On the Success Probability of Decoding (Partial) Unit Memory Codes

SVEN PUCHINGER sven.puchinger@uni-ulm.de
SVEN MÜELICH sven.mueelich@uni-ulm.de
MARTIN BOSSERT martin.bossert@uni-ulm.de
Institute of Communications Engineering, University of Ulm, Germany

Abstract. In this paper, we derive analytic expressions for the success probability of decoding (Partial) Unit Memory codes in memoryless channels. An application of this result is that these codes outperform individual block codes in certain channels.

1 Introduction

(Partial) Unit Memory ((P)UM) codes, introduced in [7] and [6], are convolutional codes, defined using block codes. Several (P)UM code constructions and a decoder based on the underlying block codes were proposed in [2–4]. Since these publications, there have been results on improving the decoding algorithm [9], extension to rank-metric codes [10], and applications to random linear network coding [8] and the streaming scenario [5]. In these applications, the codes were evaluated numerically in probabilistic channels and it was observed that (P)UM codes often outperform individual block codes in these scenarios.

In this paper, we derive analytic expressions for the probability of successfully recovering an information block that is encoded with a (P)UM code, in memoryless channels. Using these new expressions, we are able to partly explain the numerical observations in [8] and [5] analytically.

2 (Partial) Unit Memory Codes

We use the description of (P)UM codes as in [2]. Let $k \leq n$ and $k_1 \leq \min\{k, n-k\}$ be non-negative integers. We choose matrices $G_0$ and $G_1$ of the form

$$G_0 = \begin{bmatrix} G_0^* \\ G_0^\perp \end{bmatrix}, \quad G_1 = \begin{bmatrix} G_1^* \\ 0 \end{bmatrix},$$

where the row spaces of the three matrices $G_0^*, G_1^* \in \mathbb{F}^{k_1 \times n}$ and $G_0^\perp \in \mathbb{F}^{k-k_1 \times n}$ pairwise intersect only in the zero codeword. Let $\langle G \rangle$ denote the row space of a matrix $G$. We define the following codes:

$$\mathcal{C}_\alpha := \langle \begin{bmatrix} G_0^* \\ G_0^\perp \\ G_1^* \\ G_0^\perp \end{bmatrix} \rangle, \quad \mathcal{C}_0 := \langle \begin{bmatrix} G_0^* \\ G_0^\perp \end{bmatrix} \rangle, \quad \mathcal{C}_1 := \langle \begin{bmatrix} G_1^* \\ G_0^\perp \end{bmatrix} \rangle, \quad \mathcal{C}_{01} := \langle G_0^\perp \rangle.$$
By the properties of $G_0^*, G_0^0, G_1^*$, the codes have parameters

$C_\alpha(n, k + k_1), \ C_0(n, k), \ C_1(n, k), \ C_{01}(n, k - k_1)$.

Since $C_{01} \subseteq C_1 \subseteq C_\alpha$ and $C_{01} \subseteq C_0 \subseteq C_\alpha$, the error correction capability of $C_{01}$ is typically the largest, followed by both $C_0$ and $C_1$. $C_\alpha$ is the weakest code in terms of error correction.

### 2.1 Encoding

Given the generator matrices $G_0$ and $G_1$, we encode a sequence of information vectors $\mathbf{v}_t \in \mathbb{F}^k (t = 0, \ldots, L)$, where we choose $\mathbf{i}_0 = \mathbf{i}_L = \mathbf{0}$ into a code sequence $\mathbf{c}_t = \mathbf{v}_t \cdot G_0 + \mathbf{v}_{t-1} \cdot G_1$ for $t = 1, \ldots, L$.

Note that we can re-write this relation into

$$\mathbf{c}_t = \mathbf{i}_t^* \cdot G_0^* + \mathbf{i}_t^0 \cdot G_0^0 + \mathbf{i}_{t-1}^* \cdot G_1^*.$$  (1)

The information vectors and codewords corresponding to an index $t$ are called $t$-th block. If $k < k_1$, the resulting code is called $(n, k|k_1)$ partial unit memory code since the current codeword $\mathbf{c}_t$ contains parts of the previous information word $\mathbf{i}_{t-1}$. If $k = k_1$ (note that we require $k \leq \frac{n}{2}$ in this case), the code is called $(n, k)$ unit memory code since $\mathbf{c}_t$ depends on the entire information vector $\mathbf{i}_{t-1}$ (in particular, $\mathbf{i}_{t-1}$ can be completely recovered by knowing $\mathbf{c}_t$ or $\mathbf{c}_{t-1}$).

### 2.2 Decoding

The sequence of received words is of the form

$$\mathbf{r}_t = \mathbf{c}_t + \mathbf{e}_t \quad \text{for } t = 1, \ldots, L.$$  

We choose some\(^1\) metric $d(\cdot, \cdot) : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{R}_{\geq 0}$, and the corresponding weight $\text{wt}(\cdot) = d(\cdot, \mathbf{0})$, for which we know decoders of the codes

$C_\alpha, C_0, C_1, C_{01}$

that can find all codewords with distance to the received word at most

$\tau_\alpha, \tau_0, \tau_1, \tau_{01}$,

respectively. We assume that $\tau_\alpha < \tau_0 = \tau_1 < \tau_{01}$ in this paper.\(^2\) For notational convenience, we say that $t$ errors occurred if the error word has weight $t$.

We use the description of decoding as in [4]. There, the Hamming metric in combination with bounded-minimum-distance decoders was used. However, the decoder also works with list decoders in the Hamming metric [9], with rank-metric PUM codes [10], or with erasures [5]. First, candidates for the codewords $\mathbf{c}_t$ are found in 4 steps (see below). Afterwards, the most likely sequence $\mathbf{c}_1, \ldots, \mathbf{c}_L$ is found among these candidates using the Viterbi algorithm. In this paper, we say that decoding is successful at the $t$-th position if the sent codeword $\mathbf{c}_t$ is among the candidates. Finding the candidates works in 4 steps:

\(^1\)This can e.g. be the Hamming metric as in [3] and [5], or the rank metric as in [10].

\(^2\)This is not a major restriction since most known PUM constructions, e.g. based on Reed–Solomon, BCH [3], or Gabidulin codes [10], provide codes $C_0, C_1$ of the same minimum distance.
1. Each received word $r_t = c_t + e_t$ is decoded independently using the decoder of $C_\alpha$ (note $c_t \in C_\alpha$). We can decode up to $\tau_\alpha$ errors in this step.

2. Using the information fragment $i^*_t-1$ given by a candidate codeword $c_{t-1}$, we can successfully decode the right neighbor $c_t$ in the code $C_0$ if $\text{wt}(e_t) \leq \tau_0$, using the following relation (note that the left-hand side is known)
$$r_t - i^*_t \cdot G^*_1 = i^*_t \cdot G^*_0 + i^*_t \cdot G^*_0 + e_t.$$ 

We can repeat this so-called *forward* step iteratively for all candidates.

3. Similar to Step 2, we can go in *backward* direction by decoding
$$r_t - i^*_t \cdot G^*_0 = i^*_t \cdot G^*_0 + i^*_t \cdot G^*_0 + e_t,$$
in the code $C_1$, which is successful if the number of errors is at most $\tau_1$.

4. Using $C_{01}$, we can find the $c_t$ in positions $t$, where both neighbor blocks $t-1$ and $t+1$ have been successfully decoded and $\text{wt}(e_t) \leq \tau_{01}$, using
$$r_t - i^*_t \cdot G^*_0 - i^*_t-1 \cdot G^*_1 = i^*_t \cdot G^*_0 + e_t,$$
in the code $C_{01}$.

3 New Expressions for the Success Probability

Let the PUM code and constituent decoders with decoding radii $\tau_\alpha, \tau_0, \tau_1, \tau_{01}$ be given. We assume that the error words $e_t$ are drawn i.i.d. at random according to an arbitrary distribution (memoryless channel). Let $X_1, \ldots, X_L$ be the random variables describing the error weight, i.e., $X_t := \text{wt}(e_t)$. Thus, the $X_t$ are also independently and identically distributed as some random variable $X$.

In the following, we derive an expression for the probability
$$P_t = P(i_t \text{ is found})$$
that the $t$-th information word $i_t$ of the PUM code is successfully recovered (i.e., among the candidates), only depending on the distribution of $X$ and the position $t$. The expression depends on the probabilities
$$p_a := P(0 \leq X \leq \tau_\alpha), \quad p_b := P(\tau_\alpha < X \leq \tau_0),$$
$$p_c := P(\tau_0 < X \leq \tau_{01}), \quad p_d := P(\tau_{01} < X).$$

Note that $p_a + p_b + p_c + p_d = 1$. Let $Q_t$ denote the probability that the $t$-th block is correctly decoded by Step 1 or 2 (individually or in forward direction). Similarly, by $R_t$ we define the probability that it is found by Step 1 or 3.

**Lemma 1.** For all $t = 1, \ldots, L$, we have
$$Q_t = \frac{p_a}{1-p_b} + p_b \cdot \left(\frac{1-p_a-p_b}{1-p_b}\right)$$
and
$$R_t = \frac{p_a}{1-p_b} + p_b^{L-t+1} \cdot \left(\frac{1-p_a-p_b}{1-p_b}\right).$$
Proof. We prove the claim by induction. Since the information word \( i_0 = 0 \) is known, we can directly decode the first codeword \( c_1 \) in \( C_0 \) and obtain
\[
Q_1 = P(X_1 \leq \tau_0) = p_a + p_b = \frac{p_a + p_b - p_a p_b - p_b^2}{1 - p_b} = \frac{p_a}{1 - p_b} + p_b \left( \frac{1 - p_a - p_b}{1 - p_b} \right).
\]
The probability that the \( t \)-th block is found in forward direction is given by the sum of the probability that it is found individually and the probability that Step 1 fails, but it is successfully recovered in forward direction, i.e.,
\[
Q_t = P(X_t \leq \tau_0) + P(\tau_0 < X_t \leq \tau_0) \cdot Q_{t-1}
\]
\[
= p_a + p_b \left( \frac{p_a}{1 - p_b} + p_b^{t-1} \cdot \left( \frac{1 - p_a - p_b}{1 - p_b} \right) \right) = \frac{p_a}{1 - p_b} + p_b \left( \frac{1 - p_a - p_b}{1 - p_b} \right).
\]
The proof of for \( R_t \) is equivalent using the base case \( R_L = p_a + p_b \).

\[\square\]

3.1 Partial Unit Memory Codes \((k_1 < k)\)

In the case of PUM codes, the correct information vector \( i_t \) is found if and only if \( c_t \) is found. Hence, we can state the following result.

**Theorem 1.** For any \( t = 1, \ldots, L \), we have
\[
P_t = p_a + \frac{p_a}{1 - p_b} \left[ p_b (2 - p_a - 2p_b) + p_a p_c \right] + \varepsilon(t, L),
\]
where \( \varepsilon(t, L) \geq 0 \) and \( \varepsilon(t, L) \in O(\max\{p_b^t, p_b^{L-t}\}) \) (i.e., the term \( \varepsilon(t, L) \) is negligible if \( t \) is sufficiently far away from 0 and \( L \)).

**Proof.** We can write
\[
P_t = P(i_t \text{ is found}) = P(c_t \text{ is found})
\]
\[
= P(X_t \leq \tau_0) + P(\tau_0 < X_t \leq \tau_0) \cdot \left( Q_{t-1} + R_{t+1} - Q_{t-1} R_{t+1} \right)
\]
\[
= P(\tau_0 < X_t \leq \tau_0) \cdot \left( Q_{t-1} + R_{t+1} - Q_{t-1} R_{t+1} \right)
\]
\[
= p_a + p_b \left( Q_{t-1} + R_{t+1} - Q_{t-1} R_{t+1} \right) + p_c Q_{t-1} R_{t+1}.
\]
Let \( A := \frac{p_a}{1 - p_b} \), \( B := \frac{1 - p_a - p_b}{1 - p_b} p_b^{t-1} \), and \( C := \frac{1 - p_a - p_b}{1 - p_b} p_b^{L-t} \). Then, \( A, B, C \geq 0 \) and \( B \in O(p_b^t) \) and \( C \in O(p_b^{L-t}) \). Also, \( Q_{t-1} = A + B \) and \( R_{t+1} = A + C \), so
\[
P_t = p_a + p_a \left( A + B + A + C - (A + B)(A + C) \right) + p_c (A + B)(A + C)
\]
\[
= p_a + \frac{p_a}{1 - p_b} \left[ p_b (2 - p_a - 2p_b) + p_a p_c \right] + \varepsilon(t, L),
\]
where
\[
\varepsilon(t, L) = p_b \left( B + C - AB - AC - BC \right) + p_c (AB + AC + BC) \geq 0.
\]
Since all terms depend on \( B \) or \( C \), we have \( \varepsilon(t, L) \in O(\max\{p_b^t, p_b^{L-t}\}) \).

\[\square\]
3.2 Unit Memory Codes ($k = k_1$)

Unit memory codes have the advantage that we can obtain $i_t$ from either $c_t$ or $c_{t+1}$. In UM codes, $C_{01}$ has dimension $k - k_1 = 0$, and hence, Step 4 is not useful. On the other hand, we can define $\tau_{01} := \infty$, so $p_d = 0$ and $p_c = 1 - p_a - p_b$.

**Theorem 2.** For any $t$, there is a $\delta(t, L) \geq 0$ with $\delta(t, L) \in O(\max\{p_a^L, p_b^{L-t}\})$:

$$P_t = 1 - \left(\frac{p_a}{1-p_b}\right)^2 + \delta(t, L).$$

*Proof.* We define $A, B, C$ as in the proof of Theorem 1. Then, we can write

$$p_t = Q_t + R_{t+1} - Q_tR_{t+1} = A + B + A + C + (A + B)(A + C)$$

$$= A(2 - A) + B + C - A(B + C) - BC = 1 - \left(\frac{p_a}{1-p_b}\right)^2 + \delta(t, L),$$

where $\delta(t, L)$ has the desired properties.

4 Applications

4.1 Fast Code Design

Based on the results in Section 3, it is possible to determine the failure probability of decoding a PUM code block only from the probability density function (pdf) of the error weight in a block (which is given by the channel and the block length $n$). Hence, as soon as this pdf is determined (either theoretically or numerically), one can compute the decoding failure probability for any code parameter set, i.e., variations of $k, k_1, \tau_\alpha, \tau_0, \tau_1$, and $\tau_{01}$, without the need for computationally expensive Monte-Carlo simulations. This allows to optimize code parameters (e.g., $k_1$ for given $k$) quickly.

Figure 1 shows the results of a Monte-Carlo simulation compared to the exact failure probability expressions from Section 3. As expected, the resulting curves coincide up to the estimation error of the Monte-Carlo simulation.

4.2 (P)UM Codes vs. Independent Block Codes

Let $C(n, k)$ be a linear block code with the same rate as the PUM code. For a fair comparison, we assume that decoding in $C$ is possible up to $\tau_0$ (i.e., as the decoding radius of the code $C_0$ in the PUM coding scheme). Consider a channel in which a position independently adds 1 to the error weight of the block with probability $p$ (i.e., the error weight is binomially distributed with parameters $n$ and $p$).

In this section, we show that for $p \to 0$, the failure probability of decoding (P)UM codes gets below the one of encoding/decoding each information block
Figure 1: Estimated failure probability by Monte-Carlo simulation with $10^6$ samples (solid lines) compared to the exact failure probability expressions $P_t$ from Section 3 of a $(15,5|2)$ PUM code ($\tau_\alpha = 8, \tau_0 = \tau_1 = 10, \tau_{01} = 12$) and a $(15,5)$ UM code ($\tau_\alpha = 5, \tau_0 = \tau_1 = 10$) with $L = 100$ and $t = 50$. The error weight in each block is independently binomially distributed with parameters $n = 15$ and $p$ (varying parameter).

Independently in $C$ (i.e., for a generator matrix $G$ of $C$, we have $c_t = i_t \cdot G$ for all $t$). This fact was observed before in numerical simulations, e.g., in [9] or [5], but no theoretical explanation was known. We require the following observations.

**Lemma 2** ([1, page 115]). For $\tau > pn$, we have

\[
P(X \geq \tau) \begin{cases} 
\leq \exp \left( -\tau \log \left( \frac{\tau}{n p} \right) - (n - \tau) \log \left( \frac{n - \tau}{n (1 - p)} \right) \right) \\
g \geq \frac{1}{\sqrt{2n}} \exp \left( -\tau \log \left( \frac{\tau}{n p} \right) - (n - \tau) \log \left( \frac{n - \tau}{n (1 - p)} \right) \right)
\end{cases}
\]

Lemma 2 implies that $P(X \geq \tau) \in \Theta(p^\tau (1 - p)^{n - \tau})$ when considering $n$ and $\tau$ as constants. For $p \to 0$, this means that $P(X \geq \tau) \in \Theta(p^\tau)$, which implies the following lower and upper bounds on the probabilities $p_a, \ldots, p_d$.

**Lemma 3.** For $p \to 0$, we have

\[
p_a \in \Theta(1 - p_{\tau_\alpha+1}) \quad p_b \in \Theta(p_{\tau_\alpha+1} - p_{\tau_0+1})
\]
\[
p_c \in \Theta(p_{\tau_0+1} - p_{\tau_{01}+1}) \quad p_d \in \Theta(p_{\tau_{01}+1})
\]

In the following subsection, we show that UM and PUM codes outperform decoding in the code $C$ for small values of $p$. The result is illustrated in Figure 2.
4.2.1 UM Codes

Let $P_t$ be the probability that decoding in the UM code is correct in block $t$ and let $P_{t,\text{ind}}$ be the probability that decoding in $C$ is successful.

**Theorem 3.** There is a $p' > 0$ such that $P_t > P_{t,\text{ind}}$ for all $p < p'$.

**Proof.** Since $P_t \geq 1 - \left(\frac{p_c}{1-p_b}\right)^2$ and $P_{t,\text{ind}} = p_a + p_c = 1 - p_c$, it suffices to show that $\frac{p_c}{(1-p_b)^2} < 1$ for small $p$. This directly follows from

$$\frac{p_c}{(1-p_b)^2} \in \Theta\left(\frac{p_{\alpha+1}}{1-p_{\alpha+1}}\right) = \Theta\left(p_{\alpha+1} \cdot \frac{1-p_{\alpha+1}}{1-p_{\alpha+1}}\right) \to 0 \quad (p \to 0).$$

\[\square\]

4.2.2 PUM Codes

Now, let $P_t$ be the probability that decoding in the PUM code is correct in block $t$. We obtain as similar result as for UM codes.

**Theorem 4.** There is a $p' > 0$ such that $P_t > P_{t,\text{ind}}$ for all $p < p'$.

**Proof.** By Theorem 1, we get $P_t \geq p_a + \frac{p_a}{(1-p_b)^2} [p_b(2 - p_a - 2p_b) + p_ap_c]$, so it suffices to show that $p_a + \frac{p_a}{(1-p_b)^2} [p_b(2 - p_a - 2p_b) + p_ap_c] > p_a + p_b = P_{t,\text{ind}}$ for small $p$. This condition can be reformulated into

$$\frac{p_a(p_c+p_d)^2}{p_a-p_b^2} < 1.$$

The left-hand side is

$$\frac{p_a(p_c+p_d)^2}{p_a-p_b^2} \in \Theta\left(\frac{p_{\alpha+1}^2}{p_{\alpha+1}}\right) \leq \Theta\left(p_{\alpha+2} + 1 - p_{\alpha+1}\right) \to 0 \quad (p \to 0),$$

which proves the claim. \[\square\]

4.2.3 Adaptions in the Streaming Scenario

In [5], PUM codes were used for streaming. In this scenario, in contrast to the assumption above, we do not know $i_L$ and therefore need to decode $c_L$ in $C_\alpha$ instead of $C_0$ in the first decoding step. In addition, one is interested in reconstructing $c_t$ for $t$ close to $L$ (i.e., the so-called coding delay $L - t$ should be small). In this case, $Q_t$ remains unchanged. However, $R_t$ is always smaller than $\frac{p_a}{1-p_b}$, but approaches $\frac{p_a}{1-p_b}$ exponentially in $L - t + 1$, i.e.,

$$R_t = \frac{p_a}{1-p_b} - \frac{L-t+1}{1-p_b} \to \frac{p_a}{1-p_b} \quad (L - t + 1 \to \infty).$$

This also means that for a large coding delay $L - t$, we approach the failure probability values in Theorem 1 and 2 from below, and the results in this section (Theorem 3 and 4) also hold.
Figure 2: Comparison of failure probabilities of a $(15, 5|2)$ PUM code, a $(15, 5)$ UM code, and independent encoding in $\mathcal{C}(15, 5)$, in an erasure channel with erasure probability $p$. The codes are based on MDS codes (i.e., $\tau_0 = n - k$), similar to the results in [5]. **Upper half**: Exact failure probability of the PUM, UM, and $\mathcal{C}$ code. The dashed lines indicate the value $p'$, for which $P_t > P_{t,\text{ind}}$ for all $p < p'$ for UM and PUM, respectively. **Lower half**: Upper bounds on $p_c(1 - p_c)p^n$ (cf. proof of Theorem 3) and $p_c(p_e + p_d)^n$ (cf. proof of Theorem 4) using Theorem 2. The dashed lines indicate for which $p$ these values drop below 1, providing lower bounds on $p'$.

### 4.3 Rank-Metric (P)UM Codes in Network Coding

In [10] and [8], (P)UM codes in the rank metric were used for error correction in variants of random linear network coding. It was observed numerically that (P)UM codes result in lower failure probabilities compared to independent rank-metric codes in this scenario. The results in this paper might provide a basis for an analytical explanation of this observation. Although the channel model in [8] is quite complex, it is reasonable that bounds on the tail probabilities of the error weight can be derived, resulting in similar results as in Section 4.2.
5 Conclusion

In this paper, we have derived analytic expressions for the success probability of (P)UM codes in memoryless channels and have shown applications for them. Besides the already mentioned future work, the results should be generalized—if possible—to certain channels with memory (e.g. burst channels).

Acknowledgement: This work was supported by the German Research Foundation (DFG), grant BO 867/29-3.

References

[1] R. B. Ash, Information Theory, *Dover Publications*, 1990.
[2] U. Dettmar, Partial Unit Memory Codes, _diss._, TU Darmstadt, 1994.
[3] U. Dettmar and U. Sorger, New Optimal Partial Unit Memory Codes based on Extended BCH Codes, *Electronics Letters*, _29_, 2024–2025, 1993.
[4] U. Dettmar and U. Sorger, Bounded Minimum Distance Decoding of Unit Memory Codes, *IEEE Trans. Inf. Theory*, _41_, 591–596, 1995.
[5] M. Kuijper and M. Bossert, On (Partial) Unit Memory Codes based on Reed-Solomon Codes for Streaming, in *IEEE ISIT*, 2016, 920-924.
[6] G. Lauer, Some optimal partial-unit-memory codes (Corresp.), *IEEE Trans. Inf. Theory*, _25_, 240–243, 1979.
[7] L. Lee, Short Unit-Memory Byte-oriented Binary Convolutional Codes having maximal free distance (Corresp.), *IEEE Trans. Inf. Theory*, _22_, 349–352, 1976.
[8] S. Puchinger, M. Cyran, R. F. H. Fischer, M. Bossert, J. B. Huber, Error Correction for Differential Linear Network Coding in Slowly-Varying Networks, in *ITG SCC* 2015, 1-6.
[9] S. Puchinger, A. Wachter-Zeh and M. Bossert, Improved Decoding of Partial Unit Memory Codes Using List Decoding of Reed-Solomon Codes, in *IZS*, 2014, 87-90.
[10] A. Wachter-Zeh, M. Stinner and V. Sidorenko, Convolutional Codes in Rank Metric with Application to Random Network Coding, *IEEE Trans. Inf. Theory*, _61_, 3199–3213, 2015.