# Block Symmetry in Discrete Memoryless Channels 

Jakob Bøje Pedersen<br>Frederiksborg Gymnasium<br>Hillerød<br>Denmark<br>e-mail: jakobbp@worldonline.dk

Flemming Topsøe ${ }^{1}$<br>Department of Mathematics<br>University of Copenhagen Denmark.<br>e-mail: topsoe@math.ku.dk

Abstract - Notions of block symmetry for discrete, memoryless channels are introduced. The results deal with capacity and optimal distributions and appear to be simple and natural ones which somehow were overlooked or not considered in the early development of information theory.

## I. Preview

Let $\mathbf{P}$ be the transition matrix for a discrete memoryless channel (DMC) and consider a block decomposition $\left(\mathbf{P}^{i j}\right)_{i, j}$ of $\mathbf{P}$ as indicated in the figure. Such a decomposition is induced by two decompositions - or equivalence relations - one of the input-, the other of the output alphabet. Assume that, within each block $\mathbf{P}^{i j}$, all row sums are equal and also that all column sums are equal. Assume further, that rows in the full matrix $\mathbf{P}$ which correspond to equivalent input letters have equal entropy. Then there exists an optimal input distribution - i.e. one for which the transmission rate reaches capacity - which is consistent with the decomposition of the input alphabet in the sense that equivalent input letters are sent with equal probability. The optimal output distribution is consistent in a similar way. This is the key result, stated in detail in Theorem 2.


## II. DMC's with Benefit

Let $\mathbf{P}=\left(p_{x y}\right)_{x \in X, y \in Y}$ be a stochastic matrix, fixed in the sequal. We view $\mathbf{P}$ as the transition matrix of a DMC. The sets $X$ and $Y$, the input- and output alphabets, are assumed to be finite. For $x \in X, \vec{q}_{x}$ denotes the $x$ 'th row vector in $\mathbf{P}$. An input distribution is a distribution $\vec{p}=\left(p_{x}\right)_{x \in X}$ over $X$. The induced output distribution is the mixture $\vec{q}=\sum p_{x} \vec{q}_{x}$. The information transmission rate $I(\vec{p})$ can be expressed, using " D " for Kullback-Leibler divergence, as

$$
\begin{equation*}
I(\vec{p})=\sum_{x \in X} p_{x} D\left(\vec{q}_{x} \| \vec{q}\right) \tag{1}
\end{equation*}
$$

[^0]We need a refined notion of capacity, which allows that the sending of an input symbol may be associated with a certain benefit. This idea, and the basic result connected with it, has been considered before, cf. Blahut [2, Theorem 9], where it was found more natural to associate a "cost" with the transmission of an input symbol. Consider a benefit function a : $x \curvearrowright a_{x}$ which maps $X$ into the reals, and define the modified capacity with benefit a, by

$$
\begin{equation*}
C(\mathbf{P} ; \mathbf{a})=\sup _{\vec{p}}(I(\vec{p})+\langle\mathbf{a}, \vec{p}\rangle) . \tag{2}
\end{equation*}
$$

The bracket notation indicates mean value: $\langle\mathbf{a}, \vec{p}\rangle=$ $\sum_{x} p_{x} a_{x}$. Clearly, the supremum in (2) is attained, and we are led to consider optimal input- and output distributions for the modified problem.

Theorem 1 (Kuhn-Tucker conditions). Let $\vec{p}^{*}$ be an input distribution and $\vec{q}^{*}$ the induced output distribution. A necessary and sufficient condition that $\vec{p}^{*}$ be optimal for the modified problem with benefit a is that, for some constant $C$, the following two conditions hold:

$$
\begin{align*}
& D\left(\vec{q}_{x} \| \vec{q}^{*}\right)+a_{x} \leq C \text { for all } x  \tag{3}\\
& D\left(\vec{q}_{x} \| \vec{q}^{*}\right)+a_{x}=C \text { for all } x \text { with } p_{x}^{*}>0 . \tag{4}
\end{align*}
$$

If these conditions are satisfied, $C=C(\mathbf{P} ; \mathbf{a})$.
Proof. We present a simple proof based on [8]. First assume that (3) and (4) hold. Employ the identity ${ }^{1}$

$$
I(\vec{p})+D\left(\vec{q} \| \vec{q}^{*}\right)=\sum_{x \in X} p_{x} D\left(\vec{q}_{x} \| \vec{q}^{*}\right)
$$

valid for any input distribution $\vec{p}$ with induced output distribution $\vec{q}$, to conclude that for any such $\vec{p}$,

$$
I(\vec{p})+\langle\mathbf{a}, \vec{p}\rangle \leq \sum_{x \in X} p_{x}\left(D\left(\vec{q}_{x} \| \vec{q}^{*}\right)+a_{x}\right) \leq C
$$

It readily follows that $C(\mathbf{P} ; \mathbf{a})=I\left(\vec{p}^{*}\right)+\left\langle\mathbf{a}, \vec{p}^{*}\right\rangle$.
To prove necessity, assume that the stated conditions fail. Denote the left hand side of (3) by $K_{x}$. Choose $x_{0}$ with $K_{x_{0}}$ maximal. Then

$$
\begin{equation*}
K_{x_{0}}>\sum_{x \in X} p_{x}^{*} K_{x} . \tag{5}
\end{equation*}
$$

[^1]For $0 \leq \varepsilon \leq 1$, put $\vec{p}_{\varepsilon}=(1-\varepsilon) \vec{p}^{*}+\varepsilon \vec{p}_{x_{0}}$ with $\vec{p}_{x_{0}}$ representing a unit mass at $x_{0}$. Let $\vec{q}_{\varepsilon}$ be the distribution induced by $\vec{p}_{\varepsilon}$. Then, by the compensation identity,

$$
(1-\varepsilon) I\left(\vec{p}^{*}\right)+(1-\varepsilon) D\left(\vec{q}^{*} \| \vec{q}_{\varepsilon}\right)+\varepsilon D\left(\vec{q}_{x_{0}} \| \vec{q}_{\varepsilon}\right)=I\left(\vec{p}_{\varepsilon}\right)
$$

Writing $I\left(\vec{p}^{*}\right)+\left\langle\mathbf{a}, \vec{p}^{*}\right\rangle$ as $\sum p_{x}^{*} K_{x}$, it follows from this that $I\left(\vec{p}_{\varepsilon}\right)+\left\langle\mathbf{a}, \vec{p}_{\varepsilon}\right\rangle$ is lower bounded by

$$
\sum_{x \in X} p_{x}^{*} K_{x}+\varepsilon\left(D\left(\vec{q}_{x_{0}} \| \vec{q}_{\varepsilon}\right)+a_{x_{0}}-\sum_{x \in X} p_{x}^{*} K_{x}\right)
$$

By (5) and lower semi-continuity of divergence, it follows that for $\varepsilon$ sufficiently small, but positive, $I\left(\vec{p}_{\varepsilon}\right)+$ $\left\langle\mathbf{a}, \vec{p}_{\varepsilon}\right\rangle$ is strictly larger than $I\left(\vec{p}^{*}\right)+\left\langle\mathbf{a}, \vec{p}^{*}\right\rangle$, hence $\vec{p}^{*}$ is not optimal.

Though some parts of the proof can be modified to cover cases with $X$ or $Y$ infinite, care has to be taken for several reasons, e.g. there may be no optimal distribution at all (consider $\mathbf{P}$ with rows $\left.(1,0),\left(\frac{1}{2}, \frac{1}{2}\right),\left(\frac{1}{4}, \frac{3}{4}\right), \cdots\right)$.

Every input distribution $\vec{p}^{*}$ with all $p_{x}^{*}$ positive is optimal for the modified problem for some choice of benefit function. Indeed, with benefits $a_{x}=-D\left(\vec{q}_{x} \| \vec{q}^{*}\right), \vec{p}^{*}$ is optimal and the modified capacity is 0 . In this setting, it is more natural to consider $D\left(\vec{q}_{x} \| \vec{q}^{*}\right)$ as a cost associated with the transmission of $x$. This remark illuminates the very definition of optimal distributions.

Whereas there may be several optimal input distributions, the optimal output distribution is unique, as in the case with zero benefit. This follows by concavity of $\vec{p} \curvearrowright I(\vec{p})+\langle\mathbf{a}, \vec{p}\rangle$.

Explicit formulas for the calculation of optimal distributions and modified capacity do not exist in general, and even when they do, they become complicated. In the appendix we develop formulas pertaining to a $2 \times 2$ matrix.

## III. The Basic Result

For any set $W, \operatorname{DEC}(W)$ denotes the set of decompositions of $W$, ordered by subdecomposition. Put $Z=X \times Y$ corresponding to given finite sets $X$ and $Y$. A block decomposition of $Z$ is a decomposition of the form $\eta_{X} \times \eta_{Y}=$ $\left\{A \times B \mid A \in \eta_{X}, B \in \eta_{Y}\right\}$ with $\eta_{X} \in \operatorname{DEC}(X)$, and $\eta_{Y} \in \operatorname{DEC}(Y)$. A set $A \times B \in \eta_{X} \times \eta_{Y}$ is called a block of the decomposition. The set of block decompositions of $Z$ is denoted $\operatorname{BDE}(Z)$.

Consider $\eta=\eta_{X} \times \eta_{Y} \in \operatorname{BDE}(Z)$, to be fixed from now on. As $\eta$ is seen in conjunction with $\mathbf{P}$, we write $\eta \in \operatorname{BDE}(\mathbf{P})$. The number of classes in $\eta_{X}$ and $\eta_{Y}$ are denoted by $M$, respectively $N$. We put $\eta_{X}=\left\{X_{i} \mid i \leq\right.$ $M\}$ and $\eta_{Y}=\left\{Y_{j} \mid j \leq N\right\}$. We denote by $\mathbf{P}^{i j}$ the $i j$ 'th block in $\mathbf{P}$, i.e. $\mathbf{P}^{i j}=\left(p_{x y}\right)_{x \in X_{i}, j \in Y_{j}}$. We write $\eta \in \operatorname{BDE}\left(\mathbf{P} ; \sigma_{-}\right)$if, within each block $\mathbf{P}^{i j}$, the row sums are equal, say $=\sigma_{-}^{i j}$. If $\eta \in \operatorname{BDE}\left(\mathbf{P} ; \sigma_{-}\right)$, we define the derived DMC as the DMC with transition matrix $\partial_{\eta} \mathbf{P}=$ $\left(\sigma_{-}^{i j}\right)_{i \leq M, j \leq N}$ and we denote the $i^{\prime}$ th row in $\partial_{\eta} \mathbf{P}$ by $\vec{\sigma}_{i}$. We write $\eta \in \operatorname{BDE}\left(\mathbf{P} ; \sigma_{+}\right)$if $\eta \in \operatorname{BDE}\left(\mathbf{P} ; \sigma_{-}\right)$and if,
within each block $\mathbf{P}^{i j}$, the column sums are equal, say $=\sigma_{1}^{i j}$.

We denote by $m_{i}\left(n_{j}\right)$ the number of elements in $X_{i}$ $\left(Y_{j}\right)$ and by $\vec{u}^{i}\left(\vec{v}^{j}\right)$ the uniform distribution over $X_{i}\left(Y_{j}\right)$. As indicated in section I, a consistent (or $\eta$-consistent) input distribution is a distribution $\vec{p}$ for which, given $i \leq M$, $p_{x}$ is independent of $x \in X_{i}$. Clearly, an input distribution $\vec{p}$ is consistent if and only if it is a convex combination $\vec{p}=\sum_{i \leq M} \alpha_{i} \vec{u}^{i}$ of the $\vec{u}^{i}$. Similarly, we consider consistent output distributions which are convex combinations of the form $\vec{q}=\sum_{j \leq N} \beta_{j} \vec{v}^{j}$.
Lemma 1. Assume that $\eta \in \operatorname{BDE}\left(\mathbf{P} ; \sigma_{+}\right)$. Let $\vec{p}=$ $\sum_{i \leq M} \alpha_{i} \vec{u}^{i}$ be a consistent input distribution and $\vec{q}$ the induced output distribution. Let $\vec{\beta}=\left(\beta_{j}\right)_{j \leq N}$ be the output distribution for $\partial_{\eta} \mathbf{P}$ induced by $\vec{\alpha}=\left(\alpha_{i}\right)_{i \leq M}$. Then $\vec{q}=\sum_{j \leq N} \beta_{j} \vec{v}^{j}$. In particular, $\vec{q}$ is consistent.
Proof. This follows by simple computation, relying also on the relation $n_{j} \sigma_{1}^{i j}=m_{i} \sigma_{-}^{i j}$.

The connection between $\mathbf{P}$ and $\partial_{\eta} \mathbf{P}$ will be further exploited. For this we strengthen the conditions on $\eta$. We say that $\eta$ is a generalized block symmetric decomposition, and write $\eta \in \operatorname{GBSD}(\mathbf{P})$, if $\eta \in \operatorname{BDE}\left(\mathbf{P} ; \sigma_{+}\right)$and if, for each $i \leq M, H\left(\vec{q}_{x}\right)$ is independent of $x$ for $x \in X_{i}$.

For each $x \in X$ we consider the $\eta_{Y}-$ conditional divergence of $\vec{q}_{x}$ w.r.t. $\left(\vec{v}^{j}\right)_{j \leq N}$, a quantity defined by first determining $i$ such that $x \in X_{i}$ and then setting

$$
\begin{equation*}
D^{\eta}\left(\vec{q}_{x} \| \cdot\right)=\sum_{j \leq N} \sigma_{-}^{i j} D\left(\vec{q}_{x} \mid Y_{j} \| \vec{v}^{j}\right) \tag{6}
\end{equation*}
$$

with $\vec{q}_{x} \mid Y_{j}$ the usual conditional distribution of $\vec{q}_{x}$ given $Y_{j}$. If the output distribution $\vec{q}$ is consistent, say $\vec{q}=$ $\sum_{j \leq N} \beta_{j} \vec{v}_{j}$ then, by a simple datareduction identity,

$$
\begin{equation*}
D\left(\vec{q}_{x} \| \vec{q}\right)=D\left(\vec{\sigma}_{i} \| \vec{\beta}\right)+D^{\eta}\left(\vec{q}_{x} \| \cdot\right) . \tag{7}
\end{equation*}
$$

Here, we still assume that $x \in X_{i}$. For more on identities like (7), see [9]. We can now state the main result.
Theorem 2. Assume that $\eta \in \operatorname{BDE}\left(\mathbf{P} ; \sigma_{+}\right)$.
(i). If $\eta \in \operatorname{GBSD}(\mathbf{P})$, there exists an optimal consistent input distribution. In this case, $a_{i}=D^{\eta}\left(\vec{q}_{x} \| \cdot\right)$ is independent of $x$ for $x \in X_{i}$ and $C(\mathbf{P})=C\left(\partial_{\eta} \mathbf{P} ; \mathbf{a}\right)$ with benefit vector $\mathbf{a}=\left(a_{i}\right)_{i \leq M}$.
(ii). If an optimal consistent input distribution exists with all point probabilities positive, then $\eta \in \operatorname{GBSD}(\mathbf{P})$.
Proof. (i) follows by Theorem 1 (applied both to $\mathbf{P}$ without benefit and to $\partial_{\eta} \mathbf{P}$ with benefit $\mathbf{a}$ ) in conjunction with Lemma 1 and (7).

To prove (ii) let $\vec{p}$ be an optimal consistent input distribution with positive point probabilities and let $\vec{q}=$ $\sum_{j \leq N} \beta_{j} \vec{v}^{j}$ be the induced output distribution. By Theorem $1, D\left(\vec{q}_{x} \| \vec{q}\right)$ is indepent of $x$. By (7), $D^{\eta}\left(\vec{q}_{x} \| \cdot\right)$ is independent of $x$ when restricting $x$ to a class $X_{i}$. As

$$
D^{\eta}\left(\vec{q}_{x} \| \cdot\right)=-H\left(\vec{q}_{x}\right)+\sum_{j \leq N} \sigma_{-}^{i j} \log \frac{n_{j}}{\sigma_{-}^{i j}}
$$

it follows that $H\left(\vec{q}_{x}\right)$ is independent of $x$ for $x \in X_{i}$.

It is a bit surprising that the condition of equal entropies for the $\vec{p}_{i}$ 's plays a central role. It does not have much of the flavour of a symmetry condition. Previous results work with stronger but more "clean" conditions of symmetry. Such notions were studied already by Shannon, cf. [6, Sections 15 and 16] and appear in most textbooks. For our purposes, a matrix is called weakly symmetric if the rows are permutations of each other and if all column sums are equal. This terminology is in consistency with Cover and Thomas [3, p. 190]. We call $\eta$ a block symmetric decomposition of $\mathbf{P}$ if all blocks $\mathbf{P}^{i j}$ are weakly symmetric. Notationally we write $\eta \in \operatorname{BSD}(\mathbf{P})$. Clearly, if $\eta \in \operatorname{BSD}(\mathbf{P})$, then $\eta \in \operatorname{GBSD}(\mathbf{P})$, hence:

Corollary 1. If $\eta \in \operatorname{BSD}(\mathbf{P})$, there exist consistent optimal input- and output distributions.

The case $M=N=1$ is dealt with in [3]. In Gallager [4, p. 94] one finds a variant of the corollary corresponding to the case $M=1, N$ arbitrary, though there with the stronger requirement of equal columns modulo permutations.

Example 1. Theorem 2 is stronger than Corollary 1. This is seen from the example of the $10 \times 5$ matrix $\mathbf{P}$ which is $\frac{1}{8}$ times the transpose of the matrix

$$
\left(\begin{array}{llllllllll}
1 & 1 & 1 & 1 & 4 & 2 & 2 & 2 & 2 & 0 \\
1 & 1 & 1 & 4 & 1 & 2 & 2 & 2 & 0 & 2 \\
1 & 1 & 4 & 1 & 1 & 2 & 2 & 0 & 2 & 2 \\
1 & 4 & 1 & 1 & 1 & 2 & 0 & 2 & 2 & 2 \\
4 & 1 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 2
\end{array}\right)
$$

By Theorem 2, the uniform distribution $\left(\frac{1}{10}, \cdots, \frac{1}{10}\right)$ is an optimal input distribution. This result is not covered by a direct application of Corollary 1, but could have been obtained by two successive applications of the corollary. Possibly, this kind of iterative procedure can be applied more generally. A complete answer to the questions this raises will contain the characterization of channels with the uniform distribution as an optimal input distribution. Even the simple case of a binary channel is not entirely trivial. ${ }^{2}$

## IV. Coarsest decompositions, symmetry profiles

Theorem 2 may not be all that informative. For instance, in case $\eta$ is the finest block symmetric decomposition (consisting of singletons), it contains no information. The coarser $\eta$ is, the more informative is the result. It is

[^2]important that, given any DMC P , a coarsest block symmetric decomposition exists. Moreover, there is a simple algorithm to determine this most informative block symmetric decomposition. A similar result does not hold for the generalized notion of block symmetry.

Theorem 3. Any $D M C \mathbf{P}=\left(p_{x y}\right)_{x \in X, y \in Y}$ has a coarsest block symmetric decomposition.

Proof. The key point is to show that $\operatorname{BSD}(\mathbf{P})$ is closed under the lattice operation $\wedge .{ }^{3}$

Assume that $\eta^{\prime}=\eta_{X}^{\prime} \times \eta_{Y}^{\prime}$ and $\eta^{\prime \prime}=\eta_{X}^{\prime \prime} \times \eta_{Y}^{\prime \prime}$ are in $\operatorname{BSD}(\mathbf{P})$ and put $\eta=\eta^{\prime} \wedge \eta^{\prime \prime}=\eta_{X} \times \eta_{Y}$, say. Consider an $\eta$-class $A \times B$ and let $\mathbf{Q}=\left(p_{x y}\right)_{x \in A, y \in B}$. We shall show that $\mathbf{Q}$ is weakly symmetric. This involves a condition on the rows and a condition on the columns in $\mathbf{Q}$. Consider first the rows.

As $\eta_{X}=\eta_{X}^{\prime} \wedge \eta_{x}^{\prime \prime}$, we can pass from one element of $A$ to another by a finite number of equivalences, each one being either under $\eta_{X}^{\prime}$ (denoted $\equiv^{\prime}$ ) or under $\eta_{X}^{\prime \prime}$ (denoted $\equiv^{\prime \prime}$ ). Note that if $a_{1}, a_{2} \in A$ and $a_{1} \equiv^{\prime} a_{2}$, then the $a_{1}$-row and the $a_{2}$-row of $\mathbf{Q}$ are decomposed into parts corresponding to the decomposition of $B$ into $\eta_{Y}^{\prime}$-classes. Mutually, these parts are permutations of each other. Then so are the $a_{1-}$ and $a_{2}$ rows of $\mathbf{Q}$. A similar argument applies if $a_{1} \equiv{ }^{\prime \prime} a_{2}$. Applying this reasoning a finite number of times, we conclude that the rows in $\mathbf{Q}$ are indeed permutations of each other.

A similar analysis applied to the columns of $\mathbf{Q}$ show that the corresponding column sums are equal.

We conclude, that each $\eta$-block $\mathbf{Q}$ of $\mathbf{P}$ is weakly symmetric, hence $\eta \in \operatorname{BSD}(\mathbf{P})$.

Theorem 3 gives rise to the following concept. Consider a map $\tau$ which, to every stochastic matrix $\mathbf{P}$, associates a subset $\tau(\mathbf{P})$ of $\operatorname{BDE}(\mathbf{P})$. We use the notation $\eta_{\tau}(\mathbf{P})$ to denote the coarsest decomposition in $\tau(\mathbf{P})$, provided this is well defined. We call $\eta_{\tau}(\mathbf{P})$ the $\tau$-profile of $\mathbf{P}$. In this terminology, Theorem 3 asserts that the BSD-profile exists for every $\mathbf{P}$. We write $\eta_{\alpha}(\mathbf{P})$ for $\eta_{\mathrm{BSD}}(\mathbf{P})$. The strong symmetry profile of $\mathbf{P}$, denoted $\eta_{\beta}(\mathbf{P})$, is defined as the profile corresponding to the subset $\operatorname{SBS}(\mathbf{P})$ of strong block symmetric decomposition of $\mathbf{P}$. This set consists of $\eta \in \operatorname{BDE}(\mathbf{P})$ such that, for each $\eta$-block of $\mathbf{P}$, not only the rows, but also the columns are permutations of each other. Applying the same technique as in the proof above, we see that also $\eta_{\beta}(\mathbf{P})$ exists for every $\mathbf{P}$. We always have $\eta_{\alpha}(\mathbf{P}) \leq \eta_{\beta}(\mathbf{P})$. In general, the profiles are different. ${ }^{4}$

It lies nearby to ask for an effective algorithm which determines $\eta_{\alpha}(\mathbf{P})$. In fact, such an algorithm exists. ${ }^{5}$ Briefly, this works as follows. Firstly, $\eta_{1} \in \operatorname{BDE}(\mathbf{P})$ is constructed corresponding to the two equivalence relations "corresponding rows in $\mathbf{P}$ are permutations of each

[^3]other", and, "corresponding column sums in $\mathbf{P}$ are equal". Each of the $\eta_{1}$-blocks of $\mathbf{P}$ are then handled one by one in a similar way. Each step introduces a block decomposition of $\mathbf{P}$, finer than the previous one. The process continues until no block gives rise to a finer decomposition. A finite sequence $0 \leq \eta_{1} \leq \eta_{2} \leq \cdots \leq \eta_{k}$ is then constructed with $\eta_{k}=\eta_{\alpha}(\mathbf{P})$. The algorithm needs approximately $\nu^{3} \log \nu$ steps where $\nu=\max (m, n)$.

## V. Discussion

Theorem 2 reduces the problem to determine capacity and optimal distributions from $\mathbf{P}$ to $\partial_{\eta} \mathbf{P}$ (e.g. with $\left.\eta=\eta_{\alpha}(\mathbf{P})\right)$. However, the reduced problem cannot, in general, be solved in closed form. One often has to turn to numerical methods, and here, the Arimoto-Blahut algorithm is the obvious choice, cf. [1] and [2]. Note that this algorithm can be modified without difficulty to the case when we allow benefits. Theoretical results and numerical experiments have shown the feasibility of this approach but, at the same time, indicated that there is little or no saving in using the reduction provided by our results as compared to an approach where the Arimoto-Blahut algorithm is employed directly to the original problem.

In the literature (Silverman [7], [3], [4], [5] etc.), nontrivial concrete examples of DMC's are often pointed out with $\mathbf{P}$ a $3 \times 3$ matrix. They all have a non-trivial block symmetric decomposition, hence are of the form

$$
\mathbf{P}=\left(\begin{array}{lll}
\alpha & \beta & \gamma  \tag{8}\\
\beta & \alpha & \gamma \\
\delta & \delta & \varepsilon
\end{array}\right)
$$

For instance, [7] has $\beta=\varepsilon=0$. Applying our results leads to substantial simplifications.

## VI. Appendix

Consider the DMC $\mathbf{P}$ given by

$$
\mathbf{P}=\left(\begin{array}{ll}
p_{11} & p_{12}  \tag{9}\\
p_{21} & p_{22}
\end{array}\right)
$$

and an associated benefit vector $\mathbf{a}=\left(a_{1}, a_{2}\right)$.
Below, $i$ and $j$ are either 1 or 2 and $i \neq j$. Denote by $d$ the determinant of $\mathbf{P}$, by $H_{i}$ the entropy of $\vec{q}_{i}$ and by $D_{i j}$ the divergence $D\left(\vec{q}_{i} \| \vec{q}_{j}\right)$. Put $a_{i j}=a_{i}-a_{j}, H_{i j}=$ $H_{i}-H_{j}$ and define, for $d \neq 0$, quantities $h_{i}, h_{i j}$, and $d_{i j}$ by $h_{i}=d^{-1}\left(p_{j j}\left(a_{i}-H_{i}\right)-p_{i j}\left(a_{j}-H_{j}\right)\right), h_{i j}=h_{i}-h_{j}=$ $d^{-1}\left(a_{i j}-H_{i j}\right)$ and $d_{i j}=d^{-1}\left(D_{i j}+a_{i j}\right)$.

For $d \neq 0$ consider $\vec{q}^{*}=\left(q_{1}^{*}, q_{2}^{*}\right)$ given by

$$
q_{i}^{*}=\left(1+e^{h_{j i}}\right)^{-1}
$$

and consider the unique signed (!) input distribution $\vec{p}^{*}$ which induces $\vec{q}^{*}$ i.e.

$$
p_{i}^{*}=d^{-1}\left(q_{i}^{*}-p_{j i}\right) .
$$

Elementary calculations lead to the formulas:

$$
\begin{aligned}
q_{i}^{*} & =\frac{p_{i i}}{p_{i i}+p_{i j} e^{d_{j i}}}=\frac{p_{j i}}{p_{j i}+p_{j j} e^{-d_{i j}}} \\
p_{i}^{*} & =\frac{q_{i}^{*}}{d}\left(p_{j j}-p_{j i} e^{h_{j i}}\right)=\frac{q_{j}^{*}}{d}\left(p_{j j} e^{h_{i j}}-p_{j i}\right), \\
p_{i}^{*} & =\frac{p_{j i} q_{j}^{*}}{d}\left(e^{d_{i j}}-1\right)=\frac{p_{j j} q_{i}^{*}}{d}\left(1-e^{-d_{i j}}\right),
\end{aligned}
$$

which apply when $d \neq 0$. Continuity considerations may have to be taken into account, however, we can always select formulas to avoid this. Applying Theorem 1, one finds:

Theorem 4. Consider $\mathbf{P}$ given by (9) and with associated benefit vector $\mathbf{a}=\left(a_{1}, a_{2}\right)$. If $d=0$ and $a_{1}>a_{2}$, then $(1,0)$ is the unique optimal input distribution and $C(\mathbf{P} ; \mathbf{a})=a_{1} ;$ if $d=0$ and $a_{2}>a_{1}$, a similar statement holds, and if $d=0$ and $a_{1}=a_{2}$, any input distribution is optimal and $C(\mathbf{P} ; \mathbf{a})=a_{1}$.

If $d \neq 0$, the optimal input distribution is unique, and a necessary and sufficient condition that this distribution is non-trivial (i.e. both input probabilities are positive) is that

$$
\begin{equation*}
-D_{21}<a_{2}-a_{1}<D_{12} \tag{10}
\end{equation*}
$$

When (10) holds, the optimal input- and output distributions are $\vec{p}^{*}$ and $\vec{q}^{*}$ given by the formulas above and the modified capacity can be determined from Theorem 1 or from the formulas

$$
C(\mathbf{P} ; \mathbf{a})=h_{1}-\log q_{1}^{*}=h_{2}-\log q_{2}^{*}=\log \left(e^{h_{1}}+e^{h_{2}}\right)
$$

If $a_{2}-a_{1} \leq-D_{21}$, the optimal input distribution is $(1,0)$ and $C(\mathbf{P} ; \mathbf{a})=a_{1}$, and if $a_{2}-a_{1} \geq D_{12}$, the optimal input distribution is $(0,1)$ and $C(\mathbf{P} ; \mathbf{a})=a_{2}$.

By Theorem 1, this is easily checked.

## References

[1] S. Arimoto "An Algorithm for Computing the Capacity of Arbitrary Discrete Memoryless Channels", IEEE Trans. Inform. Theory, vol. IT-18, pp. 14-20, Jan. 1972.
[2] R. E. Blahut, "Computation of Channel Capacity and RateDistortion Functions", IEEE Trans. Inform. Theory, vol. IT-18, pp. 460-473, July 1972.
[3] T. M. Cover and J. A. Thomas, Elements of Information Theory. New York: Wiley 1991.
[4] R. C. Gallager, Information Theory and Reliable Communication. New York: Wiley 1968.
[5] C. M. Goldie and R. G. E. Pinch, Communication Theory, Cambridge: Cambridge University Press 1991.
[6] C. Shannon, "A mathematical theory of communication", Bell Syst. Tech. J., vol. 27, pp. 379-423, 623-656, 1948.
[7] R. A. Silverman, "On Binary Channels and their Cascades", IRE Trans. on Inform. Theory, vol. IT-1, pp. 19-27, Dec. 1955.
[8] F. Topsøe, "A New Proof of a Result Concerning Computation of the Capacity for a Discrete Channel", Z. Wahrscheinlichkeitstheorie verw. Geb., vol. 22, pp. 166-168, 1972.
[9] F. Topsøe, "Basic Concepts, Identities and Inequalities - the Toolkit of Information Theory", Entropy, vol. 3, pp. 162-190, 2001, http://www.unibas.ch/mdpi/entropy/ [ONLINE].


[^0]:    ${ }^{1}$ Supported by the Danish Natural Science Research Council and by INTAS, project 00-738.

[^1]:    ${ }^{1}$ This is the "compensation identity", cf. [9].

[^2]:    ${ }^{2}$ This case may be discussed by considering the function $D\left(\vec{q}_{1} \| \vec{q}\right)-D\left(\overrightarrow{q_{2}} \| \vec{q}\right)$ with $\vec{q}=\frac{1}{2} \overrightarrow{q_{1}}+\frac{1}{2} \vec{q}_{2}$ as a function of $p_{11}$ and $p_{22}$, observing that the determinant of the Hessian has a simple factorization; indeed, the determinant in question is

    $$
    \frac{-(1-\alpha-\beta)^{4}}{\alpha \beta(1-\alpha)(1-\beta)(1-\beta+\alpha)^{2}(1-\alpha+\beta)^{2}}
    $$

    where $\alpha=p_{11}, \beta=p_{22}$. This is the key fact needed to show that the function only vanishes on the diagonals of the unit square (for this argument, we acknowledge discussions with J. P. R. Christensen).

[^3]:    ${ }^{3}$ The set $\operatorname{BDE}(Z)$ is a sublattice of $\operatorname{DEC}(Z)$, but $\operatorname{BSD}(\mathbf{P})$ is not a further sublattice. To see this, consider $\mathbf{P}$ consisting of the two rows $\left(0, \frac{1}{2}, 0, \frac{1}{2}\right)$ and $\left(\frac{1}{2}, 0, \frac{1}{2}, 0\right)$ and note that $\operatorname{BSD}(\mathbf{P})$ is not closed under the lattice operation $\vee$.
    ${ }^{4}$ Consider the $2 \times 3$ matrix with rows $\left(0, \frac{1}{3}, \frac{2}{3}\right)$ and $\left(\frac{2}{3}, \frac{1}{3}, 0\right)$.
    ${ }^{5}$ This observation resulted from discussions with Mr. Thomas Jakobsen, the Danish Technical University, who also implemented the algorithm.

