|X' \dot{-} Y| \leq t_-$ and $|Y \dot{-} X'| \leq t_+$ then $cor = 1$ and so $X' = X \in \mathcal{C}$. And this is a good definition of $\mathcal{C}$ being a (t_-,t_+)-EC code.

The following combinatorial characterization holds.

Theorem 1: A code $\mathcal{C} \subseteq \mathbb{Z}_m^n$ is a (t_-,t_+)-EC/(d_-,d_+)-ED code iff for all distinct $X, Y \in \mathcal{C}$,

$$\begin{cases} \text{either } d_A(X,Y) > \max\{t_- + d_+, d_- + t_+\} \\ \text{or } \quad \delta(X,Y) > \min\{t_- + d_+, d_- + t_+\}. \end{cases} \tag{2}$$

Proof: The proof is given in [9]. We only note here that there is a typo in the proof where in the right column lines 20 and 26, "$\min\{0$," should be replaced with "$\max\{0$,". ■

Note that, Theorem 1 for $d_+ = t_+ + e$ and $d_- = t_- + e$ gives

Theorem 2: Given $t_+, t_-, e \in \mathbb{N}$, a code $\mathcal{C} \subseteq \mathbb{Z}_m^n$ is a (t_+,t_-)-EC/$(t_+ + e, t_- + e)$-ED code iff $d_A(\mathcal{C}) > t_+ + t_- + e$.

An efficient decoding algorithm was given in [9] for a wide class of Goppa like codes (the σ-codes) satisfying the hypothesis of Theorem 2.

In this section, we efficiently reduce the problem of designing (t_-,t_+)-EC/(d_-,d_+)-ED decoding algorithms for a code to the design problem of (τ_-,τ_+)-EC decoding algorithms for the same code. To this aim, let $\mathcal{C}$ be a code satisfying (2) and let $\mathcal{D}ec(\mathcal{C}, \tau_-, \tau_+)$ be an efficient (τ_-,τ_+)-EC algorithm for $\mathcal{C}$, where $\tau_-, \tau_+ \in \mathbb{N}$ and $d_A(\mathcal{C}) > \tau_- + \tau_+$. Then, the following is an efficient (t_+,t_-)-EC/(d_+,d_-)-ED algorithm for $\mathcal{C}$; where $t_-, t_+, d_-, d_+ \in \mathbb{N}$, $t_- \leq d_-$, and $t_+ \leq d_+$.

Algorithm 1 (general (t_-,t_+)-EC/(d_-,d_+)-ED decoding):

Input: The received word $Y \in \mathbb{Z}_m^n$.

Output: A word $X' \in \mathbb{Z}_m^n$ and a signal $cor \in \{0,1\}$.

Assume that the combinatorial property (2) holds for $\mathcal{C}$ and let $d \stackrel{\text{def}}{=} \max\{t_- + d_+, d_- + t_+\} \geq \min\{t_- + d_+, d_- + t_+\} \stackrel{\text{def}}{=} t$. So, from (2), if $X, Y \in \mathcal{C}$ and $X \neq Y$ then either $d_A(X,Y) > d \geq t$ or $d_A(X,Y) \geq \delta(X,Y) > t$ Hence, (2) implies $d_A(\mathcal{C}) > t \geq t_- + t_+$.

Assume $X \in \mathcal{C}$ is sent, Y is received and

$$|X \dot{-} Y| \leq d_- \text{ and } |Y \dot{-} X| \leq d_+. \tag{3}$$

Execute the following steps.

S1: Execute algorithm $\mathcal{D}ec(\mathcal{C}, \tau_- = t - t_+, \tau_+ = t_+)$ and let X' be its output. Note that $d_A(\mathcal{C}) > t \geq t_- + t_+$ and so $\mathcal{D}ec(\mathcal{C}, \tau_-, \tau_+)$ is a (τ_-,τ_+)-EC algorithm for $\mathcal{C}$. Now, there can be two cases: either $X' \notin \mathcal{C}$ or $X' \in \mathcal{C}$. So,

S2: If $X' \notin \mathcal{C}$ then set $cor = 0$, output X', output cor and exit.

S3: (If $X' \in \mathcal{C}$, and) if

$$|X' \dot{-} Y| \leq t_- \text{ and } |Y \dot{-} X'| \leq t_+ \tag{4}$$

then set $cor = 1$, output X', output cor and exit. Note that if $X' \in \mathcal{C}$ and $X \in \mathcal{C}$ is sent then

$$|X' \dot{-} X| \leq |X' \dot{-} Y| + |Y \dot{-} X| \leq t_- + d_+ \text{ and}$$
$$|X \dot{-} X'| \leq |X \dot{-} Y| + |Y \dot{-} X'| \leq d_- + t_+$$

because of (3) and (4). So, in this case, $X, X' \in \mathcal{C}$,

$$\delta(X, X') = \min\{|X' \dot{-} X|, |X \dot{-} X'|\} \leq \min\{t_- + d_+, d_- + t_+\} \text{ and}$$
$$d_A(X, X') = \max\{|X' \dot{-} X|, |X \dot{-} X'|\} \leq \max\{t_- + d_+, d_- + t_+\}.$$

Hence, $X' = X \in \mathcal{C}$ because (2) holds for $\mathcal{C}$.

S4: Otherwise, if ($X' \in \mathcal{C}$ and) (4) does not hold, then set $cor = 0$, output X', output cor and exit.

The above Algorithm 1 is indeed a well defined (t_-, t_+)-EC/(d_-, d_+)-ED error control algorithm for $\mathcal{C}$ according to Definition 3. In fact, first note that Algorithm 1 sets $cor = 1$ iff $X' \in \mathcal{C}$ and (4) holds (that is, whenever the algorithm terminates in step S3). So, condition C1) of Definition 3 holds because if (3) holds and $cor = 1$ then (3), $X' \in \mathcal{C}$, (4) and $X \in \mathcal{C}$ hold; and, we already have shown above that $X' = X \in \mathcal{C}$. Condition C2) of Definition 3 holds as well because if $|X \dot{-} Y| \leq t_-$ ($\leq t - t_+$) and $|Y \dot{-} X| \leq t_+$ then $|X \dot{-} Y| \leq t - t_+$ and $|Y \dot{-} X| \leq t_+$, and so, $X' = X \in \mathcal{C}$ (because X' is the output from the $(t - t_+, t_+)$-EC algorithm $\mathcal{D}ec(\mathcal{C}, t - t_+, t_+)$ for $\mathcal{C}$). This implies $X' \in \mathcal{C}$, $|X' \dot{-} Y| = |X \dot{-} Y| \leq t_-$ and $|Y \dot{-} X'| = |Y \dot{-} X| \leq t_+$; and, in this case, Algorithm 1 sets $cor = 1$.

Note that Algorithm 1 in [9] is a (t_-, t_+)-EC/$(t_- + e, t_+ + e)$-ED algorithm, $e \in \mathbb{N}$, which is the implementation of Algorithm 1 to the σ-codes $\mathcal{C}_{\sigma,p}$ given in Theorem 5 of [9]. In this case, it can be shown that step S2 of Algorithm 1 is not needed.

III. Hybrid error control codes

Given the general Algorithm 1, hybrid asymmetric/unidirectional/symmetric error control algorithms can be defined in various ways for codes satisfying the combinatorial property (2) of Theorem 1. For simplicity, consider the following.

***Definition** 4 (of $\{t_1, t_2\}$-EC/(d, d)-ED codes):* A code $\mathcal{C} \subseteq \mathbb{Z}_m^n$, $m, n \in \mathbb{N}$, is capable of being **simultaneously** (t_1, t_2)-EC/(d, d)-ED and (t_2, t_1)-EC/(d, d)-ED (i. e., $\mathcal{C}$ is a $\{t_1, t_2\}$-EC/(d, d)-ED code – please, note the curly braces to indicate the unordered pair $\{t_1, t_2\}$), with $t_1, t_2, d \in \mathbb{N}$, $t_1, t_2 \leq d$, iff there exists an algorithm, say $\mathcal{D}ec(\mathcal{C}, t_1, t_2, d)$, which, for all sent codeword $X \in \mathcal{C}$, takes the corresponding received word $Y \in \mathbb{Z}_m^n$ as the input and gives a word $X' \in \mathbb{Z}_m^n$ as the output with a correct signal $cor \in \{0, 1\}$ such that

C1) if $d_A(X, Y) \leq d$ and $cor = 1$ then $X' = X \in \mathcal{C}$; and
C2) if $|X \dot{-} Y| \leq t_1$ ($\leq d$) and $|Y \dot{-} X| \leq t_2$ ($\leq d$) then $cor = 1$ (meaning that the errors are corrected); and
C3) if $|Y \dot{-} X| \leq t_1$ and $|X \dot{-} Y| \leq t_2$ then $cor = 1$.

Note that condition C2) and C3) can be replaced with

C2′) if $d_A(X, Y) \leq \max\{t_1, t_2\}$ and $\delta(X, Y) \leq \min\{t_1, t_2\}$ then $cor = 1$ (that is, the errors are corrected).

We call any $\mathcal{D}ec(\mathcal{C}, t_1, t_2, d)$ satisfying the above properties a (well defined) decoding algorithm (for $\mathcal{C}$).

Given a code $\mathcal{C}$ satisfying (2) with $t_- = t_1$, $t_+ = t_2$ and $d_- = d_+ = d$, the following is an efficient $\{t_1, t_2\}$-EC/(d, d)-ED algorithm for $\mathcal{C}$ (and so, $\mathcal{C}$ is a $\{t_1, t_2\}$-EC/(d, d)-ED code).

***Algorithm** 2 (general $\{t_1, t_2\}$-EC/(d, d)-ED decoding):*
Input: The received word $Y \in \mathbb{Z}_m^n$.
Output: A word $X' \in \mathbb{Z}_m^n$ and a signal $cor \in \{0, 1\}$.
Assume $\mathcal{C}$ satisfies (2) for $t_- = t_1$, $t_+ = t_2$ and $d_- = d_+ = d$. This is equivalent to the condition that for all distinct $X, Y \in \mathcal{C}$,

$$\begin{cases} \text{either } d_A(X, Y) > \max\{t_1, t_2\} + d \\ \text{or } \quad \delta(X, Y) > \min\{t_1, t_2\} + d \end{cases} \tag{5}$$

because $\max\{t_1 + d, d + t_2\} = \max\{t_1, t_2\} + d$ and $\min\{t_1 + d, d + t_2\} = \min\{t_1, t_2\} + d$.
Assume $\mathcal{D}ec(\mathcal{C}, t_1, t_2, d, d)$ is an efficient (t_1, t_2)-EC/(d, d)-ED algorithm such as Algorithm 1.
Assume $X \in \mathcal{C}$ is sent, Y is received and

$$d_A(X, Y) \leq d \iff |X \dot{-} Y| \leq d \text{ and } |Y \dot{-} X| \leq d. \tag{6}$$

Execute the following steps.
S1: Execute algorithm $\mathcal{D}ec(\mathcal{C}, t_1, t_2, d, d)$ and let $X_1 \in \mathbb{Z}_m^n$ be its output word and $cor_1 \in \{0, 1\}$ be its output signal.
S2: Execute algorithm $\mathcal{D}ec(\mathcal{C}, t_2, t_1, d, d)$ and let $X_2 \in \mathbb{Z}_m^n$ be its output word and $cor_2 \in \{0, 1\}$ be its output signal.
S3: At this point there can be at most four cases. So,
S3.1: If $cor_1 = 1$ and $cor_2 = 1$ then set $cor = 1$ and $X' = X_1$.
S3.2: If $cor_1 = 1$ and $cor_2 = 0$ then set $cor = 1$ and $X' = X_1$.
S3.3: If $cor_1 = 0$ and $cor_2 = 1$ then set $cor = 1$ and $X' = X_2$.
S3.4: If $cor_1 = 0$ and $cor_2 = 0$ then set $cor = 0$ and $X' = X_1$.
S4: Output X', output cor and exit.

The above Algorithm 2 is indeed a well defined $\{t_1, t_2\}$-EC/(d, d)-ED error control algorithm for $\mathcal{C}$ according to Definition 4. In fact, first note that if (6) holds then both algorithms $\mathcal{D}ec(\mathcal{C}, t_1, t_2, d, d)$ and $\mathcal{D}ec(\mathcal{C}, t_2, t_1, d, d)$ give the correct output; that is, both the algorithms satisfy C1) and C2) of Definition 3 for $\mathcal{C}$ with $d_- = d_+ = d$, $t_- = t_1$, $t_+ = t_2$ and $t_- = t_2$, $t_+ = t_1$, respectively. Also note that Algorithm 2 sets $cor = 1$ iff cor_1 or cor_2 is equal to 1 (that is, whenever the then clause of step S3.1, S3.2 or S3.3 are executed). So, C1) of Definition 4 holds because if (6) holds and $cor = 1$ then at least one of cor_1 or cor_2 is equal to 1 and so, from C1) of Definition 3, at least one of X_1 or X_2 is equal to X. Condition C2) of Definition 4 holds as well because if $|X \dot{-} Y| \leq t_1 \leq d$ and $|Y \dot{-} X| \leq t_2 \leq d$ then $\mathcal{D}ec(\mathcal{C}, t_1, t_2, d, d)$ outputs $cor_1 = 1$ and so, Algorithm 2 sets $cor = 1$ (in step S3.1 or S3.2). Analogously, C3) of Definition 4 holds because if $|X \dot{-} Y| \leq t_2 \leq d$ and $|Y \dot{-} X| \leq t_1 \leq d$ then $\mathcal{D}ec(\mathcal{C}, t_2, t_1, d, d)$ outputs $cor_2 = 1$ and so $cor = 1$ (in step S3.3). A consequence of Algorithm 2 is the following combinatorial characterization of $\{t_1, t_2\}$-EC/(d, d)-ED codes.

***Theorem** 3:* Given $t_1, t_2, d \in \mathbb{N}$, with $t_1, t_2 \leq d$, and $\mathcal{C} \subseteq \mathbb{Z}_m^n$, $m, n \in \mathbb{N}$, the following statements are equivalent.

S1) $\mathcal{C}$ is a (t_1, t_2)-EC/(d, d)-ED code;
S2) $\mathcal{C}$ is a (t_2, t_1)-EC/(d, d)-ED code;
S3) for all distinct $X, Y \in \mathcal{C}$ relation (5) holds;
S4) $\mathcal{C}$ is a $\{t_1, t_2\}$-EC/(d, d)-ED code.

Proof: If $d_- = d_+ = d$ then property (2) of Theorem 1 is symmetric with respect to $t_- = t_1$, $t_+ = t_2$, and equivalent to (5). Hence S1), S2) and S3) are equivalent. If (5) holds then S4) holds because Algorithm 2 is a $\{t_1, t_2\}$-EC/(d, d)-ED decoding algorithm for $\mathcal{C}$. On the other hand, if S4 holds then $\mathcal{C}$ is a $\{t_1, t_2\}$-EC/(d, d)-ED code and so it is a (t_1, t_2)-EC/(d, d)-ED code; that is, S1) holds. ∎

Analogously to Definition 4, another noticeable type of error control codes can be defined as follows.

***Definition** 5 (of (t, t)-EC/$\{d_1, d_2\}$-ED codes):* $\mathcal{C} \subseteq \mathbb{Z}_m^n$, $m, n \in \mathbb{N}$, is a (t, t)-EC/$\{d_1, d_2\}$-ED code (please, note the

curly braces to indicate the unordered pair $\{d_1, d_2\}$), with $t, d_1, d_2 \in \mathbb{N}$, $t \leq d_1, d_2$, iff there exists an algorithm, say $\mathcal{D}ec(\mathcal{C}, t, d_1, d_2)$, which, for all sent codeword $X \in \mathcal{C}$, takes the corresponding received word $Y \in \mathbb{Z}_m^n$ as the input and gives a word $X' \in \mathbb{Z}_m^n$ as the output with a correct signal $cor \in \{0, 1\}$ such that

C1) if $d_A(X,Y) \leq \max\{d_1, d_2\}$, $\delta(X,Y) \leq \min\{d_1, d_2\}$ and $cor = 1$ then $X' = X \in \mathcal{C}$; and
C2) if $d_A(X,Y) \leq t$ ($\leq \min\{d_1, d_2\}$) then $cor = 1$.

In this case, the (t,t)-EC/$\{d_1, d_2\}$-ED error control problem can be reduced to the (t_-, t_+)-EC/(d_-, d_+)-ED error control problem by means of the following algorithm.

***Algorithm** 3 (general (t,t)-EC/$\{d_1, d_2\}$-ED decoding):*
Input: The received word $Y \in \mathbb{Z}_m^n$.
Output: A word $X' \in \mathbb{Z}_m^n$ and a signal $cor \in \{0, 1\}$.
Assume $\mathcal{C}$ satisfies (2) for $t_- = t_+ = t$, $d_- = d_1$ and $d_+ = d_2$. This is equivalent to assume that for all distinct $X, Y \in \mathcal{C}$,

$$\begin{cases} \text{either } d_A(X,Y) > t + \max\{d_1, d_2\} \\ \text{or} \qquad \delta(X,Y) > t + \min\{d_1, d_2\} \end{cases} \tag{7}$$

because $\max\{t + d_2, d_1 + t\} = t + \max\{t_1, t_2\}$ and $\min\{t + d_2, d_1 + t\} = t + \min\{d_1, d_2\}$.
Assume $\mathcal{D}ec(\mathcal{C}, t, t, d_1, d_2)$ is an efficient (t,t)-EC/(d_1, d_2)-ED algorithm such as Algorithm 1.
Assume $X \in \mathcal{C}$ is sent, Y is received, $d_A(X,Y) \leq \max\{d_1, d_2\}$ and $\delta(X,Y) \leq \min\{d_1, d_2\}$.
Execute the following steps.
S1: Execute algorithm $\mathcal{D}ec(\mathcal{C}, t, t, d_1, d_2)$ and let $X_1 \in \mathbb{Z}_m^n$ be its output word and $cor_1 \in \{0, 1\}$ be its output signal.
S2: Execute algorithm $\mathcal{D}ec(\mathcal{C}, t, t, d_2, d_1)$ and let $X_2 \in \mathbb{Z}_m^n$ be its output word and $cor_2 \in \{0, 1\}$ be its output signal.
S3: Set $cor = cor_1$ AND cor_2, set $X' = X_1$, output X', output cor and exit.
As before, Algorithm 3 is a (t,t)-EC/$\{d_1, d_2\}$-ED error control algorithm for $\mathcal{C}$ according to Definition 5. So, the following combinatorial characterization holds.

***Theorem** 4:* Given $t, d_1, d_2 \in \mathbb{N}$, with $t \leq d_1, d_2$, and $\mathcal{C} \subseteq \mathbb{Z}_m^n$, $m, n \in \mathbb{N}$, the following statements are equivalent.

S1) $\mathcal{C}$ is a (t,t)-EC/(d_1, d_2)-ED code;
S2) $\mathcal{C}$ is a (t,t)-EC/(d_2, d_1)-ED code;
S3) for all distinct $X, Y \in \mathcal{C}$ relation (7) holds;
S4) $\mathcal{C}$ is a (t,t)-EC/$\{d_1, d_2\}$-ED code.

IV. Algorithms for constrained weight codes

From Theorem 1, the error control problems considered previously can be tackled with the CW codes in (9) below.

***Theorem** 5:* For $n, \hat{r}, T, w \in \mathbb{N}$, $m, D \in \mathbb{N} \cup \{+\infty\}$ let $\tilde{\mathcal{C}} \subseteq \mathbb{Z}_m^{\tilde{n}}$ be any code with $T \stackrel{\text{def}}{=} d_A(\tilde{\mathcal{C}})$ and $\varphi : \tilde{\mathcal{C}} \to \mathbb{Z}_m^{\hat{r}}$ be any function, $\varphi \stackrel{\text{def}}{=} \varphi(\tilde{\mathcal{C}}, \hat{r}, m, w, D)$, such that

$$|\tilde{X}\varphi(\tilde{X})| = |\tilde{X}| + |\varphi(\tilde{X})| = w \bmod D, \text{ for all } \tilde{X} \in \tilde{\mathcal{C}}. \tag{8}$$

The code $\mathcal{C} \stackrel{\text{def}}{=} \mathcal{C}(\tilde{\mathcal{C}}, \varphi) \subseteq \mathcal{S}(m, n \stackrel{\text{def}}{=} \tilde{n} + \hat{r}, w, D)$ defined as

$$\mathcal{C} \stackrel{\text{def}}{=} \{X : X = \tilde{X}\, C_{\tilde{X}},\ \tilde{X} \in \tilde{\mathcal{C}} \text{ and } C_{\tilde{X}} = \varphi(\tilde{X})\} \tag{9}$$

satisfies the following combinatorial property:

$$\begin{aligned} &\text{for all distinct } X, Y \in \mathcal{C}, \\ &\quad \text{either } d_A(X,Y) \geq D \text{ or } \delta(X,Y) \geq T. \end{aligned} \tag{10}$$

Proof: By construction, $\mathcal{C} \subseteq \mathcal{S}(m, n, w, D)$. So, $|Y| - |X| = 0 \bmod D$ for all $X, Y \in \mathcal{C}$. Now, if $|Y| - |X| = 0$ then

$$\Delta(X,Y) = |Y \dot{-} X| - |X \dot{-} Y| = |Y| - |X| = 0,$$

and so, $|Y \dot{-} X| = |X \dot{-} Y|$. This implies,

$$\begin{aligned} \delta(X,Y) &= \min\{|Y \dot{-} X|, |X \dot{-} Y|\} = \\ &\max\{|Y \dot{-} X|, |X \dot{-} Y|\} = d_A(X,Y) \geq d_A(\mathcal{C}) \geq T. \end{aligned}$$

In this case, (10) is satisfied because $\delta(X,Y) \geq T$. If instead $0 \neq |Y| - |X| = q \cdot D$ with $q \in \mathbb{Z} - \{0\}$ then

$$d_A(X,Y) \geq |\Delta(X,Y)| = ||Y| - |X|| = |q| \cdot D \geq D.$$

In this case, (10) is satisfied because $d_A(X,Y) \geq D$. ∎

From Theorem 1 and Theorem 5 above, the codes $\mathcal{C}$ defined in (9) can be used to perform (t_-, t_+)-EC/(d_-, d_+)-ED provided that the parameters $t_-, t_+, d_-, d_+, D, T \in \mathbb{N}$ are chosen so that (please, see (2)),

$$\begin{aligned} &D > \max\{t_- + d_+, d_- + t_+\} = d \text{ and} \\ &T > \min\{t_- + d_+, d_- + t_+\} = t. \end{aligned} \tag{11}$$

This (t_-, t_+)-EC/(d_-, d_+)-ED error control can be done efficiently with Algorithm 1 if there exists an efficient $(t - t_+, t_+)$-EC error control algorithm for $\mathcal{C}$. This is given below.

***Algorithm** 4 ((τ_-, τ_+)-EC decoding for CW codes (9)):*
Input: A word $Y = \tilde{Y}\, E \in \mathbb{Z}_m^n$, $\tilde{Y} \in \mathbb{Z}_m^{\tilde{n}}$ and $E \in \mathbb{Z}_m^{\hat{r}}$.
Output: A word $X' = \tilde{X}'\, C' \in \mathbb{Z}_m^n$, $\tilde{X}' \in \mathbb{Z}_m^{\tilde{n}}$ and $C' \in \mathbb{Z}_m^{\hat{r}}$.
Assume (11) and $d_A(\tilde{\mathcal{C}}) = T > t = \tau_- + \tau_+$ hold. Let $\mathcal{D}ec(\tilde{\mathcal{C}}, \tau_-, \tau_+)$ be an efficient (τ_-, τ_+)-EC decoding for $\tilde{\mathcal{C}}$. Assume the codeword $X = \tilde{X}\, C_{\tilde{X}} \in \mathcal{C}$ is sent, where $\tilde{X} \in \tilde{\mathcal{C}}$, the word $Y = \tilde{Y}\, E$ is received and

$$|X \dot{-} Y| \leq \tau_- \text{ and } |Y \dot{-} X| \leq \tau_+. \tag{12}$$

Execute the following steps.
S1: Execute algorithm $\mathcal{D}ec(\tilde{\mathcal{C}}, \tau_-, \tau_+)$ with input $\tilde{Y} \in \mathbb{Z}_m^{\tilde{n}}$ and let $\tilde{X}'$ be its output.
S2: If $\tilde{X}' \notin \tilde{\mathcal{C}}$ then output any $X' \in \mathbb{Z}_m^n$ and exit.
S3: Set $C' = C_{\tilde{X}'} = \varphi(\tilde{X}')$, output $X' = \tilde{X}'\, C'$ and exit.
If (12) holds then $|\tilde{X} \dot{-} \tilde{Y}| \leq |X \dot{-} Y| \leq \tau_-$ and $|\tilde{Y} \dot{-} \tilde{X}| \leq |Y \dot{-} X| \leq \tau_+$, and so, $\tilde{X}' = \tilde{X} \in \tilde{\mathcal{C}}$, $C' = \varphi(\tilde{X}') = \varphi(\tilde{X}) = C_{\tilde{X}}$ (because φ is a function which is well defined for all $\tilde{X} \in \tilde{\mathcal{C}}$) and $X' = X$; that is, the algorithm is correct.

So, the general (t_-, t_+)-EC/(d_-, d_+)-ED decoding problem for $\mathcal{C}$ can be reduced efficiently to the (τ_-, τ_+)-EC decoding problem for $\tilde{\mathcal{C}}$ by simply replacing step S1 of Algorithm 1 with Algorithm 4. From this, also the error control problems discussed in Section III can be solved efficiently with the CW codes $\mathcal{C}$ defined in (9).

V. Efficient design of constrained weight σ-codes

In (9), we may choose the σ-codes defined in Theorem 5 of [9] as the code $\tilde{\mathcal{C}}$. They are defined as follows. Let K be **any** field and $S \in \mathbb{Z}_m^n$ be a multiset over K. Let $\partial S = \{a_0, a_1, \ldots, a_{n-1}\} \subseteq K$ be a set of n distinct elements such that $0 \in \partial S \iff a_0 = 0$ and $\sigma_X(z) \stackrel{\text{def}}{=} z^{x_0} \prod_{i=1}^{n-1} (1 - a_i z)^{x_i}$. For all polynomials $g(z) \in K[z]$ such that $\gcd(\sigma, g) = 1$ (for simplicity), the m-ary σ-code of length n and minimum asymmetric distance at least $\deg(g)$ are defined as $\mathcal{C}_{\sigma,g}(n) \stackrel{\text{def}}{=}$

$$\{X \subseteq S\colon \sigma_X(z) = c_X \sigma(z) \bmod g(z) \text{ with } c_X \in K - \{0\}\},$$

for all $\sigma(z) \in K[z]$. When K is a finite field, by the pigeon hole principle, given $\mathcal{T} \subseteq \mathbf{Z}\mathbf{Z}_m^n$ there exists $\sigma(z) \in \Sigma(g) \stackrel{\text{def}}{=} \{\sigma(z) \in K[z] : \sigma \text{ is monic, } \deg(\sigma) < \deg(g) \text{ and } \gcd(\sigma, g) = 1\}$ such that $|\mathcal{T} \cap \mathcal{C}_{\sigma,g}(n)| \geq |\{X \in \mathcal{T} : X \subseteq S\}|/|\Sigma(g)|$. So, given $T \in \mathbb{N}$ and $D \in \mathbb{N} \cup \{+\infty\}$, if we let $\partial S \subseteq K - \{0\}$, $\tilde{n} = |\partial S| \leq |K| - 1$, $g(z) = z^T$ and $\mathcal{T} = \mathcal{S}(m, \tilde{n}, w, D)$ for any convenient $w \in \mathbf{Z}\mathbf{Z}_D$, then there exists a $\sigma(z) \in K[z]$ such that the code $\tilde{\mathcal{C}} \stackrel{\text{def}}{=} \mathcal{T} \cap \mathcal{C}_{\sigma,g}(\tilde{n}) \subseteq \mathcal{T}$ of length $\tilde{n}$ satisfies (10) and $|\tilde{\mathcal{C}}| \geq |\mathcal{S}(m, \tilde{n}, w, D)|/|K|^{T-1}$. With this choice of $\tilde{\mathcal{C}} \subseteq \mathcal{S}(m, \tilde{n}, w, D)$ in (9), we may let $\hat{r} = 0$, $n = \tilde{n} \leq |K| - 1$ and get a code $\mathcal{C} = \tilde{\mathcal{C}}$ satisfying (10) whose redundancy is $\rho(\mathcal{C}) \stackrel{\text{def}}{=} n - \log_m |\mathcal{C}| \leq \rho(\mathcal{S}(m, n, w, D)) + (T-1)\log_m |K|$.

Section V of [9] gives the following essentially linear codes which are easy to encode/decode (given $X \in \mathbf{Z}\mathbf{Z}_m^n$, below we let $S_X(z) \stackrel{\text{def}}{=} \sum_{i=1}^{+\infty} S_i(X) z^i$ where $S_i(X) \stackrel{\text{def}}{=} \sum_{j=1}^{n} m_X(j) a_j^i$)

$$\mathcal{C}_{1,z^T}(n) = \{X \subseteq S : \sigma_X(z) = 1 \bmod z^T\} = \{X \subseteq S : S_X(z) = 0 \bmod z^T\} = \mathcal{C}_{BCH-like}(n)$$

where $T \leq p = char(K) \in \mathbb{N} \cup \{+\infty\}$, $\partial S \stackrel{\text{def}}{=} \partial I \cup \partial R \subseteq K - \{0\}$, $\partial I \stackrel{\text{def}}{=} \{a_1, a_2, \ldots, a_k\}$, $\partial R \stackrel{\text{def}}{=} \{a_{k+1}, a_{k+2}, \ldots, a_n\}$ and $S \stackrel{\text{def}}{=} (m-1)\partial I \cup (p-1)\partial R \subseteq \mathbf{Z}\mathbf{Z}_m^n$. So, given $T \leq p$ and $D \in [2, m]$, if we let $\tilde{\mathcal{C}} \stackrel{\text{def}}{=} \mathcal{C}_{1,z^T}(\tilde{n})$ and $w \in \mathbf{Z}\mathbf{Z}_D$ in (9) we need $\hat{r} = 1$ extra check digit to get a code $\mathcal{C}$ satisfying (10) of length $n = \tilde{n} + 1 = |\partial S| + 1 \leq |K|$. To satisfy (8), the extra check digit can be simply computed as $C_{\tilde{X}} = \varphi(\tilde{X}) = (w - |\tilde{X}|) \bmod D \in \mathbf{Z}\mathbf{Z}_D$. Hence, $\mathcal{C}$ has $k \leq |K| - (T-1)\log_m |K| - 1$ information digits in $\mathbf{Z}\mathbf{Z}_m$ and $n - k = (T-1)\log_m |K| + 1$ check digits, of which, $\hat{r} = 1$ is in $\mathbf{Z}\mathbf{Z}_D$ and the remaining $(T-1)\log_m |K|$ are in $\mathbf{Z}\mathbf{Z}_p$. In general, given $T \leq p$ and $D - 1 \in [(\hat{r}-1)(m-1)+1, \hat{r}(m-1)]$ $\iff$ $D \in [\hat{r}(m-1) - m + 3, \hat{r}(m-1) + 1]$, $\hat{r} \in \mathbb{N}$ extra check digit are sufficient to get a code $\mathcal{C}$ satisfying (10) of length $n = \tilde{n} + \hat{r} = |\partial S| + \hat{r} \leq |K| + (\hat{r} - 1)$. In fact, relation (8) is satisfied if we use a simple function $\varphi : \mathbf{Z}\mathbf{Z}_m^{\tilde{n}} \to \mathbf{Z}\mathbf{Z}_m^{\hat{r}}$ such that $|C_{\tilde{X}}| = |\varphi(\tilde{X})| = (w - |\tilde{X}|) \bmod D \in \mathbf{Z}\mathbf{Z}_D$ (there are many ways to define such φ). In any case, $\mathcal{C}$ has $k \leq |K| - (T-1)\log_m |K| - 1$ information digits in $\mathbf{Z}\mathbf{Z}_m$ and $n - k = (T-1)\log_m |K| + \hat{r}$ check digits, of which, $\hat{r}$ are in $\mathbf{Z}\mathbf{Z}_m$ and the remaining $(T-1)\log_m |K|$ are in $\mathbf{Z}\mathbf{Z}_p$.

From Algorithm 4 and Algorithm 1 in [9], the core decoding Algorithm 1 based on σ-codes becomes

***Algorithm** 5 ((t_-, t_+)-EC/(d_-, d_+)-ED for CW σ-codes):*
Input: A word $Y = \tilde{Y}\, E \in \mathbf{Z}\mathbf{Z}_m^n$, $\tilde{Y} \in \mathbf{Z}\mathbf{Z}_m^{\tilde{n}}$ and $E \in \mathbf{Z}\mathbf{Z}_m^{\hat{r}}$.
Output: A word $X' = \tilde{X}'\, C' \in \mathbf{Z}\mathbf{Z}_m^n$, $\tilde{X}' \in \mathbf{Z}\mathbf{Z}_m^{\tilde{n}}$ and $C' \in \mathbf{Z}\mathbf{Z}_m^{\hat{r}}$, and a signal $cor \in \{0, 1\}$.

Assume (11) holds for $\mathcal{C}$ in (9) with $\tilde{\mathcal{C}} \stackrel{\text{def}}{=} \mathcal{C}_{\sigma,g}(n)$ and $T = \deg(g)$. Assume $X = \tilde{X}\, C_{\tilde{X}} \in \mathcal{C}$ is sent with $\tilde{X} \in \tilde{\mathcal{C}}$, the word $Y = \tilde{Y}\, E$ is received, $|X \dot{-} Y| \leq d_-$ and $|Y \dot{-} X| \leq d_+$.
Execute the following steps.
S1: Execute algorithm $\mathcal{D}ec(\tilde{\mathcal{C}}, \tau_- = t - t_+, \tau_+ = t_+)$ with input $\tilde{Y} \in \mathbf{Z}\mathbf{Z}_m^{\tilde{n}}$ and let $\tilde{X}'$ be its output. For example, use Algorithm 1 in [9] for error correction based on the Extended Euclidean Algorithm.
S2: Set $X' = \tilde{X}'\, C'$ with $C' = C_{\tilde{X}'} = \varphi(\tilde{X}')$.
S3: If $|X' \dot{-} Y| \leq t_-$ and $|Y \dot{-} X'| \leq t_+$ then set $cor = 1$. Otherwise, set $cor = 0$.
S4: Output X', output cor and exit.

For example, let $m = 16$, $K = GF(13)$, $p = 13$, $\partial S = K - \{0\}$. As $\tilde{\mathcal{C}}$, let $T = 5$ and the Reed-Solomon-like σ-code be $\tilde{\mathcal{C}} = \mathcal{C}_{1,z^5}$ of length $\tilde{n} = 12$ with $k = 8$ information digits in $\mathbf{Z}\mathbf{Z}_{16}$ and $r = n - k = 4$ check digits in $\mathbf{Z}\mathbf{Z}_{13}$. By adding $\hat{r} = 1$ extra check digit in $\mathbf{Z}\mathbf{Z}_D$, the following CW codes of length $n = 13$ with $k = 8$ information digits in $\mathbf{Z}\mathbf{Z}_{16}$, $r = 4$ check digits in $\mathbf{Z}\mathbf{Z}_{13}$ and $\hat{r} = 1$ check digit in $\mathbf{Z}\mathbf{Z}_D$ can be defined as in (9) for any $w \in \mathbf{Z}\mathbf{Z}_D$.
• $D = 16$: by using Algorithm 5, the code $\mathcal{C}$ can be decoded, for example, **as** a $(3,1)$-EC/$(14,1)$-ED, $(3,1)$-EC/$(3,12)$-ED (or as the combination of the two decodings like Algorithm 3), $(2,1)$-EC/$(14,2)$-ED, $(2,1)$-EC/$(3,13)$-ED, $(1,0)$-EC/$(15,3)$-ED, $(1,0)$-EC/$(4,14)$-ED code or, by using Algorithm 3, $\mathcal{C}$ can be decoded, for example, **as** a $(2,2)$-EC/$\{13,2\}$-ED, $(1,1)$-EC/$\{14,3\}$-ED, $(0,0)$-EC/$\{15,4\}$-ED code or, by using the Algorithms in [6], $\mathcal{C}$ can be decoded, for example, **as** a 4-SyEC/5-SyED/11-UED code for the L_1 metric.
• $D = 9$: by using Algorithm 5, the code $\mathcal{C}$ can be decoded, for example, **as** a $(3,1)$-EC/$(7,1)$-ED, $(3,1)$-EC/$(3,5)$-ED, $(2,1)$-EC/$(7,2)$-ED,$(2,1)$-EC/$(3,6)$-ED,$(1,0)$-EC/$(8,3)$-ED,$(1,0)$-EC/$(4,7)$-ED code or, by using Algorithm 3, $\mathcal{C}$ can be decoded, for example, **as** a $(2,2)$-EC/$\{6,2\}$-ED, $(1,1)$-EC/$\{7,3\}$-ED, $(0,0)$-EC/$\{8,4\}$-ED code or, by using Algorithm 2, $\mathcal{C}$ can be decoded, for example, **as** a $\{4,0\}$-EC/$(4,4)$-ED code or, by using the Algorithms in [6], $\mathcal{C}$ can be decoded, for example, **as** a 4-SyEC code for the L_1 metric.
• $D = 6$: by using Algorithm 5, the code $\mathcal{C}$ can be decoded, for example, **as** a $(3,1)$-EC/$(4,1)$-ED, $(3,1)$-EC/$(3,2)$-ED code or, by using Algorithm 3, $\mathcal{C}$ can be decoded, for example, **as** a $(2,2)$-EC/$\{3,2\}$-ED, $(1,1)$-EC/$\{4,3\}$-ED, $(0,0)$-EC/$\{5,4\}$-ED code or, by using Algorithm 2, $\mathcal{C}$ can be decoded, for example, **as** a $\{2,1\}$-EC/$(3,3)$-ED, $\{1,0\}$-EC/$(4,4)$-ED code.

ACKNOWLEDGMENT

This work is supported by the NSF Grant CCF-1117215 and by the Italian MIUR Grant PRIN 2009-2009EL7424.

REFERENCES

[1] M. Blaum, *Codes fo Detecting and Correcting Unidirectional Errors*, IEEE Computer Society Press, 1993.
[2] Y. Cassuto, M. Schwartz, V. Bohossian, J. Bruck, "Codes for multi-level flash memories: Correcting asymmetric limited-magnitude errors", *Proc. of 2007 IEEE ISIT*, pp. 1176-1180, June 2007.
[3] R. Mascella, L. G. Tallini, "Efficient m-ary balanced codes which are invariant under symbol permutation", *IEEE Trans. Comput.*, vol. 55, pp. 929–946, Aug. 2006.
[4] L. Pezza, L. G. Tallini, B. Bose, "Variable Length Unordered Codes", *IEEE Trans. Inform. Theory*, vol. 58, pp. 548–569, Feb. 2012.
[5] R. Roth, *Introduction to Coding Theory*, Cambridge Univ. Press, 2006.
[6] L. G. Tallini, B. Bose, "On L_1 metric t-SyEC/s-SyED/u-UED, $t \leq s \leq u$, codes, constrained weight codes and σ-codes", technical report.
[7] L. G. Tallini, B. Bose, "On symmetric L_1 distance error control codes and elementary symmetric functions", *Proc. 2012 IEEE ISIT*, pp. 741-745, July 2012.
[8] L. G. Tallini, B. Bose, "On symmetric/asymmetric Lee distance error control codes and elementary symmetric functions", *Proc. 2012 IEEE ISIT*, pp. 746-750, July 2012.
[9] L. G. Tallini, B. Bose, "On L_1-distance error control codes", *Proc. 2011 IEEE ISIT*, pp. 1026-1030, July/August 2011.
[10] L. G. Tallini, B. Bose, "Reed-Muller codes, elementary symmetric functions and asymmetric error correction", *Proc. 2011 IEEE ISIT*, pp. 1016-1020, July/August 2011.
[11] L. G. Tallini, N. Elarief, B. Bose, "On Efficient Repetition Error Correcting Codes", *Proc. 2010 IEEE ISIT*, pp. 1012-1016, June 2010.
[12] L. G. Tallini, B. Bose, "On a new class of error control codes and symmetric functions", *Proc. 2008 IEEE ISIT*, pp. 980-984, July 2008.
[13] L. G. Tallini, S. Al-Bassam, B. Bose, "Feedback Codes Achieving the Capacity of the Z-Channel", *IEEE Trans. Inform. Theory*, vol. 54, pp. 1357–1362, March 2008.
[14] L. G. Tallini, "Bounds on the capacity of the unidirectional channels", *IEEE Transactions on Computers*, vol. 54, no. 2, pp. 232-235, Feb. 2005.