Recursions for the Trapdoor Channel and an Upper Bound on its Capacity

Tobias Lutz
Institute for Communications Engineering
Technische Universität München
Munich, 80290 Germany
Email: tobi.lutz@tum.de

***Abstract*—The problem of maximizing the n-letter mutual information of the trapdoor channel is considered. It is shown that $\frac{1}{2}\log_2\left(\frac{5}{2}\right) \approx 0.6610$ bits per use is an upper bound on the capacity of the trapdoor channel. This upper bound, which is the tightest upper bound known, proves that feedback increases the capacity.**

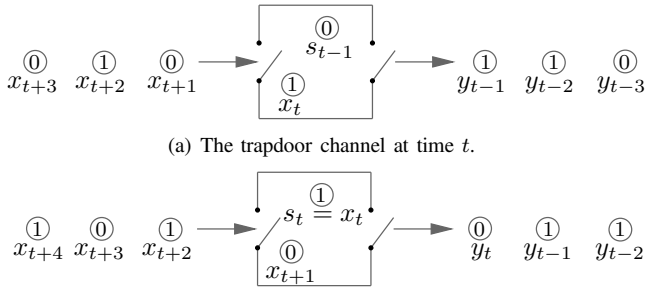
I. Introduction and Channel Model

The trapdoor channel was introduced by David Blackwell in 1961 [1] and is used by Robert Ash both as a book cover and as an introductory example for channels with memory [2]. The mapping of channel inputs to channel outputs can be described as follows. Consider a box that contains a ball that is labeled $s_0 \in \{0, 1\}$, where the index 0 refers to time 0. Both the sender and the receiver know the initial ball. In time slot 1, the sender places a new ball labeled $x_1 \in \{0, 1\}$ in the box. In the same time slot, the receiver chooses one of the two balls s_0 or x_1 at random while the other ball remains in the box. The chosen ball is interpreted as channel output y_1 at time $t = 1$ while the remaining ball becomes the channel state s_1. The same procedure is applied in every future channel use. In time slot 2, for instance, the sender places a new ball $x_2 \in \{0, 1\}$ in the box and the corresponding channel output y_2 is either x_2 or s_1. The transmission process is visualized in Fig. 1. Fig. 1(a) shows the trapdoor channel at time t when the sender places ball x_t in the box. In the same time slot, the receiver chooses randomly one of the two balls x_t or s_{t-1} as channel output, in the figure s_{t-1}. Consequently, the upcoming channel state s_t becomes x_t (see Fig. 1(b)). At time $t + 1$ the sender places a new ball x_{t+1} in the box and the receiver draws y_{t+1} from s_t and x_{t+1}. Table I depicts the probability of an output y_t given an input x_t and state s_{t-1}.

TABLE I
Transition probabilities of the trapdoor channel

x_t	s_{t-1}	$P(y_t = 0 \mid x_t, s_{t-1})$	$P(y_t = 1 \mid x_t, s_{t-1})$
0	0	1	0
0	1	0.5	0.5
1	0	0.5	0.5
1	1	0	1

Despite the simplicity of the trapdoor channel, deriving its capacity seems challenging and is an open problem. One feature that makes the problem cumbersome is that the distribution of the output symbols may depend on events



(a) The trapdoor channel at time t.

(b) The trapdoor channel at time $t + 1$. Here $y_t = s_{t-1}$.

Fig. 1. The trapdoor channel.

happening arbitrarily far back in the past since each ball has a positive probability to remain in the channel over any finite number of channel uses. Instead of maximizing $I(X;Y)$ one rather has to consider the multi-letter mutual information, i.e., $\limsup_{n\to\infty} I(\mathbf{X}^n; \mathbf{Y}^n)$.

Let $\mathbf{P}_{n|s_0}$ denote the matrix of conditional probabilities of output sequences of length n given input sequences of length n where the initial state equals s_0. The following ordering of the entries of $\mathbf{P}_{n|s_0}$ is assumed. Row indices represent input sequences and column indices represent output sequences. The (i, j)th entry of $\mathbf{P}_{n|s_0}$, indicated as $\left[\mathbf{P}_{n|s_0}\right]_{i,j}$, is the conditional probability of the binary output sequence corresponding to the integer $j - 1$ given the binary input sequence corresponding the the integer $i - 1$, $1 \le i, j \le 2^n$. For instance, if $n = 3$, then $\left[\mathbf{P}_{3|s_0}\right]_{5,3}$ denotes the conditional probability that the channel input $x_1, x_2, x_3 = 1, 0, 0$ will be mapped to the channel output $y_1, y_2, y_3 = 0, 1, 0$.

Kobayashi and Morita showed [3] that $\mathbf{P}_{n|s_0}$, $s_0 \in \{0, 1\}$, satisfies the *recursion laws*

$$\mathbf{P}_{n+1|0} = \begin{bmatrix} \mathbf{P}_{n|0} & \mathbf{0} \\ \frac{1}{2}\mathbf{P}_{n|1} & \frac{1}{2}\mathbf{P}_{n|0} \end{bmatrix} \tag{1}$$

$$\mathbf{P}_{n+1|1} = \begin{bmatrix} \frac{1}{2}\mathbf{P}_{n|1} & \frac{1}{2}\mathbf{P}_{n|0} \\ \mathbf{0} & \mathbf{P}_{n|1} \end{bmatrix} \tag{2}$$

where the initial matrices are given by $\mathbf{P}_{0|0} = \mathbf{P}_{0|1} = 1$. Ahlswede and Kaspi [4] derived the *zero-error capacity* of the trapdoor channel which equals 0.5 b/u. Permuter et al. [5] considered the trapdoor channel under the additional assumption of having a unit delay feedback link available from the receiver

978-1-4799-5186-4/14/$31.00 ©2014 IEEE

to the sender. They established that the *feedback capacity* of the trapdoor channel is equal to the logarithm of the golden ratio.

In this paper, we consider the problem of maximizing the n-letter mutual information of the trapdoor channel for any $n \in \mathbb{N}$. We relax the problem by permitting distributions that are not probability distributions. The resulting optimization problem is convex but the feasible set is larger than the probability simplex. Using the method of Lagrange multipliers via a theorem presented in [2], we show that $\frac{1}{2}\log_2\left(\frac{5}{2}\right) \approx 0.6610$ b/u is an upper bound on the capacity of the trapdoor channel. Specifically, the same absolute maximum $\frac{1}{2}\log_2\left(\frac{5}{2}\right) \approx 0.6610$ b/u results for all trapdoor channels which process input blocks of even length n. And the sequence of absolute maxima corresponding to trapdoor channels which process inputs of odd lengths converges to $\frac{1}{2}\log_2\left(\frac{5}{2}\right)$ b/u from below as the block length increases. Unfortunately, the absolute maxima of our relaxed optimization are attained outside the probability simplex. Otherwise we would have established the capacity. Nevertheless, $\frac{1}{2}\log_2\left(\frac{5}{2}\right) \approx 0.6610$ b/u is, to the best of our knowledge, the tightest capacity upper bound. Moreover, this bound is less than the feedback capacity of the trapdoor channel.

The notation used in this paper is as follows. The symbols $\mathbb{N}_0$ and $\mathbb{N}$ refer to the natural numbers with and without 0, respectively. The input corresponding to the ith row of $\mathbf{P}_{n|s_0}$ is denoted as $\mathbf{x}_i$. Further, $\mathbf{I}_n$ denotes the $2^n \times 2^n$ identity matrix, $\tilde{\mathbf{I}}_n$ is a $2^n \times 2^n$ matrix whose secondary diagonal entries are all equal to 1 while the remaining entries are all equal to 0, and $\mathbf{1}_n$ denotes a column vector of length 2^n consisting only of ones. The vector $\mathbf{1}_n^T$ is the transpose of $\mathbf{1}_n$. The functions $\exp_2(\cdot)$ and $\log_2(\cdot)$ indicate the exponential function to base 2 and the logarithm to base 2. If applied to a vector/matrix, $\log_2(\cdot)$ or $\exp_2(\cdot)$ of each element is taken and a vector/matrix results. Finally, the symbol $\circ$ refers to the Hadarmard product, i.e., the entry wise product of two matrices.

II. A Lagrange Multiplier Approach to the Trapdoor Channel

A. Problem Formulation

We derive an upper bound on the capacity of the trapdoor channel. Specifically, for any $n \in \mathbb{N}$, we find a solution to the optimization problem

$$\begin{aligned}\underset{P_{\mathbf{X}^n}}{\text{maximize}} \quad & \frac{1}{n} I\left(\mathbf{X}^n; \mathbf{Y}^n | s_0\right) \\ & = \frac{1}{n} \sum_{i=1}^{2^n} \sum_{j=1}^{2^n} p_i \left[\mathbf{P}_{n|s_0}\right]_{i,j} \log \frac{\left[\mathbf{P}_{n|s_0}\right]_{i,j}}{\sum_{k=1}^{2^n} p_k \left[\mathbf{P}_{n|s_0}\right]_{k,j}} \qquad (3)\end{aligned}$$

$$\text{subject to} \quad \sum_{i=1}^{2^n} p_i = 1 \qquad (4)$$

$$\sum_{k=1}^{2^n} p_k \left[\mathbf{P}_{n|s_0}\right]_{k,j} \geq 0 \quad \forall 1 \leq j \leq 2^n. \qquad (5)$$

Note that the pmf $P_{\mathbf{X}^n}$ represents the 2^n-sequences $(p_1, \ldots, p_{2^n})$ where p_i denotes the probability of the ith input sequence $\mathbf{x}_i$, i.e., the binary sequence corresponding to the integer $i-1$. Constraint (5) guarantees that the argument of the logarithm does not become negative. The feasible set, defined by (4) and (5), is convex. It includes the set of probability mass functions, but might be larger. To see this note that (5) is a weighted sum of all p_k where each weight $\left[\mathbf{P}_{n|s_0}\right]_{k,j}$ is non negative. Clearly, (4) and (5) are satisfied by probability distributions. However, there might exist "distributions" which involve negative values and sum up to one but still satisfy (5). Moreover, the objective function $n^{-1} I\left(\mathbf{X}^n; \mathbf{Y}^n | s_0\right)$ is concave on the set of probability distributions, which follows by using the same arguments that show that mutual information is concave on the set of input probability distributions. Consequently, the optimization problem is convex and every solution maximizes $n^{-1} I\left(\mathbf{X}^n; \mathbf{Y}^n | s_0\right)$. In the following, we use the terminology

$$C_n^{\uparrow} \stackrel{def}{=} \max_{P_{\mathbf{X}^n}} n^{-1} I\left(\mathbf{X}^n; \mathbf{Y}^n | s_0\right).$$

Taking the limit of the sequence $\left(C_n^{\uparrow}\right)_{n \in \mathbb{N}}$ as n grows, one obtains either the capacity of the trapdoor channel or an upper bound on the capacity, depending on whether the limit is attained inside or outside the set of probability distributions. Since it does not matter whether the optimization is with respect to initial state 0 or 1 (due to symmetry reasons), we do not have to distinguish between *lower capacity* and *upper capacity* [6, Chapter 4.6]

B. Using a Result from the Literature

The reason for considering (5) and not the more natural constraints $p_k \geq 0$ for all k is that a closed form solution can be obtained by applying the method of *Lagrange multipliers* to (3) and (4). As a byproduct, (5) will be automatically satisfied. In particular, setting the partial derivatives of

$$\frac{1}{n} I\left(\mathbf{X}^n; \mathbf{Y}^n | s_0\right) + \lambda \sum_{i=1}^{2^n} p_i \qquad (6)$$

with respect to each of the p_i equal to zero results in a closed form solution of the considered optimization problem.

This was done in [2, Theorem 3.3.3] for general discrete memoryless channels which are square and non singular. Note that $\mathbf{P}_{n|s_0}$ is square and non singular (see, for instance, Lemma II.2 (b)). Moreover, we assume that the channel $\mathbf{P}_{n|s_0}$ is memoryless by repeatedly using it over a large number of input blocks of length n. Consequently, $C_n^{\uparrow}$ might be an upper bound on the capacity of the channel $\mathbf{P}_{n|s_0}$. The reason is that some input blocks possibly drive the channel $\mathbf{P}_{n|s_0}$ into the opposite state $s_0 \oplus 1$, i.e., the upcoming input block would see the channel $\mathbf{P}_{n|s_0 \oplus 1}$ (whose $C_n^{\uparrow}$ is equal to $C_n^{\uparrow}$ of $\mathbf{P}_{n|s_0}$ by symmetry) but not $\mathbf{P}_{n|s_0}$. However, by assuming that the channel does not change over time, the sender always knows the channel state before a new block is transmitted. Hence, $C_n^{\uparrow}$ might be an upper bound (even though it is attained on the set of probability distributions). Nevertheless, this issue

can be ignored if n goes to infinity because in the asymptotic regime the channel $\mathbf{P}_{n|s_0}$ is used only once. Indeed we are interested in the asymptotic regime since the limit of the sequence $\left(C_n^{\uparrow}\right)_{n\in\mathbb{N}}$ is also its supremum (see Theorem II.7 and Remark II.9).

In summary, it is valid to apply [2, Theorem 3.3.3] which yields

$$C_n^{\uparrow} = \frac{1}{n}\log_2 \sum_{j=1}^{2^n} \exp_2\left(-\sum_{i=1}^{2^n}\left[\mathbf{P}_{n|s_0}^{-1}\right]_{j,i} H\left(\mathbf{Y}^n|\mathbf{X}^n=\mathbf{x}_i\right)\right) \tag{7}$$

attained at

$$p_k = 2^{-C_n^{\uparrow}} d_k, \quad k = 1,\ldots,2^n \tag{8}$$

where d_k is given by

$$\sum_{j=1}^{2^n}\left[\mathbf{P}_{n|s_0}^{-1}\right]_{j,k} \exp_2\left(-\sum_{i=1}^{2^n}\left[\mathbf{P}_{n|s_0}^{-1}\right]_{j,i} H\left(\mathbf{Y}^n|\mathbf{X}^n=\mathbf{x}_i\right)\right). \tag{9}$$

Clearly, $\left[p_1,\ldots,p_{2^n}\right]$ is a probability distribution only if $d_k \geq 0$. Observe that the Lagrangian (6) does not involve the constraint (5). However, the proof of [2, Theorem 3.3.3] shows that $\sum_{k=1}^{2^n} p_k \left[\mathbf{P}_{n|s_0}\right]_{k,j}$ equals

$$\exp\left(\lambda - \sum_{i=1}^{M}\left[\mathbf{P}_{n|s_0}^{-1}\right]_{j,i} H\left(\mathbf{Y}^n|\mathbf{X}^n=\mathbf{x}_i\right) - 1\right) \tag{10}$$

for all $1 \leq j \leq 2^n$. Hence, (5) is satisfied.

For computational reasons we write (7) in matrix vector notation, which reads

$$C_n^{\uparrow} = \frac{1}{n}\log_2\left(\mathbf{1}_n^T \exp_2\left(\mathbf{P}_{n|s_0}^{-1}\left(\mathbf{P}_{n|s_0}\circ\log_2\mathbf{P}_{n|s_0}\right)\mathbf{1}_n\right)\right) \tag{11}$$

In the remainder, we use (11) instead of (7) and we find exact numerical expressions for (11) in Theorem II.7 below.

C. Useful Recursions

In this section, we derive recursions for $-\left(\mathbf{P}_{n|s_0}\circ\log_2\mathbf{P}_{n|s_0}\right)\mathbf{1}_n$ and $\mathbf{P}_{n|s_0}^{-1}\left(\mathbf{P}_{n|s_0}\circ\log_2\mathbf{P}_{n|s_0}\right)\mathbf{1}_n$, as stated in Lemma II.4 and Lemma II.5. The recursions, interesting by themselves, are needed to prove the main result. Both expressions are defined next.

Definition II.1. *(a) The* conditional entropy vector $\mathbf{h}_{n|s_0}$ *of* $\mathbf{P}_{n|s_0}$, $s_0\in\{0,1\}$, *is*

$$\mathbf{h}_{n|s_0} \stackrel{def}{=} \left[H(\mathbf{Y}^n|\mathbf{X}^n=\mathbf{x}_1) \quad \ldots \quad H(\mathbf{Y}^n|\mathbf{X}^n=\mathbf{x}_{2^n})\right]^T \tag{12}$$

$$= -\left(\mathbf{P}_{n|s_0}\circ\log_2\mathbf{P}_{n|s_0}\right)\mathbf{1}_n \tag{13}$$

where $n\in\mathbb{N}_0$.
(b) The weighted conditional entropy vector $\boldsymbol{\omega}_{n|s_0}$ *of* $\mathbf{P}_{n|s_0}$, $s_0\in\{0,1\}$, *is*

$$\boldsymbol{\omega}_{n|s_0} \stackrel{def}{=} -\mathbf{P}_{n|s_0}^{-1}\cdot\mathbf{h}_{n|s_0} \tag{14}$$

$$= \mathbf{P}_{n|s_0}^{-1}\left(\mathbf{P}_{n|s_0}\circ\log_2\mathbf{P}_{n|s_0}\right)\mathbf{1}_n \tag{15}$$

where $n\in\mathbb{N}_0$.

We remark that $\mathbf{h}_{n|s_0}$ and $\boldsymbol{\omega}_{n|s_0}$ are column vectors with 2^n entries. The following two lemmas provide tools that we need for the proof of Lemma II.4 and Lemma II.5.

Lemma II.2. *(a) The trapdoor channel matrices* $\mathbf{P}_{2n+2|0}$ *and* $\mathbf{P}_{2n+2|1}$, $n\in\mathbb{N}_0$, *satisfy the following recursions:*

$$\mathbf{P}_{2n+2|0} = \begin{bmatrix} \mathbf{P}_{2n|0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \frac{1}{2}\mathbf{P}_{2n|1} & \frac{1}{2}\mathbf{P}_{2n|0} & \mathbf{0} & \mathbf{0} \\ \frac{1}{4}\mathbf{P}_{2n|1} & \frac{1}{4}\mathbf{P}_{2n|0} & \frac{1}{2}\mathbf{P}_{2n|0} & \mathbf{0} \\ \mathbf{0} & \frac{1}{2}\mathbf{P}_{2n|1} & \frac{1}{4}\mathbf{P}_{2n|1} & \frac{1}{4}\mathbf{P}_{2n|0} \end{bmatrix} \tag{16}$$

$$\mathbf{P}_{2n+2|1} = \begin{bmatrix} \frac{1}{4}\mathbf{P}_{2n|1} & \frac{1}{4}\mathbf{P}_{2n|0} & \frac{1}{2}\mathbf{P}_{2n|0} & \mathbf{0} \\ \mathbf{0} & \frac{1}{2}\mathbf{P}_{2n|1} & \frac{1}{4}\mathbf{P}_{2n|1} & \frac{1}{4}\mathbf{P}_{2n|0} \\ \mathbf{0} & \mathbf{0} & \frac{1}{2}\mathbf{P}_{2n|1} & \frac{1}{2}\mathbf{P}_{2n|0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}_{2n|1} \end{bmatrix}. \tag{17}$$

(b) Let $\mathbf{M}_0 \stackrel{def}{=} \mathbf{P}_{2n|0}^{-1}\mathbf{P}_{2n|1}\mathbf{P}_{2n|0}^{-1}$ *and* $\mathbf{M}_1 \stackrel{def}{=} \mathbf{P}_{2n|1}^{-1}\mathbf{P}_{2n|0}\mathbf{P}_{2n|1}^{-1}$. *The inverses of* $\mathbf{P}_{2n+2|0}$ *and* $\mathbf{P}_{2n+2|1}$, $n\in\mathbb{N}_0$, *satisfy the following recursions:*

$$\mathbf{P}_{2n+2|0}^{-1} = \begin{bmatrix} \mathbf{P}_{2n|0}^{-1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ -\mathbf{M}_0 & 2\mathbf{P}_{2n|0}^{-1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & -\mathbf{P}_{2n|0}^{-1} & 2\mathbf{P}_{2n|0}^{-1} & \mathbf{0} \\ 2\mathbf{M}_0\mathbf{P}_{2n|1}\mathbf{P}_{2n|0}^{-1} & -3\mathbf{M}_0 & -2\mathbf{M}_0 & 4\mathbf{P}_{2n|0}^{-1} \end{bmatrix} \tag{18}$$

$$\mathbf{P}_{2n+2|1}^{-1} = \begin{bmatrix} 4\mathbf{P}_{2n|1}^{-1} & -2\mathbf{M}_1 & -3\mathbf{M}_1 & 2\mathbf{M}_1\mathbf{P}_{2n|0}\mathbf{P}_{2n|1}^{-1} \\ \mathbf{0} & 2\mathbf{P}_{2n|1}^{-1} & -\mathbf{P}_{2n|1}^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 2\mathbf{P}_{2n|1}^{-1} & -\mathbf{M}_1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}_{2n|1}^{-1} \end{bmatrix}. \tag{19}$$

Proof. (a): Substituting $\mathbf{P}_{2n+1|0}$ and $\mathbf{P}_{2n+1|1}$ into $\mathbf{P}_{2n+2|0}$ and $\mathbf{P}_{2n+2|1}$, where the four matrices are expressed as in (1) and (2), yields (16) and (17).
(b): Two versions of the matrix inversion lemma are [7]

$$\begin{bmatrix}\mathbf{A} & \mathbf{0}\\ \mathbf{C} & \mathbf{D}\end{bmatrix}^{-1} = \begin{bmatrix}\mathbf{A}^{-1} & \mathbf{0}\\ -\mathbf{D}^{-1}\mathbf{C}\mathbf{A}^{-1} & \mathbf{D}^{-1}\end{bmatrix} \tag{20}$$

$$\begin{bmatrix}\mathbf{A} & \mathbf{B}\\ \mathbf{0} & \mathbf{D}\end{bmatrix}^{-1} = \begin{bmatrix}\mathbf{A}^{-1} & -\mathbf{A}^{-1}\mathbf{B}\mathbf{D}^{-1}\\ \mathbf{0} & \mathbf{D}^{-1}\end{bmatrix}. \tag{21}$$

Now divide (16) and (17) into four blocks of equal size. A twofold application of (20) and (21), first to $\mathbf{P}_{2n+2|0}$ and $\mathbf{P}_{2n+2|1}$ and, subsequently, to each of the blocks of $\mathbf{P}_{2n+2|0}$ and $\mathbf{P}_{2n+2|1}$ yields (18) and (19). □

A transformation relating $\mathbf{P}_{n|0}$ to $\mathbf{P}_{n|1}$, $\mathbf{P}_{n|0}^{-1}$ to $\mathbf{P}_{n|1}^{-1}$, $\mathbf{h}_{n|0}$ to $\mathbf{h}_{n|1}$ and $\boldsymbol{\omega}_{n|0}$ to $\boldsymbol{\omega}_{n|1}$ is derived next.

Lemma II.3. *Let* $\mathbf{P}_{n|0}$ *and* $\mathbf{P}_{n|1}$ *be trapdoor channel matrices,* $n\in\mathbb{N}_0$. *We have the following identities.*
(a)

$$\mathbf{P}_{n|1} = \tilde{\mathbf{I}}_n\mathbf{P}_{n|0}\tilde{\mathbf{I}}_n \tag{22}$$

$$\mathbf{P}_{n|0} = \tilde{\mathbf{I}}_n\mathbf{P}_{n|1}\tilde{\mathbf{I}}_n. \tag{23}$$

(b)

$$\mathbf{P}_{n|1}^{-1} = \tilde{\mathbf{I}}_n \mathbf{P}_{n|0}^{-1} \tilde{\mathbf{I}}_n \tag{24}$$

$$\mathbf{P}_{n|0}^{-1} = \tilde{\mathbf{I}}_n \mathbf{P}_{n|1}^{-1} \tilde{\mathbf{I}}_n. \tag{25}$$

(c)

$$\mathbf{h}_{n|1} = \tilde{\mathbf{I}}_n \mathbf{h}_{n|0} \tag{26}$$

$$\mathbf{h}_{n|0} = \tilde{\mathbf{I}}_n \mathbf{h}_{n|1}. \tag{27}$$

(d)

$$\boldsymbol{\omega}_{n|1} = \tilde{\mathbf{I}}_n \boldsymbol{\omega}_{n|0} \tag{28}$$

$$\boldsymbol{\omega}_{n|0} = \tilde{\mathbf{I}}_n \boldsymbol{\omega}_{n|1}. \tag{29}$$

(e) The row sums of $\mathbf{P}_{n|0}^{-1}$ *and* $\mathbf{P}_{n|1}^{-1}$ *are* 1.

Proof. See [8]. □

We can now state the recursive laws for the *conditional entropy vector* and the *weighted conditional entropy vector*.

Lemma II.4. *For* $n \geq 1$, $\mathbf{h}_{2n+2|0}$ *satisfies the recursion*

$$\mathbf{h}_{2n+2|0} = \begin{bmatrix} \mathbf{h}_{2n|0} \\ \frac{1}{2}\mathbf{h}_{2n|0} + \frac{1}{2}\tilde{\mathbf{I}}_{2n}\mathbf{h}_{2n|0} + \mathbf{1}_{2n} \\ \frac{3}{4}\mathbf{h}_{2n|0} + \frac{1}{4}\tilde{\mathbf{I}}_{2n}\mathbf{h}_{2n|0} + \frac{3}{2}\mathbf{1}_{2n} \\ \frac{1}{4}\mathbf{h}_{2n|0} + \frac{3}{4}\tilde{\mathbf{I}}_{2n}\mathbf{h}_{2n|0} + \frac{3}{2}\mathbf{1}_{2n} \end{bmatrix}. \tag{30}$$

The initial value for $n = 0$ *is given by* $\mathbf{h}_{0|0} = 0$.

Proof. See [8]. □

Lemma II.5. *(a) For* $n \in \mathbb{N}_0$, $\boldsymbol{\omega}_{2n|0}$ *satisfies the recursion*

$$\boldsymbol{\omega}_{2n+2|0} = \begin{bmatrix} \boldsymbol{\omega}_{2n|0} \\ \boldsymbol{\omega}_{2n|0} - 2 \cdot \mathbf{1}_{2n} \\ \boldsymbol{\omega}_{2n|0} - 2 \cdot \mathbf{1}_{2n} \\ \boldsymbol{\omega}_{2n|0} \end{bmatrix} \tag{31}$$

with initial value $\boldsymbol{\omega}_{0|0} = 0$.
(b) For $n \in \mathbb{N}$, $\boldsymbol{\omega}_{2n+1|0}$ *satisfies the recursion*

$$\boldsymbol{\omega}_{2n+1|0} = \begin{bmatrix} \boldsymbol{\omega}_{2n-1|0} \\ \tilde{\mathbf{I}}_{2n-1}\boldsymbol{\omega}_{2n-1|0} \\ \boldsymbol{\omega}_{2n-1|0} - 2 \cdot \mathbf{1}_{2n-1} \\ \tilde{\mathbf{I}}_{2n-1}\boldsymbol{\omega}_{2n-1|0} - 2 \cdot \mathbf{1}_{2n-1} \end{bmatrix} \tag{32}$$

with initial value $\boldsymbol{\omega}_{1|0} = \begin{bmatrix} 0 & -2 \end{bmatrix}^T$.

Proof. (a): The proof is by induction. The case $n = 0$ can be verified using Definition II.1 (b) with $P_{0|0} = P_{0|0}^{-1} = 1$. Now assume that (31) holds for some n. In order to show (31) for $n + 1$, we evaluate $\omega_{2n+2|0}$ using (15) and replacing $P_{2n+2|0}^{-1}$ and $h_{2n+2|0}$ with (18) and (30). The details of the simplification steps can be found in [8].

(b): Recall the recursions

$$\mathbf{P}_{2n+2|0} = \begin{bmatrix} \mathbf{P}_{2n+1|0} & \mathbf{0} \\ \frac{1}{2}\mathbf{P}_{2n+1|1} & \frac{1}{2}\mathbf{P}_{2n+1|0} \end{bmatrix} \tag{33}$$

$$\mathbf{P}_{2n+2|0}^{-1} = \begin{bmatrix} \mathbf{P}_{2n+1|0}^{-1} & \mathbf{0} \\ \mathbf{P}_{2n+1|0}^{-1}\mathbf{P}_{2n+1|1}\mathbf{P}_{2n+1|0}^{-1} & 2\mathbf{P}_{2n+1|0}^{-1} \end{bmatrix}, \tag{34}$$

which follow from (1) and (20). Computing the first half (i.e., the first 2^{2n+1} entries) of $\boldsymbol{\omega}_{2n+2|0}$, indicated as $\boldsymbol{\omega}_{2n+2|0}^{(1)}$, based on Definition II.1(b) and using (33) and (34) yields

$$\boldsymbol{\omega}_{2n+2|0}^{(1)} = \mathbf{P}_{2n+1|0}^{-1} \left(\mathbf{P}_{2n+1|0} \circ \log_2 \mathbf{P}_{2n+1|0} \right) \mathbf{1}_{2n+1}. \tag{35}$$

By definition, the right hand side of (35) is $\boldsymbol{\omega}_{2n+1|0}$. Hence, under consideration of (31), we have

$$\boldsymbol{\omega}_{2n+1|0} = \begin{bmatrix} \boldsymbol{\omega}_{2n|0} \\ \boldsymbol{\omega}_{2n|0} - 2 \cdot \mathbf{1}_{2n} \end{bmatrix}. \tag{36}$$

It remains to express $\boldsymbol{\omega}_{2n|0}$ in (36) in terms of $\boldsymbol{\omega}_{2n-1|0}$. By the same argument as just used, the first half of the vector $\boldsymbol{\omega}_{2n|0}$ equals $\boldsymbol{\omega}_{2n-1|0}$. Since $\boldsymbol{\omega}_{2n|0}$ is a palindrome[1] by assumption, the second half of $\boldsymbol{\omega}_{2n|0}$ equals $\tilde{\mathbf{I}}_{2n-1} \cdot \boldsymbol{\omega}_{2n-1|0}$. Hence,

$$\boldsymbol{\omega}_{2n|0} = \begin{bmatrix} \boldsymbol{\omega}_{2n-1|0} \\ \tilde{\mathbf{I}}_{2n-1} \cdot \boldsymbol{\omega}_{2n-1|0} \end{bmatrix}. \tag{37}$$

By replacing $\boldsymbol{\omega}_{2n|0}$ in (36) with (37), we obtain (32). The initial value $\boldsymbol{\omega}_1 = \begin{bmatrix} 0 & -2 \end{bmatrix}^T$ follows from (36) for $n = 0$ and noting that $\boldsymbol{\omega}_{0|0} = 0$. □

Remark II.6. *The recursions derived in Lemma II.4 and II.5 are with respect to initial state* $s_0 = 0$. *They can be transformed to recursions with respect to initial state* $s_0 = 1$ *by using (26) and (28) from Lemma II.3.*

D. Proof of the Main Result

In this section, we evaluate (11) based on Lemma II.5.

Theorem II.7. *Consider the convex optimization problem (3) to (5). The absolute maximum for input blocks of even length* $2n$ *is*

$$C_{2n}^{\uparrow} = \frac{1}{2}\log_2\left(\frac{5}{2}\right) \text{ b/u} \quad \text{for all } n \in \mathbb{N}. \tag{38}$$

For input blocks of odd length $2n - 1$, *the absolute maximum is*

$$C_{2n-1}^{\uparrow} = \frac{1}{2n-1}\left[\log_2\left(\frac{5}{4}\right) + (n-1)\cdot\log_2\left(\frac{5}{2}\right)\right] \text{ b/u} \tag{39}$$

where $n \in \mathbb{N}$.

Proof. Without loss of generality, the initial state is assumed to be $s_0 = 0$. Recall (11), which for input blocks of length $2n+k$ reads

$$C_{2n+k}^{\uparrow} = \frac{1}{2n+k}\log_2\left(\mathbf{1}_{2n+k}^T \exp_2\left(\boldsymbol{\omega}_{2n+k|0}\right)\right) \text{ b/u} \tag{40}$$

where $n \in \mathbb{N}_0$ and $k = 1, 2$. For $n = 0$, a straightforward computation shows, using (31) and (32), that $C_1^{\uparrow} = \log_2\left(\frac{5}{4}\right)$ b/u and $C_2^{\uparrow} = \frac{1}{2}\log_2\left(\frac{5}{2}\right)$ b/u. Now assume that (38) and (39) hold for some n. In particular, suppose that

$$\mathbf{1}_{2n}^T \exp_2\left(\boldsymbol{\omega}_{2n|0}\right) = \left(\frac{5}{2}\right)^n \tag{41}$$

[1] A palindrome is a finite sequence of symbols, numbers or elements, which reads the same backwards as forward.

and

$$\mathbf{1}_{2n-1}^T \exp_2\left(\boldsymbol{\omega}_{2n-1|0}\right) = \frac{5}{4}\left(\frac{5}{2}\right)^{n-1}. \tag{42}$$

We now show that (38) and (39) hold if n is replaced by $n+1$. By means of the recursions derived in Lemma II.5, we have

$$\begin{aligned}&\mathbf{1}_{2n+2}^T \exp_2\left(\boldsymbol{\omega}_{2n+2|0}\right)\\ &= \mathbf{1}_{2n}^T\left[2\exp_2\left(\boldsymbol{\omega}_{2n|0}\right) + 2\exp_2\left(\boldsymbol{\omega}_{2n|0} - 2\cdot\mathbf{1}_{2n}\right)\right]\\ &= \left(2+2\cdot 2^{-2}\right)\mathbf{1}_{2n}^T \exp_2\left(\boldsymbol{\omega}_{2n|0}\right)\end{aligned} \tag{43}$$

and

$$\begin{aligned}&\mathbf{1}_{2n+1}^T \exp_2\left(\boldsymbol{\omega}_{2n+1|0}\right)\\ &= \mathbf{1}_{2n-1}^T\left[2\exp_2\left(\boldsymbol{\omega}_{2n-1|0}\right) + 2\exp_2\left(\boldsymbol{\omega}_{2n-1|0} - 2\cdot\mathbf{1}_{2n}\right)\right]\end{aligned} \tag{44}$$

$$= \left(2+2\cdot 2^{-2}\right)\mathbf{1}_{2n-1}^T \exp_2\left(\boldsymbol{\omega}_{2n-1|0}\right). \tag{45}$$

Observe that we used the property

$$\mathbf{1}_{2n-1}^T \exp_2\left(\tilde{\mathbf{I}}_{2n-1}\boldsymbol{\omega}_{2n-1|0}\right) = \mathbf{1}_{2n-1}^T \exp_2\left(\boldsymbol{\omega}_{2n-1|0}\right)$$

in (44). Finally, using (40) under consideration of (43) and (45) and the induction hypotheses (41) and (42), we obtain

$$\begin{aligned}C_{2n+2}^{\uparrow} &= \frac{1}{2n+2}\log_2\left(\left(2+2\cdot 2^{-2}\right)\mathbf{1}_{2n}^T \exp_2\left(\boldsymbol{\omega}_{2n|0}\right)\right)\\ &= \frac{1}{2}\log_2\left(\frac{5}{2}\right) \text{ b/u}\end{aligned}$$

and

$$\begin{aligned}C_{2n+1}^{\uparrow} &= \frac{1}{2n+1}\log_2\left(\left(2+2\cdot 2^{-2}\right)\mathbf{1}_{2n-1}^T \exp_2\left(\boldsymbol{\omega}_{2n-1|0}\right)\right)\\ &= \frac{1}{2n+1}\left[\log_2\left(\frac{5}{4}\right) + n\cdot\log_2\left(\frac{5}{2}\right)\right] \text{ b/u.}\end{aligned}$$

□

Remark II.8. *Observe that* $\lim_{n\to\infty} C_{2n+1}^{\uparrow} = \frac{1}{2}\log_2\left(\frac{5}{2}\right)$*, where convergence is from below. Hence, we have*

$$\max_{n\in\mathbb{N}} C_n^{\uparrow} = \frac{1}{2}\log_2\left(\frac{5}{2}\right) \text{ b/u.}$$

Unfortunately, the distributions corresponding to (38) and (39) involve negative "probabilities" – otherwise the capacity of the trapdoor channel would have been established. We elaborate this issue in the following remark.

Remark II.9. *Note that condition (9) does not hold for all* $k = 1, \ldots, 2^n$*. This can be verified as follows. For a trapdoor channel* $\mathbf{P}_{n|0}$*, condition (9) reads in matrix vector notation as*

$$\left[d_k\right]_{1\le k\le 2^n} = \left(\mathbf{P}_{n|0}^{-1}\right)^T \exp_2\left(\boldsymbol{\omega}_n\right). \tag{46}$$

We now compute the second last row of $\left(\mathbf{P}_{n|0}^{-1}\right)^T$ *by the following recursive scheme. Applying the matrix inversion lemma in the form of (20) to* $\mathbf{P}_{n|0}$*, which is written as in (1), and subsequently taking the transpose, then replacing the right bottom block of this matrix, which is* $2\left(\mathbf{P}_{n-1|0}^{-1}\right)^T$*, with the just obtained matrix times two (where* $n-1$ *is replaced by* $n-2$*), then applying the same procedure to the right bottom block of* $2\left(\mathbf{P}_{n-1|0}^{-1}\right)^T$ *and so on until the right bottom block equals* $2^{n-1}\left(\mathbf{P}_{1|0}^{-1}\right)^T$ *shows that the second last row of* $\left(\mathbf{P}_{n|0}^{-1}\right)^T$ *equals* $\begin{bmatrix}0 & \cdots & 0 & 2^{n-1} & -2^{n-1}\end{bmatrix}$*. Further, using Lemma II.5, it follows that the second to last entry and the last entry of* $\boldsymbol{\omega}_n$ *equals* -2 *and* 0 *if* $n \in \mathbb{N}$ *is even, and* -4 *and* -2 *if* $n \in \mathbb{N}$ *is odd. Inserting the gathered quantities into (46) yields*

$$d_{2^n-1} = \begin{cases} -3\cdot 2^{n-3} & \text{if } n \text{ is even}\\ -3\cdot 2^{n-5} & \text{if } n \text{ is odd.}\end{cases}$$

Hence, condition (9) does not hold for all $k = 1, \ldots, 2^n$*.*

III. Conclusions

We have focused on the convex optimization problem (3) to (5) where the feasible set is larger than the probability simplex. An absolute maximum of the n-letter mutual information was established for any $n \in \mathbb{N}$ by using the method of Lagrange multipliers. The same absolute maximum $\frac{1}{2}\log_2\left(\frac{5}{2}\right) \approx 0.6610$ b/u results for all even n and the sequence of absolute maxima corresponding to odd block lengths converges from below to $\frac{1}{2}\log_2\left(\frac{5}{2}\right)$ b/u as the block length increases. Unfortunately, all absolute maxima are attained outside the probability simplex. Hence, instead of establishing the capacity of the trapdoor channel, we have shown only that $\frac{1}{2}\log_2\left(\frac{5}{2}\right)$ b/u is an upper bound on the capacity. To the best of our knowledge, this upper bound is the tightest known bound. Notably, this upper bound is strictly smaller than the feedback capacity [5]. Moreover, the result gives an indirect justification that the capacity of the trapdoor channel is attained on the boundary of the probability simplex.

Acknowledgment

The author is supported by the German Ministry of Education and Research in the framework of the Alexander von Humboldt-Professorship and would like to thank Prof. Haim Permuter who suggested to use [2, Theorem 3.3.3]. Moreover, the author wishes to thank Prof. Gerhard Kramer and Prof. Tsachy Weissman for helpful discussions.

References

[1] D. Blackwell, *Information Theory*, E. F. Beckenbach, Ed. McGraw-Hill Book Co., New York, 1961, vol. Modern Mathematics for the Engineer.
[2] R. Ash, *Information Theory*. Interscience Publishers, 1965.
[3] K. Kobayashi and H. Morita, "An input/output recursion for the trapdoor channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Lausanne, Switzerland, Jun. 30–Jul. 5 2002, p. 423.
[4] R. Ahlswede and A. H. Kaspi, "Optimal coding strategies for certain permuting channels." *IEEE Trans. Inf. Theory*, vol. 33, no. 3, pp. 310–314, 1987.
[5] H. Permuter, P. Cuff, B. Van Roy, and T. Weissman, "Capacity of the trapdoor channel with feedback," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3150–3165, Jul. 2008.
[6] R. G. Gallager, *Information Theory and Reliable Communication*. John Wiley & Sons, Inc., 1968.
[7] G. H. Golub and C. F. van Van Loan, *Matrix Computations*, 3rd ed. The Johns Hopkins University Press, 1996.
[8] T. Lutz, "Various views on the trapdoor channel and an upper bound on its capacity," 2014, available online: http://arxiv.org/abs/1401.4575.