Ars Combinatoria, 159: 51–58
DOI:10.61091/ars159-06
http://www.combinatorialpress.com/ars
Received 15 March 2019, Accepted 18 March 2020, Published 30 June 2024

Article

Some Properties of Channel Detecting Codes on Specific Domains

Jen-Tse Wang[1], **and Cheng-Chih Huang**[2,*]

[1] Department of Information Management, Hsiuping University of Science and Technology, Taichung, Taiwan 412

[2] Department of Computer Science and Information Engineering, National Taichung University of Science and Technology, Taichung, Taiwan 403

* **Correspondence:** jimhuang@nutc.edu.tw

Abstract: This project aims at investigating properties of channel detecting codes on specific domains 1^+0^+. We focus on the transmission channel with the deletion errors. Firstly we discuss properties of channels with the deletion errors. We propose a certain kind of code that is a channel detecting (abbr. γ-detecting) code for the channel $\gamma = \delta(m, N)$ where $m < N$. The characteristic of this γ-detecting code is considered. One method is provided to construct γ-detecting code. Finally, we also study a kind of special channel code named $\tau(m, N)$-srp code.

Keywords: Channel codes, Error-correcting codes, Error-detecting codes
2010 Mathematics Subject Classification: 05C78, 05C25

---

1. Introduction

The classical coding theory pays attention to substitution errors occurring when the messages are communicated through the transmission channel. In [1], an abstract channel with combinations of substitutions, deletions and insertions and its properties are discussed. Moreover, the authors [2] provide the concepts of singleton-detecting and $(\gamma, *)$-detecting codes which can detect both synchronous and asynchronous errors when the finite-length messages are communicated through the transmission channel. Some concepts related to the error detecting property have been studied in [3], [4]. In this project, we first study the concept of γ-detecting codes which are applied for the infinite-length messages communicated in the transmission channel. Furthermore we consider some properties of γ-detecting codes. Next, we investigate some properties of the codes of the form 1^n0^n with $n \geq 1$ for the transmission channel $\delta(m, N)$ and propose one method to construct $\delta(m, N)$-detecting code. Some properties of the special channel code named $\tau(m, N)$-srp code are studied in the final section. We also find the maximal $\delta(m, N)$-srp code on specific domains 1^+0^+.

2. Preliminaries

Let X be a finite alphabet and let X^* be the free monoid generated by X. The set of natural numbers is denoted by $\aleph$. Any element of X^* is called a *word*. The length of a word w is denoted by $\lg(w)$. Any subset of X^* is called a *language*. Let $X^+ = X^* \setminus \{\lambda\}$, where λ is the empty word. The concatenation of two words w and v over X is denoted by wv. For each positive integer n and $L \subseteq X^*$, the notation

$L^n = \{u_1u_2 \cdots u_n | \ u_i \in L, 1 \le i \le n\}$. Let $L^0 = \{\lambda\}$. Then $X^n = \{w \in X^* | \ \lg(w) = n\}$. The set consisting of all infinite sequences of nonempty words of L is denoted by $L^\omega = \{u_1u_2 \cdots u_i \cdots | \ u_i \in L \setminus L^0, i \ge 1\}$. Let $L^\infty = L^* \cup L^\omega$, where $L^* = \bigcup_{n=0}^{\infty} L^n$. Note that $L^* \cap L^\omega = \emptyset$.

Let $Y \subseteq X^*$. If $y \in Y^\omega$, then a factorization of y over Y is an element $(y_1, y_2, \ldots, y_n, \ldots)$ of the countably infinite Cartesian product of Y, denoted by $\Pi^\infty Y$, for which $y = y_1y_2 \cdots y_n \cdots$. If $y \in Y^+$, then a factorization of y over Y with order n is an ordered n-tuple $(y_1, y_2, \ldots, y_n)$ such that $y_i \in Y, 1 \le i \le n$, and $y = y_1y_2 \cdots y_n$. A factorization of $y \in Y^+$ over Y is a factorization of y over Y with some order n.

A channel γ over X is a subset of the Cartesian product $X^\infty \times X^\infty$. An element $(y', y) \in \gamma$ means that for an input y, the channel could output y'. A channel is noiseless if $\gamma \subseteq \{(y, y) | y \in X^\infty\}$. Otherwise, it is noisy. Denote by π_2 the projection onto the second coordinate, which is defined by $\pi_2(y_1, y_2) = y_2$ for every $(y_1, y_2) \in X^\infty \times X^\infty$. For $\gamma \subseteq X^\infty \times X^\infty$, this notation can be extended to $\pi_2(\gamma) = \bigcup_{y' \in X^\infty} \{y \in X^\infty | (y', y) \in \gamma\}$. Thus $\langle y \rangle_\gamma$ is the set of all possible outputs of with respect to the input y. Given a subset Y of $\pi_2(\gamma)$, we define $\langle Y \rangle_\gamma = \cup_{y \in Y} \langle y \rangle_\gamma$ to be the γ-spanned set of Y.

Three basic error types σ, ι, and δ indicate substitutions, insertions, and deletions, respectively. For a natural number N and a nonnegative integer m with $m \le N$, $\gamma(m, N)$ denotes that at most m errors of type γ can occur in any consecutive N symbols in a channel, where γ may be σ, ι, δ, or their combinations. Note that (see [5]) for a nonempty word w with $\lg(w) = n$ where $n \le N$,

$$\langle w \rangle_{\gamma(m,N)} = \begin{cases} \langle w \rangle_{\gamma(m,n)}, & \text{if } N \ge n \ge m; \\ \langle w \rangle_{\gamma(n,n)}, & \text{if } m > n. \end{cases}$$

For instance, $\langle 1100 \rangle_{\delta(1,4)} = \{1100, 100, 110\} = \langle 1100 \rangle_{\delta(1,5)}$ and $\langle 1100 \rangle_{\delta(1,3)} = \{1100, 100, 110, 10\}$. Items not defined in this project can be found in ([6], [5]).

Remark 1. *Let $N_2 \ge N_1 \ge N$ for some nature numbers N, N_1, N_2. Then $\langle w \rangle_{\delta(1,N_2)} \subseteq \langle w \rangle_{\delta(1,N_1)}$ where* $\lg(w) = n \le N$.

Definition 1. *Let γ be a channel. A code $C \subseteq X^+$ is detecting for γ or γ-detecting, if the following condition is satisfied : for all $w \in C^\infty$, $C^\infty \cap \langle w \rangle_\gamma = \{w\}$.*

From the above definition of the channel detecting code, we have that if the code C is called channel detecting, then for all $w_1, w_2 \in C^\infty$ with $w_1 \ne w_2$, $w_1 \notin \langle w_2 \rangle_\gamma$ for channel γ. For instance, let $C = \{1^20^4, 1^60^6\}$, $w_1 = 110000(1^60^6)^\omega, w_2 = 110000110000(1^60^6)^\omega \in C^\infty$. It is clear that $w_1 \ne w_2$, but $w_1 \in \langle w_2 \rangle_\gamma$ where $\gamma = \delta(3, 4)$ because w_1 can be obtained from $w_2 = 11\underline{0}00\underline{011}00\underline{00}(1^60^6)^\omega$ after deleting the underlined symbols. Then C is not $\delta(3, 4)$-detecting code.

3. Properties of Channel Detecting Codes

In this section, the channel with deletion errors is considered. We consider the case $\gamma = \delta(m, N)$ where $m < N$. The case $\gamma = \delta(m, N)$ where $m \ge N$ is omitted because there does not exist such a γ-detecting code. First, we study the sufficient conditions of γ-detecting code. For instance, let $X = \{0, 1\}$, $C = \{1^20^4\}$ and $\gamma = \delta(6, 10)$. Let $w_1 = (1^20^4)^4$ and $w_2 = (1^20^4)^5$. Then $w_1 \ne w_2$ for $w_1, w_2 \in C^\infty$. We have $w_1 \in \langle w_2 \rangle_\gamma$. This implies that C is not γ-detecting.

Remark 2. *Let $C = \{w\}$ and $\gamma = \delta(m, N)$ where $m < N$. If* $\lg(w) \le m$*, then C is not γ-detecting.*

Proof. Suppose that C is γ-detecting. Let $w^k, w^{k+1} \in C^\infty$ for some $k \ge 1$. Then $w^k \ne w^{k+1}$. Since $\lg(w) \le m$, by the definition of channel detecting code, $w^k \in \langle w^{k+1} \rangle_\gamma$, a contradiction. Thus C is not γ-detecting. □

Remark 3. *Let $\gamma = \delta(m, N)$ where $m < N$. Let C be a γ-detecting code with $N \ge \max\{\lg(w) | \ w \in C\}$. If there exist $p, q \in X^*$ such that $w, pwq \in C$, then $pq = \lambda$ or $\lg(pq) > m$.*

Proof. Let C be a γ-detecting code. Suppose that there exist $w, pwq \in C$ such that $u = pwq$ for some $p, q \in X^*$ with $1 \leq \lg(pq) \leq m$. Since $N \geq \max\{\lg(w)|w \in C\}$, we have $w \in \langle u\rangle_\gamma$. This contradicts that C is a γ-detecting code.

□

Lemma 1. *Let $X = \{0,1\}$ and $w_1 = 1^i0^i$, $w_2 = 1^j0^j$ where $i, j \in \aleph$ and $j > i$. Let $\gamma = \delta(m, N)$ where $m < N$ and $t = \lfloor\frac{\lg(w_2)}{N}\rfloor$. Then $w_1 \in \langle w_2\rangle_\gamma$ if and only if* $\lg(w_2) - \lg(w_1) \leq tm + \min\{m, \lg(w_2) - tN\}$.

Proof. Let $w_1 = 1^i0^i$, $w_2 = 1^j0^j$ where $i, j \in \aleph$ and $j > i$. Let $t = \lfloor\frac{\lg(w_2)}{N}\rfloor$. Then $t \leq \frac{\lg(w_2)}{N} < t + 1$. It follows that $tN \leq \lg(w_2) < tN + N$. We have $w_2 = 1^j0^j = a_1 \cdots a_{tN} \cdots a_{2j}$, where $a_k \in \{0,1\}$ for $1 \leq k \leq 2j$. First, we consider to delete m digits from $a_{sN+1} \cdots a_{sN+N}$ whenever $0 \leq s < t$. Then the total tm digits are deleted from 1^j0^j. Secondly, the $\min\{m, \lg(w_2) - tN\}$ digits are deleted from $a_{tN+1} \cdots a_{2j}$. Thus for any word $w_1 = 1^i0^i$ with $i < j$, the condition $\lg(w_2) - \lg(w_1) \leq tm + \min\{m, \lg(w_2) - tN\}$ implies that $w_1 \in \langle w_2\rangle_\gamma$. By an analogous proof, the condition $\lg(w_2) - \lg(w_1) > tm + \min\{m, \lg(w_2) - tN\}$, implies that $w_1 \notin \langle w_2\rangle_\gamma$.

□

Corollary 1. *Let $\gamma = \delta(m, N)$ where $m < N$. Then $a^k \in \langle a^j\rangle_\gamma$ with $j \geq k$ for some $a \in X$ and $k, j \in \aleph$ if and only if $k \geq j - (tm + \min\{m, j - tN\})$ where $t = \lfloor\frac{j}{N}\rfloor$.*

We study the relationship between words which have the form $1^{s_1}0^{s_2} \in \langle 1^j0^j\rangle_\gamma$ with $s_1, s_2 \in \aleph$ and words which have the form $1^i0^i \notin \langle 1^j0^j\rangle_\gamma$ with $i \in \aleph$ where $j \in \aleph$ for the channel $\gamma = \delta(m, N)$ where $m < N$. For instance, let $\gamma = \delta(1, 3)$. Then $\langle 1^50^5\rangle_\gamma = \{1^{s_1}0^{s_2}|\ 3 \leq s_1 \leq 5,\ 3 \leq s_2 \leq 5\}$. It is clear that $10,\ 1^20^2 \notin \langle 1^50^5\rangle_\gamma$.

Lemma 2. *Let $X = \{0,1\}$ and $w_1 = 1^i0^i$, $w_2 = 1^{s_1}0^{s_2}$, $w_3 = 1^j0^j$ where $i, j, s_1, s_2 \in \aleph$ and $j > i$. Let $\gamma = \delta(m, N)$ where $m < N$. If $w_1 \notin \langle w_3\rangle_\gamma$ and $w_2 \in \langle w_3\rangle_\gamma$, then $s_1, s_2 > i$.*

Proof. Let $\gamma = \delta(m, N)$ where $m < N$ and $t = \lfloor\frac{\lg(w_3)}{N}\rfloor$. We consider $w_1 \notin \langle w_3\rangle_\gamma$ and $w_2 \in \langle w_3\rangle_\gamma$. As $w_2 \in \langle w_3\rangle_\gamma$, by Lemma 1, we have $\lg(w_3) - \lg(w_2) \leq tm + \min\{m, \lg(w_3) - tN\}$. Since $w_1 \notin \langle w_3\rangle_\gamma$, by Lemma 1 again, we have $\lg(w_3) - \lg(w_1) > tm + \min\{m, \lg(w_3) - tN\}$. It follows that $\lg(w_3) - \lg(w_2) < \lg(w_3) - \lg(w_1)$. Thus $\lg(w_1) < \lg(w_2)$. We have $2i < s_1 + s_2$. There are the following cases:

(1) $i \geq s_1$. By corollary 1, we have $s_1 \geq j - (tm + \min\{m, j - tN\})$ and $i < j - (tm + \min\{m, j - tN\})$ where $t = \lfloor\frac{j}{N}\rfloor$. It follows that $s_1 > i$, a contradiction.

(2) $i < s_1$ and $i \geq s_2$.

As $i \geq s_2$, the proof is similar to case (1). It follows that $s_2 > i$, a contradiction. From case (1) and case (2), we have $s_1, s_2 > i$.

□

Lemma 3. *Let $X = \{0,1\}$ and $w_1 = 1^i0^i$, $w_2 = 1^j0^j$ where $i, j \in \aleph$ and $j > i$. Let $\gamma = \delta(m, N)$ where $m < N$ and $k = \lfloor\frac{\lg(w_1)}{N-m}\rfloor$. Then the following statements are true:*

(1) $w_1 \in \langle w_2\rangle_\gamma$ when $\lg(w_2) \leq \lg(w_1) + (k+1)m$.

(2) $w_1 \notin \langle w_2\rangle_\gamma$ when $\lg(w_2) \geq \lg(w_1) + (k+1)m + 1$.

Proof. Let $w_1 = 1^i0^i$, $w_2 = 1^j0^j$ where $i, j \in \aleph$ and $j > i$. Let $t = \lfloor\frac{\lg(w_2)}{N}\rfloor$. Then $t \leq \frac{\lg(w_2)}{N} < t + 1$. It follows that

$$tN \leq \lg(w_2) < (t+1)N. \tag{1}$$

Let $k = \lfloor\frac{\lg(w_1)}{N-m}\rfloor$. We consider the following cases:

(1) $\lg(w_2) \leq \lg(w_1) + (k+1)m$. Since $k = \lfloor \frac{\lg(w_1)}{N-m} \rfloor$, we have $k \leq \frac{\lg(w_1)}{N-m} < k+1$. It follows that

$$k(N-m) \leq \lg(w_1) < (k+1)(N-m). \tag{2}$$

This in conjunction with $\lg(w_2) \leq \lg(w_1) + (k+1)m$ yields that $\lg(w_2) < (k+1)(N-m) + (k+1)m = (k+1)N$. By Eq. (1), we have $t \leq \frac{\lg(w_2)}{N}$. Thus $tN \leq \lg(w_2)$. This in conjunction with $\lg(w_2) < (k+1)N$ yields that $t < (k+1)$; hence $t \leq k$. By Lemma 1, we want to show that $\lg(w_2) - tm - \min\{m, \lg(w_2) - tN\} \leq \lg(w_1)$. It will imply that $w_1 \in \langle w_2 \rangle_\gamma$. We consider the following subcases:

(1-1) $\lg(w_2) - tN < m$. We have $\lg(w_2) - tm - \min\{m, \lg(w_2) - tN\} = \lg(w_2) - tm - (\lg(w_2) - tN) = t(N-m) \leq k(N-m)$. This in conjunction with Eq. (2) yields that $\lg(w_2) - tm - \min\{m, \lg(w_2) - tN\} \leq \lg(w_1)$.

(1-2) $\lg(w_2) - tN \geq m$. We have $\lg(w_2) - tm - \min\{m, \lg(w_2) - tN\} = \lg(w_2) - tm - m = \lg(w_2) - (t+1)m$. From Eq. (1), we have $\lg(w_2) < (t+1)N$. It follows that $\lg(w_2) - (t+1)m < (t+1)N - (t+1)m = (t+1)(N-M) \leq k(N-M) \leq \lg(w_1)$ whenever $t < k$. If $t = k$, then $\lg(w_2) - (t+1)m = \lg(w_2) - (k+1)m$. This in conjunction with $\lg(w_2) \leq \lg(w_1) + (k+1)m$ yields that $\lg(w_2) - tm - \min\{m, \lg(w_2) - tN\} \leq \lg(w_1)$.

Therefore, we showed that $\lg(w_2) - tm - \min\{m, \lg(w_2) - tN\} \leq \lg(w_1)$. Thus $w_1 \in \langle w_2 \rangle_\gamma$.

(2) $\lg(w_1) + (k+1)m + 1 \leq \lg(w_2)$. From Eq. (2), we have $k(N-m) \leq \lg(w_1)$. This in conjunction with $\lg(w_1) + (k+1)m + 1 \leq \lg(w_2)$ yields that $k(N-m) + (k+1)m + 1 \leq \lg(w_1) + (k+1)m + 1 \leq \lg(w_2)$. Thus $kN + m + 1 \leq \lg(w_2)$. By Lemma 1, we want to show that $\lg(w_2) - tm - \min\{m, \lg(w_2) - tN\} > \lg(w_1)$. We consider the following subcases:

(2-1) $\lg(w_2) - tN \leq m$. We have $kN + m + 1 \leq \lg(w_2) \leq tN + m$. This implies that $k < t$. Since $\lg(w_2) - tN \leq m$, we have $\lg(w_2) - tm - \min\{m, \lg(w_2) - tN\} = \lg(w_2) - tm - (\lg(w_2) - tN) = t(N-m)$. This in conjunction with $k < t$ yields that $t(N-m) \geq (k+1)(N-m)$. From Eq. (2), we have $\lg(w_1) < (k+1)(N-m)$. Hence $\lg(w_2) - tm - \min\{m, \lg(w_2) - tN\} > \lg(w_1)$.

(2-2) $\lg(w_2) - tN > m$. Since $kN + m + 1 \leq \lg(w_2)$, this in conjunction with Eq. (1) which $\lg(w_2) < (t+1)N$ yields that $kN + m + 1 < (t+1)N = tN + N$. Note that $m < N$. This implies that $k \leq t$. Since $\lg(w_2) - tN > m$, we have $\lg(w_2) - tm - \min\{m, \lg(w_2) - tN\} = \lg(w_2) - tm - m$ and $\lg(w_2) > tN + m$. It follows that $\lg(w_2) - tm - m > tN + m - tm - m = t(N-m)$. If $t > k$, then $t(N-m) \geq (k+1)(N-m)$. From Eq. (2), $\lg(w_2) - tm - \min\{m, \lg(w_2) - tN\} < (k+1)(N-m)$. We have $\lg(w_2) - tm - \min\{m, \lg(w_2) - tN\} > \lg(w_1)$. If $t = k$, then $\lg(w_2) - tm - m = \lg(w_2) - km - m$. Since $\lg(w_1) + (k+1)m + 1 \leq \lg(w_2)$, we have $\lg(w_2) - km - m \geq \lg(w_1) + (k+1)m + 1 - km - m = \lg(w_1) + 1 > \lg(w_1)$.

Therefore, we showed that $\lg(w_2) - tm - \min\{m, \lg(w_2) - tN\} > \lg(w_1)$. Thus $w_1 \notin \langle w_2 \rangle_\gamma$.

□

We extend the concept of the above Lemma 2 and Lemma 3. We have the following lemma.

Lemma 4. *Let $X = \{0, 1\}$ and $w_1 = 1^i 0^i$, $w_2 = 1^{s_1} 0^{s_2}$, $w_3 = 1^j 0^j$ where $i, j, s_1, s_2 \in \aleph$ and $j > i$. Let $\gamma = \delta(m, N)$ where $m < N$ and $k = \lfloor \frac{\lg(w_1)}{N-m} \rfloor$. If $w_2 \in \langle w_3 \rangle_\gamma$ and $\lg(w_3) \geq \lg(w_1) + (k+1)m + 1$, then $s_1, s_2 > i$.*

Proposition 1. *Let $X = \{0, 1\}$, $C \subseteq \{1^n 0^n | \ n \in \aleph\}$, and $\gamma = \delta(m, N)$ where $m < N$. Let $k = min\{ \lg(w) | \ w \in C\}$ and $k > m$. If the following conditions hold:*

(1) for $w_1, w_2 \in C$ with $\lg(w_2) > \lg(w_1)$, $\lg(w_2) > \lg(w_1) + (\lfloor \frac{\lg(w_1)}{N-m} \rfloor + 1)m$;

(2) for $w_3, w_4 \in C$ with $\lg(w_3) \geq \lg(w_4)$, $\{w_3\} \cap \langle w^* w_4 w^* \setminus w_3 \rangle_\gamma = \emptyset$ where $\lg(w) = k$,

then C is γ-detecting.

Proof. Assume that there exist $u, v \in C^\infty$ such that $u \in \langle v \rangle_\gamma$. Let $u = u_1 u_2 \cdots u_i \cdots$ and $v = v_1 v_2 \cdots v_j \cdots$, where $u_i, v_j \in C$ and $i, j \in \aleph$. Now we consider the first subword u_1 of u such that $u_1 \in \langle v_1 v_2 \cdots v_k \rangle_\gamma$ where $k \geq 1$. By Lemma 3, the statement (1) implies that $u_{i'} \notin \langle v_{j'} \rangle_\gamma$ for some $i', j' \in \aleph$. It follows that $u_{i'} \notin \langle x v_{j'} y \rangle_\gamma$ where $x, y \in C^\infty$. Indeed, if $u_{i'} \in \langle x v_{j'} y \rangle_\gamma$, then we have $\lg(x v_{j'} y) - \lg(u_{i'}) \leq (\lfloor \frac{\lg(w_1)}{N-m} \rfloor + 1)m < \lg(v_{j'}) - \lg(u_{i'})$, a contradiction. Therefore, $u_1 \in \langle v_1 v_2 \cdots v_k \rangle_\gamma$ implies that $\lg(u_1) \geq \lg(v_i)$ for all $1 \leq i \leq k$. Let $k = min\{ \lg(w) | \, w \in C\}$ and $k > m$. We consider the following cases:

(1) $2m < k$.

From the definition of the channel with deletion errors, we have $1^s \notin \langle C^\infty \rangle_\gamma$ and $0^t \notin \langle C^\infty \rangle_\gamma$ where $s, t \in \aleph$. Thus for $u_1 \in \langle v_1 v_2 \cdots v_k \rangle_\gamma$, we have $u_1 \in \langle v_1 \rangle_\gamma$. Note that if $\lg(u_1) > \lg(v_1)$, then $u_1 \notin \langle v_1 \rangle_\gamma$. This in conjunction with $\lg(u_1) \geq \lg(v_1)$ yields that $u_1 = v_1$.

(2) $2m \geq k$. Let $\lg(w) = k$ where $w \in C$. From the the statement (1), we have $\lg(w') > \lg(w) + (\lfloor \frac{\lg(w)}{N-m} \rfloor + 1)m$ for some $w' \in C \setminus \{w\}$. This in conjunction with $\lg(w) \geq m$ yields that $\lg(w') > m + (\lfloor \frac{\lg(w)}{N-m} \rfloor + 1)m > 2m$. Then we have $1^s \notin \langle C^* \rangle_\gamma \setminus \langle w^* \rangle_\gamma$ and $0^t \notin \langle C^* \rangle_\gamma \setminus \langle w^* \rangle_\gamma$ where $s, t \in \aleph$. Now we consider $u_1 \in \langle v_1 v_2 \cdots v_k \rangle_\gamma$ with $\lg(u_1) \geq \lg(v_i)$ for all $1 \leq i \leq k$. If $k = 1$, then we have $u_1 \in \langle v_1 \rangle_\gamma$. By the similar proof used in case(1), we have $u_1 = v_1$. If $k > 1$, then we can assume that $u_1 = 1^p 1^m 0^n 0^q$ where $p, q, m, n \in \aleph \cup \{0\}$ such that $1^p \in \langle w^* \rangle_\gamma$, $1^m 0^n \in \langle v_i \rangle_\gamma$ where $1 \leq i \leq k$, and $0^q \in \langle w^* \rangle_\gamma$. There are the following subcases:

(2-1) $m = 0$ or $n = 0$ or $m = n = 0$.

Since $1^s \notin \langle C^* \rangle_\gamma \setminus \langle w^* \rangle_\gamma$ and $0^t \notin \langle C^* \rangle_\gamma \setminus \langle w^* \rangle_\gamma$ where $s, t \in \aleph$, this in conjunction with $u_1 \in \langle v_1 v_2 \cdots v_k \rangle_\gamma$ yields that $u_1 \in \langle ww \cdots w \rangle_\gamma = \langle w^* w w^* \rangle_\gamma$. This result contradicts the statement (2).

(2-2) $p = 0$ and $q \neq 0$.

We have $u_1 = 1^m 0^n 0^q$. Since $u_1 \in \langle v_1 v_2 \cdots v_k \rangle_\gamma$, this implies that $u_1 \in \langle v_i w \cdots w \rangle_\gamma = \langle w^* v_i w^* \rangle_\gamma$. This result contradicts the statement (2).

(2-3) $p \neq 0$ and $q = 0$.

We have $u_1 = 1^p 1^m 0^n$. Since $u_1 \in \langle v_1 v_2 \cdots v_k \rangle_\gamma$, this implies that $u_1 \in \langle w \cdots w v_i \rangle_\gamma = \langle w^* v_i w^* \rangle_\gamma$. This result contradicts the statement (2).

(2-4) $p = 0$ and $q = 0$.

We have $u_1 = 1^m 0^n$. Then $u_1 \in \langle v_1 \rangle_\gamma$. This implies that $u_1 = v_1$.

(2-5) $p \neq 0$ and $q \neq 0$.

We have $u_1 = 1^p 1^m 0^n 0^q$. Since $u_1 \in \langle v_1 v_2 \cdots v_k \rangle_\gamma$, this implies that $u_1 \in \langle w \cdots w v_i w \cdots w \rangle_\gamma = \langle w^* v_i w^* \rangle_\gamma$. This result also contradicts the statement (2).

Therefore, we can conclude that for $u_1 \in \langle v_1 v_2 \cdots v_k \rangle_\gamma$ with $k \geq 1$, we have $u_1 \in \langle v_1 \rangle_\gamma$ and $u_1 = v_1$. By similar discussion, we can conclude the results that $u_2 = v_2$, $u_3 = v_3$, $\cdots$. Thus $u \in \langle v \rangle_\gamma$ implies that $u = v$ and C is γ-detecting.

□

4. A Construction of Channel Detecting Codes

Let $\gamma = \delta(m, N)$ for any given $1 \leq m < N$. In this section, we provide a method to construct γ-detecting code which is the subset of $\{1^n 0^n | n \geq 1\}$.

Proposition 2. *Let $X = \{0,1\}$ and $\gamma = \delta(m,N)$ where $m < N$. Let $C = \{w\}$ where $w = 1^{s_1}0^{s_2}$ for some $s_1, s_2 \in \aleph$. Then $w \notin \langle w^2\rangle_\gamma$ implies that C is γ-detecting.*

Proof. Suppose that C is not γ-detecting. There exist $w_1, w_2 \in C^\infty, w_1 \neq w_2$ such that $w_1 \in \langle w_2\rangle_\gamma$. Without loss of generality, we can assume that $w_{w_1} = w$ and $w_{w_2} = w^\infty \setminus \{w\}$ such that $w_{w_1} \in \langle w_{w_2}\rangle_\gamma$ where w_{w_1} and w_{w_2} are subwords of w_1 and w_2 respectively. Now we consider $w \in \langle w^\infty \setminus \{w\}\rangle_\gamma$. There exist $u \in \langle w^2\rangle_\gamma$ and $v \in \langle w^\infty\rangle_\gamma$ such that $w = uv$. Since $w = 1^{s_1}0^{s_2}$, it follows that $u = 1^{i_1}0^{i_2}$ for some $0 \leq i_1 \leq s_1$ and $0 \leq i_2 \leq s_2$. This in conjunction with the definition of the transmission channel $\gamma = \delta(m,N)$ yields that $\{1^{j_1}0^{j_2} \in w^2 | \ i_1 \leq j_1 \leq s_1, \ i_2 \leq j_2 \leq s_2\}$. This implies that $w \in \langle w^2\rangle_\gamma$, a contradiction. Thus C is γ-detecting.

□

In the following we define a function for constructing the γ-detecting code where $\gamma = \delta(m,N)$. A function $f_\gamma : \aleph \to \aleph$ is defined as

$$f_\gamma(1) = m + 1$$

and

$$f_\gamma(k+1) = f_\gamma(k) + \left\lceil \frac{(\lfloor \frac{2f_\gamma(k)}{N-m} \rfloor + 1)m + 1}{2} \right\rceil$$

for $k \in \aleph$.

For instance, let $\gamma = \delta(1,4)$. Then $f_\gamma(\aleph) = \{2,4,6,9,13,\cdots\}$. We have $\langle 1^6 0^6\rangle_\gamma = \{1^{s_1}0^{s_2} | \ 4 \leq s_1 \leq 6, 4 \leq s_2 \leq 6\} \setminus \{1^4 0^4\}$ and $\langle 1^4 0^4\rangle_\gamma = \{1^{s_1}0^{s_2} | \ 3 \leq s_1 \leq 4, 3 \leq s_2 \leq 4\}$. Note that $1^2 0^2 \notin \langle 1^4 0^4\rangle_\gamma$.

Proposition 3. *The code $C = \{1^{f_\gamma(k)}0^{f_\gamma(k)} \mid k \in \aleph\}$ is γ-detecting where $\gamma = \delta(m,N)$.*

Proof. Let $X = \{0,1\}$, $\gamma = \delta(m,N)$, and $C = \{1^{f_\gamma(k)}0^{f_\gamma(k)} \mid k \in \aleph\}$. We take $w_1 = 1^{f_\gamma(i)}0^{f_\gamma(i)}$ and $w_2 = 1^{f_\gamma(j)}0^{f_\gamma(j)}$ with $j > i$ where $i, j \in \aleph$. It follows $\lg(w_2) - \lg(w_1) = 2(f_\gamma(j) - f_\gamma(i)) \geq 2(f_\gamma(i+1) - f_\gamma(i)) = 2\lceil \frac{(\lfloor \frac{2f_\gamma(i)}{N-m} \rfloor + 1)m + 1}{2} \rceil \geq (\lfloor \frac{2f_\gamma(i)}{N-m} \rfloor + 1)m + 1 > (\lfloor \frac{2f_\gamma(i)}{N-m} \rfloor + 1)m$. By Lemma 3, we have $w_1 \notin \langle w_2\rangle_\gamma$. By Proposition 2, it follows that C is γ-detecting.

□

5. A Special kind of Channel Code

In this section, we study a special kind of channel code. Let $\tau = \{\delta, \sigma, \iota\}$ and let γ be a channel of the form $\tau(m,N)$ where $m < N$. We consider the following properties from [5]. For a language $L \subseteq X^+$, let

$$\mathrm{Pref}(L) = \{x \in X^+ | \ xX^* \cap L \neq \emptyset\},$$

and

$$L_s = \{y \in X^+ | \ X^*Ly \cap L \neq \emptyset\}.$$

A language $L \subseteq X^+$ is called *strongly residue preventive* if $\mathrm{Pref}(L) \cap L_s = \emptyset$. For instance, let $L = \{ab, a^2ba\}$. Then $\mathrm{Pref}(L) = \{a, ab, a^2, a^2b, a^2ba\}$ and $L_s = \{a\}$. Since $a \in \mathrm{Pref}(L) \cap L_s$, L is not strongly residue preventive. A language L is an $\tau(m,N)$-srp code [5] if $\langle L\rangle_{\tau(m,N)}$ is strongly residue preventive. For instance, let $X = \{0,1\}$, $\gamma = \delta(1,4)$. We take $w = 1^3 0^2 \in 1^+0^+$. Then $\langle w\rangle_\gamma = \{1^3 0^2, 1^3 0, 1^2 0^2, 1^2 0\}$. It follows that $(\langle w\rangle_\gamma)_s = \{0\}$ and $\mathrm{Pref}(\langle w\rangle_\gamma) = \{1, 1^2, 1^3, 1^3 0, 1^3 0^2, 1^2 0, 1^2 0^2\}$. Thus $\mathrm{Pref}(\langle w\rangle_\gamma) \cap (\langle w\rangle_\gamma)_s = \emptyset$. We study the characteristic of $\tau(m,N)$-srp code in the following proposition. For $L_1, L_2 \subseteq X^+$,

$$L_1^{-1}L_2 = \{x \in X^+ | L_1 x \cap L_2 \neq \emptyset\}.$$

and

$$L_2 L_1^{-1} = \{x \in X^+ | xL_1 \cap L_2 \neq \emptyset\}.$$

Proposition 4. *Let $X = \{0,1\}$ and $\gamma = \tau(m,N)$ where $m < N$. Let $L \subseteq X^+$. Then L is an $\tau(m,N)$-srp code if and only if $D^{-1}D \cap DD^{-1} = \emptyset$ where $D = \langle L\rangle_\gamma$.*

Proof. Let $X = \{0,1\}$ and $\gamma = \tau(m,N)$ where $m < N$. Let L is an $\tau(m,N)$-srp code and $D = \langle L\rangle_\gamma$. Suppose that $D^{-1}D \cap DD^{-1} \neq \emptyset$. There exists $x \in X^+$ such that $u = w_1x$ and $v = xw_2$ for some $u, v, w_1, w_2 \in D$. Since $v = xw_2$, we have $x \leq_p v \in D$. It follows that $x \in \text{Pref}(D)$. Since $u = w_1x$, we have $x \in D_s$. Thus $x \in \text{Pref}(D) \cap D_s$, a contradiction. Conversely, suppose that L is not an $\tau(m,N)$-srp code. There exists $x \in X^+$ such that $x \in \text{Pref}(D) \cap D_s$. This implies that $D^{-1}D \cap DD^{-1} \neq \emptyset$, a contradiction. Thus L is an $\tau(m,N)$-srp code.

□

Proposition 5. *Let $X = \{0,1\}$ and $\gamma = \delta(m,N)$ where $m < N$. There exist $p, q \in Z$ with $p \geq 1$ and $q \geq 0$ such that $1^{m+p}0^{m+q}$ is an $\delta(m,N)$-srp codeword.*

Proof. Let $X = \{0,1\}$ and $\gamma = \delta(m,N)$ where $m < N$. Let $L \subseteq 1^+0^+$ be an $\delta(m,N)$-srp code and $D = \langle L\rangle_\gamma$. Suppose that $1^{m+p}0^{m+q}$ is an $\delta(m,N)$-srp codeword where $p, q \in Z$ with $p \geq 1$ and $q \geq 0$. If $p \leq 0$, then we have $1^{m+p}0^{m+q}, 1^{m+p}0^{m+q-1}, 0^{m+q} \in D$. This implies that $0 \in \text{Pref}(D) \cap D_s$, a contradiction. If $q < 0$, then we have $1^{m+p}, 1^{m+p-1} \in D_s$. This implies that $1 \in \text{Pref}(D) \cap D_s$, a contradiction. Thus $1^{m+p}0^{m+q}$ is an $\delta(m,N)$-srp codeword with $p \geq 1$ and $q \geq 0$.

□

Proposition 6. *Let $X = \{0,1\}$ and $\gamma = \delta(m,N)$ where $m < N$. The language $L = \{1^{m+p}0^{m+q} | \, p \geq 1, q \geq 0\}$ is a maximal $\delta(m,N)$-srp code on 1^+0^+.*

Proof. Let $X = \{0,1\}$ and $\gamma = \delta(m,N)$ where $m < N$. It is sufficient to show that $L \cap \{w\}$ is not $\delta(m,N)$-srp code for any $w \in 1^+0^+ \setminus L$. If a word $w \in 1^+0^+ \setminus L$, then $w = 1^k, w = 0^k, w = 1^{m-p_1}0^k, w = 1^k0^{m-q_1}$ for some $k \geq 1, p_1 \geq 0, q_1 \geq 1$. We consider the following cases:

(1) $w = 1^k$. Let $L' = \{w = 1^k | k \geq 1\}$ and $D = \langle L'\rangle_\gamma$. We have $1^k, 1^{k-m} \in D$. This implies that $1 \in \text{Pref}(D) \cap D_s$, a contradiction.

(2) $w = 0^k$. This case is similar to case (1). We get $0 \in \text{Pref}(D) \cap D_s$ where $D = \langle\{w = 0^k | k \geq 1\}\rangle_\gamma$, a contradiction.

(3) $w = 1^{m-p_1}0^k$. Let $L' = \{w = 1^{m-p_1}0^k | k \geq 1, p_1 \geq 0\}$ and $D = \langle L'\rangle_\gamma$. We have $0^{k-k_1} \in D$ for some $k_1 \geq 0$. This implies that $0 \in \text{Pref}(D) \cap D_s$, a contradiction.

(4) $w = 1^k0^{m-q_1}$. Let $L' = \{w = 1^k0^{m-q_1} | k \geq 1, q_1 \geq 1\}$ and $D = \langle L'\rangle_\gamma$. We have $1^{k-k_2} \in D$ for some $k_2 \geq 0$. This implies that $1 \in \text{Pref}(D) \cap D_s$, a contradiction.

□

Acknowledgement

The authors would like to thank the referees for their careful reading of the manuscript and useful suggestions.

Conflict of Interest

The authors declare no conflict of interest

References

1. Konstantinidis, S., 1999. Structural analysis of error-correcting codes for discrete channels that involve combinations of three basic error types. *IEEE Trans. Inform. Theory, 45*(1), pp.60–77.

2. Jurgensen, H. and Konstantinidis, S., 1996. Error correction for channels with substitutions, insertions, and deletions. *Lecture Notes in Comput. Sci. 1133*, Springer-Verlag, pp.149–163.
3. Konstantinidis, S. and O'Hearn, A., 2002. Error-detecting properties of languages. *Theoretical Computer Science, 276*, pp.355–375.
4. Konstantinidis, S. and Silva, P.V., 2008. Maximal error-detecting capabilities of formal languages. *Journal of Automata, Languages and Combinatorics, 13*, pp.55–71.
5. Hsiao, H. K., Lin, H. H. and Yu, S. S., 2010. The Decodability and Correctability of Codes. *International Journal of Computer Mathematics, 87*(7), pp.1456–1468.
6. Berstel, J. and Perrin, D., 1985. *Theory of Codes*. Academic Press.