Codes with the Identifiable Parent Property and the Multiple-Access Channel

R. Ahlswede and N. Cai

1 Introduction

We begin with

I. The identifiable parent property and some first results about it
If $\mathcal{C}$ is a q–ary code of length n and a^n and b^n are two codewords, then c^n is called a descendant of a^n and b^n if $c_t \in \{a_t, b_t\}$ for $t = 1, \ldots, n$. We are interested in codes $\mathcal{C}$ with the property that, given any descendant c^n, one can always identify at least one of the 'parent' codewords in $\mathcal{C}$. We study bounds on $F(n, q)$, the maximal cardinality of a code $\mathcal{C}$ with this property, which we call the *identifiable parent property*. Such codes play a role in schemes that protect against piracy of software.

They have been introduced by Hollmann, van Lint, Linnartz and Tolhuizen [9]. We repeat first their concepts, basic examples and results.

Consider a code $\mathcal{C}$ of length n over an alphabet Q with $|Q| = q$ (i.e., $\mathcal{C} \subset Q^n$). For any two words a^n, b^n in Q^n we define the *set of descendants* $D(a^n, b^n)$ by

$$D(a^n, b^n) := \{x^n \in Q^n | x_t \in \{a_t, b_t\}, t = 1, 2, \ldots, n\}. \tag{1.1}$$

Note that among the descendants of a^n and b^n we also find a^n and b^n themselves. For a code $\mathcal{C}$ we define the descendant code $\mathcal{C}^*$ by

$$\mathcal{C}^* := \bigcup_{a^n \in \mathcal{C}, b^n \in \mathcal{C}} D(a^n, b^n). \tag{1.2}$$

For example, if $\mathcal{C}$ is the binary repetition code, then $\mathcal{C}^* = F_2^n$. Similarly, if $\mathcal{C}$ is the ternary Hamming code of length 4, then $\mathcal{C}^* = F_3^4$, since it is obvious that all words in a ball of radius 1 around a codeword are descendants of some pair containing that codeword.

If $c^n \in \mathcal{C}^*$ is an element of $D(a^n, b^n)$, with $a^n \in \mathcal{C}$, $b^n \in \mathcal{C}$, then we call a^n and b^n *parents* of c^n. In general, an element of $\mathcal{C}^*$ has several pairs of parents. A trivial example are words of $\mathcal{C}$ themselves. We say that $\mathcal{C}$ has the "*identifiable parent property*" (IPP) if, for every descendant in $\mathcal{C}^*$, at least one of the parents can be identified. In other words, for each $c^n \in \mathcal{C}^*$ there is a codeword $\pi(c^n)$ in $\mathcal{C}$ such that each parent pair of c^n must contain $\pi(c)$.

Example: Consider the ternary Hamming code $\mathcal{C}$ of length 4, which has size 9. Since every pair of distinct codewords has distance 3, any descendant c^n in $\mathcal{C}^*$ has distance ≤ 1 to exactly one of the parents in a parent pair. There cannot be two codewords with distance 1 to c^n, so the unique codeword with distance ≤ 1

R. Ahlswede et al. (Eds.): Information Transfer and Combinatorics, LNCS 4123, pp. 249–257, 2006.

to c^n is the identifiable parent. For the other parent there are then three choices if $c^n \notin \mathcal{C}$ (and of course eight choices if $c^n \in \mathcal{C}$).

We are interested in the *maximal size* of a code with the identifiable parent property. We define

$$F(n,q) := \max\{|\mathcal{C}| \mid \mathcal{C} \subseteq Q^n, \mathcal{C} \text{ has IPP}, |Q| = q\}.$$

Trivially, a code of cardinality 2 has IPP. If $q = 2$, a code of cardinality ≥ 3 does not have IPP. To see this, consider three binary words u_1, u_2, u_3. For $i = 1, 2, 3$, the i–th coordinate of c^n is determined by a majority vote over the corresponding coordinates of the three given words. Then c^n is clearly a descendant of any pair taken from the three words u_j. So from now on we assume $q \geq 3$.

As trivial cases we have $F(1,q) = q$, $F(2,q) = q$. (If x_t, $t = 1, 2$, is a symbol that occurs twice as t–th coordinate, then (x_1, x_2) has no identifiable parent.)

Theorem HLLT 1. $F(3,q) \leq 3q - 1$

For certain classes of codes, it is easy to see that IPP holds. We start with equidistant codes.

Theorem HLLT 2. *If $\mathcal{C}$ is an equidistant code of length n over an alphabet of size q and with distance d, then $\mathcal{C}$ has the identifiable parent property if d is odd or if d is even and $n < \frac{3}{2}d$.*

Theorem HLLT 3. *Let q be a prime power. If $q \geq n - 1$ then a (shortened, extended, or doubly extended) Reed–Solomon code over F_q with parameters $\left[n, \left\lceil \frac{n}{4} \right\rceil, n - \left\lceil \frac{n}{4} \right\rceil + 1\right]$ has IPP.*

Corollary. *If $q \geq n - 1$ and q is a prime power, then $F(n,q) \geq q^{\left\lceil \frac{n}{4} \right\rceil}$.*

Theorem HLLT 4. *We have $F(n,q) \leq 3q^{\left\lceil \frac{n}{3} \right\rceil}$.*

Theorem HLLT 5. *There is a constant c such that $F(n,q) \geq c\left(\frac{q}{4}\right)^{\frac{n}{3}}$.*

From the calculations it follows that we could take $c = 0.4$. For large q, Theorem 5 is better than the Corollary.

We expand here the model in the following direction.

II. Men and women model

Here we consider two sets of codewords $\mathcal{U}, \mathcal{V} \subset Q^n$ referred to as sets of men and of women. Naturally we define the descendant code $\mathcal{C}^*(\mathcal{U}, \mathcal{V})$ by

$$\mathcal{C}^*(\mathcal{U}, \mathcal{V}) = \bigcup_{u \in \mathcal{U}, v \in \mathcal{V}} D(u,v).$$

If $c^n \in \mathcal{C}^*(\mathcal{U}, \mathcal{V})$ is an element of $D(u,v)$, then we call u and v parents of c^n.

We say now that $(\mathcal{U}, \mathcal{V})$ has the identifiable parent property if for every descendant in $\mathcal{C}^*$ at least one of the parents can be identified. This means that for every $c^n \in \mathcal{C}^*$ there is a codeword $\pi(c^n)$ in $\mathcal{U} \cup \mathcal{V}$ such that each parent pair $\{u, v\}$ of c^n must contain $\pi(c^n)$.

III. Semicodes for MAC
The previous model suggests to look at the structure in terms of multiple–access channels (MAC) defined by a stochastic matrix $W : \mathcal{X} \times \mathcal{Y} \to Z$. Then the IPP naturally leads to the new concept of semi codes with a new Coding Theorem determining the optimal rate $\bar{C}_{semi}$ for the average error concept (Theorem 1). The proof is by no means easy.

It has three basic ingredients: a wringing technique of [3], the blowing up method of [6] and the identity for entropies of [10] in the form of [7]. We analyze this model in Section 2. In Section 3 we mention directions of further research on identifiability.

2 Semicodes for the MAC

Let W be a stochastic matrix $\mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$. We call a system $\big(\{u_i\}_{i=1}^{M_1}, \{v_j\}_{j=1}^{M_2}, \{\mathcal{E}_i\}_{i=1}^{M_1}, \{\mathcal{D}_j\}_{j=1}^{M_2}\big)$ an (n, M_1, M_2, λ)–semi–code of MAC W^n, if $u_i \in \mathcal{X}^n$ for $i = 1, \ldots, M_1$, $v_j \in \mathcal{Y}^n$ for $j = 1, \ldots, M_2$, $\mathcal{E}_i \cap \mathcal{E}_{i'} = \varnothing$ for $i \neq i'$, $\mathcal{D}_j \cap \mathcal{D}_{j'} = \varnothing$ for $j \neq j'$, $\mathcal{E}_i \cap \mathcal{D}_j = \varnothing$ for all i, j and

$$\frac{1}{M_1}\frac{1}{M_2}\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W^n(\mathcal{E}_i \cup \mathcal{D}_j | u_i, v_j) > 1 - \lambda. \tag{2.1}$$

Denote by $\bar{C}_{semi}(\lambda)$ the maximal real number such that, for all $\delta > 0$ and sufficiently large n there exists an (n, M_1, M_2, λ)–semi–code with $\frac{1}{n}\log M_1 M_2 > \bar{C}_{semi}(\lambda) - \delta$. We shall determine $\bar{C}_{semi}(\lambda)$ and show that it is independent of $\lambda \in (0, 1)$. The main issue is the (strong) converse theorem and our main idea is very similar to that in [3]. The following result (Lemma 4 of [3]) will play an important role.

Lemma A. *Let P and Q be probability distributions on $\mathcal{X}^n$ such that for a positive constant c*

$$P(x^n) \leq (1 + c)Q(x^n) \text{ for all } x^n \in \mathcal{X}, \tag{2.2}$$

then for any $0 < \gamma < c$, $0 \leq \varepsilon < 1$ there exist $t_1, \ldots, t_k \in \{1, \ldots, n\}$, where $0 \leq k \leq \frac{c}{\gamma}$ such that for some $\bar{x}_{t_1}, \ldots, \bar{x}_{t_k}$

$$P(x_t | \bar{x}_{t_1}, \ldots, \bar{x}_{t_k}) \leq \max\big((1 + \gamma)Q(x_t | \bar{x}_{t_1}, \ldots, \bar{x}_{t_k}), \varepsilon\big) \tag{2.3}$$

for all $x_t \in \mathcal{X}$ and all $t = 1, 2, \ldots, n$ and

$$P(\bar{x}_{t_1}, \ldots, \bar{x}_{t_k}) \geq \varepsilon^k. \tag{2.4}$$

To apply it, we modify its consequence (Corollary 2 in [3]) slightly

Corollary. *Let $\mathcal{U}_n \subset \mathcal{X}^n$ with $|\mathcal{U}_n| = M_1$, $\mathcal{V}_n \subset \mathcal{Y}^n$ with $|\mathcal{V}_n| = M_2$, $\mathcal{A} \subset \mathcal{U}_n \times \mathcal{V}_n$ with $|\mathcal{A}| \geq (1 - \lambda^*)M_1 M_2$ for some $\lambda^* \in (0, 1)$. Then for any $0 < \gamma < c \triangleq \frac{\lambda^*}{1-\lambda^*}$,*

$0 \leq \varepsilon < 1$ *there exist* $t_1, \ldots, t_k \in \{1, \ldots, n\}$ *where* $k \leq \frac{\lambda^*}{\gamma(1-\lambda^*)}$ *and some* $(\bar{x}_{t_1}, \bar{y}_{t_1}), \ldots, (\bar{x}_{t_k}, \bar{y}_{t_k})$ *such that for* $\bar{\mathcal{A}} \triangleq \big\{(x^n, y^n) \in \mathcal{A} : x_{t_\ell} = \bar{x}_{t_\ell}\ y_{t_\ell} = \bar{y}_{t_\ell}$, *for* $\ell = 1, \ldots, k\big\}$

(a) $|\bar{\mathcal{A}}| \geq \varepsilon^k |\mathcal{A}|$,
and

(b) $\big((1+\gamma)Pr(\bar{X}_t = x)Pr(\bar{Y}_t = y) - \gamma - |\mathcal{X}||\mathcal{Y}|\varepsilon\big)$,
$\leq Pr(\bar{X}_t = x, \bar{Y}_t = y) \leq \max\big((1+\gamma)Pr(\bar{X}_t = x)Pr(\bar{Y} = y), \varepsilon\big)$
for all $x \in \mathcal{X}$, $y \in \mathcal{Y}$, $1 \leq t \leq n$,
where $(\bar{X}^n, \bar{Y}^n)$ *is a pair of RV's with uniform distribution on* $\bar{\mathcal{A}}$.

Proof: The corollary is essentially the same as Corollary 2 of [3] and can be shown in the same way. But we give the proof because it is short.

Let P and Q be defined by $P(x^n, y^n) = \frac{1}{|\mathcal{A}|}$ if $(x^n, y^n) \in \mathcal{A}$ and $Q(x^n, y^n) = P_1(x^n)P_2(y^n)$ for $(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n$, where P_1 and P_2 are marginal distributions of P, respectively. Then $P(x^n, y^n) \leq \frac{1}{1-\lambda^*} Q(x^n, y^n)$ and therefore one can apply Lemma A to $c = \frac{1}{1-\lambda^*} - 1 = \frac{\lambda^*}{1-\lambda^*}$ to obtain (a) and the second inequality of (b), which implies

$$
\begin{aligned}
&Pr(\bar{X}_t = x, \bar{Y}_t = y) = 1 - \sum_{(x'.y') \neq (x,y)} Pr(\bar{X}_t = x', \bar{Y}_t = y') \\
&\geq 1 - \sum_{(x',y') \neq (x,y)} \max\big((1+\gamma)Pr(\bar{X}_t = x')Pr(\bar{Y}_t = y'), \varepsilon\big) \\
&\geq 1 - |\mathcal{X}||\mathcal{Y}|\varepsilon - (1+\gamma)(1 - Pr(\bar{X}_t = x)Pr(\bar{Y}_t = y))\big) \\
&= LHS \text{ of (b).}
\end{aligned}
$$

□

Another main tool here is the Blowing Up Lemma of [5]. Let d_H be Hamming distance and for all $B \subset \mathcal{Z}'^n$, $\Gamma^k B \triangleq \big\{z^n :$ there is a $b^n \in B^n$ with $d_H(z^n, b^n) \leq k\big\}$, where $\mathcal{Z}'$ is a finite set. Then

Lemma AGK. (Blowing Up) *For any finite sets* $\mathcal{X}'$ *and* $\mathcal{Z}'$ *and sequence* $\{\varepsilon_n\}_{n=1}^\infty$ *with* $\varepsilon_n \to 0$, *there exist a sequence of positive integers* $\{\ell_n\}_{n=1}^\infty$ *with* $\ell_n/n \to 0$ *and a sequence* $\{\eta_n\}_{n=1}^\infty$ *with* $\eta \to 1$ *such that for every stochastic matrix* $V : \mathcal{X}' \to \mathcal{Z}'$ *and every* $n, x^n \in \mathcal{X}'^n$, $B \subset \mathcal{Z}'^n$
$W^n(B|x^n) \geq \exp\{-n\varepsilon_n\}$ *implies* $W^n(\Gamma^{\ell_n} B|x^n) \geq \eta_n$.

Remark: One can easily see that for a stochastic matrix $W : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ and any $y^n \in \mathcal{Y}^n$, the Blowing Up Lemma is still true for the channel $W^n(\cdot|\cdot, y^n) \triangleq \prod_{t=1}^n W(\cdot|\cdot, y_t)$. We shall actually employ this version of the Blowing Up Lemma.

Theorem 1. *For all* $\lambda \in (0, 1)$,

$$
\bar{C}_{semi}(\lambda) = \max_{X,Y} \max\big\{I(X \wedge Z) + H(Y), I(Y \wedge Z) + H(X)\big\}, \tag{2.5}
$$

where the first maximum is taken over all independent pairs of RV's (X, Y) with values in $\mathcal{X} \times \mathcal{Y}$, and Z is the corresponding output variable.

Proof

Converse: Let $\left(\{u_i\}_{i=1}^{M_1}, \{v_j\}_{j=1}^{M_2}, \{\mathcal{E}_i\}_{i=1}^{M_1}, \{\mathcal{D}_j\}_{j=1}^{M_2}\right)$ be an (n, M_1, M_2, λ)–semi–code. Then (2.1) implies that

$$\frac{1}{M_1}\frac{1}{M_2}\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W^n(\mathcal{E}_i|u_i, v_j) > \frac{1-\lambda}{2} \tag{2.6}$$

or

$$\frac{1}{M_1}\frac{1}{M_2}\sum_{i=1}^{M}\sum_{j=1}^{M} W^n(\mathcal{D}_j|u_i, v_j) > \frac{1-\lambda}{2}, \tag{2.7}$$

must hold. W.l.o.g. assume (2.6) holds and therefore there is a subcode $\mathcal{A} \subset \{u_i : 1 \le i \le M_1\} \times \{v_j : 1 \le j \le M_2\}$ such that

$$|\mathcal{A}| > \frac{1-\lambda-2\mu}{2(1-\mu)} M_1 M_2, \tag{2.8}$$

and for all $(u_i, v_j) \in \mathcal{A}$

$$W^n(\mathcal{E}_i|u_i, v_j) > \mu, \tag{2.9}$$

where μ is any positive constant less than $\frac{1-\lambda}{2}$.

We apply the Corollary to $\mathcal{A}$ with $\lambda^* \triangleq 1 - \frac{1-\lambda-2\mu}{2(1-\mu)} = \frac{1+\lambda}{2(1-\mu)}$, $\varepsilon = n^{-1}$ and $\gamma = n^{-\frac{1}{2}}$ and then get $t_1, \ldots, t_k$, $(\bar{x}_{t_1}, \bar{y}_{t_1}), \ldots, (\bar{x}_{t_k}, \bar{y}_{t_k})$, $\bar{\mathcal{A}}$ and $(\bar{X}^n, \bar{Y}^n)$ in the Corollary with

$$k \le \frac{\lambda^*}{\gamma(1-\lambda^*)} = \frac{1+\lambda}{1-\lambda-2\mu} n^{\frac{1}{2}} \tag{2.10}$$

and by (2.8) and (2.10)

$$|\bar{\mathcal{A}}| \ge \varepsilon^k |\mathcal{A}| \ge (1-\lambda^*) M_1 M_2 \varepsilon^k \ge \frac{1-\lambda-2\mu}{2(1-\mu)} M_1 M_2 \exp\left\{-\frac{1+\lambda}{1-\lambda-2\mu} n^{\frac{1}{2}} \log n\right\}. \tag{2.11}$$

Therefore

$$H(\bar{X}^n, \bar{Y}^n) = \log|\bar{\mathcal{A}}| \ge \log M_1 M_2 + \log\frac{1-\lambda-2\mu}{2(1-\mu)} - \frac{1-\lambda}{1-\lambda-2\mu} n^{\frac{1}{2}} \log n. \tag{2.12}$$

Let (X_t, Y_t, Z_t) be the triple of RV's, for $t = 1, \ldots, n$, with distribution $Pr(X_t = x, Y_t = y, Z_t = z) = Pr(\bar{X}_t = x) Pr(\bar{Y}_t = y) W(z|x, y)$, and let $\bar{Z}^n$ be the output of the channel W^n for the input $(\bar{X}^n, \bar{Y}^n)$. Then by (b) of the corollary and the uniform continuity of information quantities,

$$|\big(I(X_t \wedge Z_t) + H(Y_t)\big) - \big(I(\bar{X}_t \wedge \bar{Z}_t) + H(\bar{Y}_t)\big)| < \alpha_n, \tag{2.13}$$

for all t and some sequence $(\alpha_n)_{n=1}^{\infty}$ with $\alpha_n \to 0$ as $n \to \infty$.

Recalling $\bar{\mathcal{A}} \subset \mathcal{A}$, we have (2.9) for all $(u_i, v_j) \in \bar{\mathcal{A}}$. Thus by applying the Blowing Up Lemma to $(u_i, v_j) \in \bar{\mathcal{A}}$, we obtain, for all $(u_i, v_j) \in \bar{\mathcal{A}}$

$$W^n(\Gamma^{\ell_n}\mathcal{E}_i|u_i, v_j) \geq \eta_n \text{ and } \eta_n \to 1, \frac{\ell_n}{n} \to 0 \text{ as } n \to \infty \tag{2.14}$$

(c.f. the Remark after the Blowing Up Lemma).

Notice that $z^n \in \Gamma^{\ell_n}\mathcal{E}_i$ iff there is a $z'^n \in \mathcal{E}_i$ with $d_H(z^n, z'^n) \leq \ell_n$. We define "the decoding list" of z^n as $\mathcal{L}(z^n) \triangleq \{i : z^n \in \Gamma^{\ell_n}\mathcal{E}_i\}$. Then

$$|\mathcal{L}(z^n)| \leq \sum_{m=0}^{\ell_n} \binom{n}{m} (|\mathcal{Z}| - 1)^m \leq \exp\{n\beta_n\}, \text{ (say)} \tag{2.15}$$

with $\beta_n \to 0$ as $n \to \infty$. Introduce a new RV J by setting $J = 0$ if $\bar{X}^n \in \mathcal{L}(\bar{Z}^n)$ and $J = 1$ else. Then

$$\begin{aligned}
&H(\bar{X}^n|\bar{Z}^n) = H(\bar{X}^n J|\bar{Z}^n) = H(\bar{X}^n|J\bar{Z}^n) + H(J|\bar{Z}^n) \leq H(\bar{X}^n|J\bar{Z}^n) + H(J) \\
&\leq Pr(J=0)H(\bar{X}^n|J=0, \bar{Z}^n) + Pr(J=1)H(X^n|J=1) + \log 2 \\
&\leq Pr(J=0)H(\bar{X}^n|J=0, \bar{Z}^n) + (1-\eta_n)n\log|\mathcal{X}| + \log 2 \text{ (by (2.14))} \\
&\leq n\beta_n + (1-\eta_n)n\log|\mathcal{X}| + \log 2 \text{ (by (2.15))}.
\end{aligned} \tag{2.16}$$

Next we employ a technique of [10] which appears in 3.3 of [7].
Write for all $t \in \{1, 2, \ldots, n\}$

$$\begin{aligned}
&H(\bar{Y}_t|\bar{X}^n\bar{Y}^{t-1}\bar{Z}_{t+1}, \ldots, \bar{Z}_n) - H(\bar{Z}_t|\bar{X}^n\bar{Y}^{t-1}\bar{Z}_{t+1}, \ldots, \bar{Z}_n) \\
&= H(\bar{Y}^t\bar{Z}_{t+1}, \ldots, \bar{Z}_n|\bar{X}^n) - H(\bar{Y}^{t-1}\bar{Z}_t, \ldots, \bar{Z}_n|\bar{X}^n),
\end{aligned} \tag{2.17}$$

and obtain the following, by adding up both sides of (2.17) from 1 to n.

$$\begin{aligned}
&\sum_{t=1}^{n}\big(H(\bar{Y}_t|\bar{X}^n\bar{Y}^{t-1}\bar{Z}_{t+1}, \ldots, \bar{Z}_n) - H(\bar{Z}_t|\bar{X}^n\bar{Y}^{t-1}\bar{Z}_{t+1}, \ldots, \bar{Z}_n)\big) \\
&= H(\bar{Y}^n|\bar{X}^n) - H(\bar{Z}^n|\bar{X}^n),
\end{aligned} \tag{2.18}$$

In order to show

$$\sum_{t=1}^{n}\big(H(\bar{Y}_t|\bar{X}^n\bar{Y}^{t-1}\bar{Z}_{t+1}, \ldots, \bar{Z}^n) - H(\bar{Z}_t|\bar{X}^n\bar{Y}^{t-1}\bar{Z}_{t+1}, \ldots, \bar{Z}_n)\big) \leq \sum_{t=1}^{n}\big(H(\bar{Y}_t) - H(\bar{Z}_t|\bar{X}_t)\big) \tag{2.19}$$

we have to prove for all t

$$I(\bar{Z}_t \wedge \bar{X}^{t-1}\bar{X}_{t+1}, \ldots, \bar{X}_n\bar{Y}^{t-1}\bar{Z}_{t+1}, \ldots, \bar{Z}_n|\bar{X}_t) \leq I(\bar{Y}_t \wedge \bar{X}^n\bar{Y}^{t-1}\bar{Z}_{t+1}, \ldots, \bar{Z}_n).$$

It is sufficient to show

$$\begin{aligned}
&I(\bar{Z}_t \wedge \bar{X}^{t-1}\bar{X}_{t+1}, \ldots, \bar{X}_n\bar{Y}^{t-1}\bar{Z}_{t+1}, \ldots, \bar{Z}_n|\bar{X}_t) \\
&\leq I(\bar{Y}_t \wedge \bar{X}^{t-1}\bar{X}_{t+1}, \ldots, \bar{X}_n\bar{Y}^{t-1}\bar{Z}_{t+1}, \ldots, \bar{Z}_n|\bar{X}_t).
\end{aligned} \tag{2.20}$$

Since $H(\bar{Z}_t|\bar{X}_t\bar{Y}_t) = H(\bar{Z}_t|\bar{X}_t\bar{Y}_t\bar{X}^{t-1}\bar{X}_{t+1},\ldots,\bar{X}_n\bar{Y}^{t-1}\bar{Z}_{t+1},\ldots,\bar{Z}_n)$,

$$I(\bar{Z}_t \wedge \bar{X}^{t-1}\bar{X}_{t+1},\ldots,\bar{X}_n\bar{Y}^{t-1}\bar{Z}_{t+1},\ldots,\bar{Z}_n|\bar{X}_t\bar{Y}_t) = 0. \tag{2.21}$$

By adding (2.21) to LHS of (2.20), one obtains $I(\bar{Y}_t\bar{Z}_t \wedge \bar{X}^{t-1}\bar{X}_{t+1},\ldots,\bar{X}_n\bar{Y}^{t-1}\bar{Z}_{t+1},\ldots,\bar{Z}_n|\bar{X}_t)$, which implies (2.20) and therefore (2.19) holds.

Finally, (2.12), (2.13), (2.16), (2.18) and (2.19) together yield

$$\begin{aligned}
&\frac{1}{n}\log M_1M_2 \le \frac{1}{n}H(\bar{X}^n\bar{Y}^n) - \frac{1}{n}\log\frac{1-\lambda-2\mu}{2(1-\mu)} + \frac{1-\lambda}{1-\lambda-2\mu}n^{-\frac{1}{2}}\log n\\
&\le \frac{1}{n}\big(H(\bar{X}^n\bar{Y}^n) - H(\bar{X}^n|\bar{Z}^n)\big) + \beta_n + (1-\eta_n)\log|\mathcal{X}|\\
&+ \frac{1}{n}\log 2 - \frac{1}{n}\log\frac{1-\lambda-2\mu}{2(1-\mu)} + \frac{1-\lambda}{1-\lambda-2\mu}n^{-\frac{1}{2}}\log n\\
&= \frac{1}{n}\big(I(\bar{X}^n\wedge\bar{Z}^n) + H(\bar{Y}^n|\bar{X}^n)\big) + \theta_n\\
&= \frac{1}{n}\big(H(\bar{Z}^n) + H(\bar{Y}^n|\bar{X}^n) - H(\bar{Z}^n|\bar{X}^n)\big) + \theta_n\\
&= \frac{1}{n}\big[H(\bar{Z}^n) + \sum_{t=1}^{n}\big(H(\bar{Y}_t|\bar{X}^n\bar{Y}^{t-1}\bar{Z}_{t+1},\ldots,\bar{Z}_n) - H(\bar{Z}_t|\bar{X}^n\bar{Y}^{t-1}\bar{Z}_{t+1},\ldots,\bar{Z}_n)\big)\big] + \theta_n\\
&\le \frac{1}{n}\sum_{t=1}^{n}\big(H(\bar{Z}_t) + H(\bar{Y}_t) - H(\bar{Z}_t|\bar{X}_t)\big) + \theta_n\\
&= \frac{1}{n}\sum_{t=1}^{n}\big(I(\bar{X}_t\wedge\bar{Z}_t) + H(\bar{Y}_t)\big) + \theta_n\\
&\le \frac{1}{n}\sum_{t=1}^{n}\big(I(X_t\wedge Z_t) + H(Y_t)\big) + \alpha_n + \theta_n,
\end{aligned} \tag{2.22}$$

where $\theta_n \triangleq \beta_n + (1-\eta_n)\log|\mathcal{X}| + \frac{1}{n}\log 2 - \frac{1}{n}\log\frac{1-\lambda-2\mu}{2(1-\mu)} + \frac{1-\lambda}{1-\lambda-2\mu}n^{-\frac{1}{2}}\log n \to 0$ as $n\to\infty$.

Thus we conclude our proof of the converse part by setting (XYZ) as the triple achieving $\max_t\big(I(X_t\wedge Z_t) + H(Y_t)\big)$ and requiring $n\to\infty$ in (2.22).

Direct Part: The proof of the direct part can be done in the now standard way. It was actually first done in [1]. W.l.o.g. assume RHS of (2.5) is $I(X\wedge Z)+H(Y)$ and (X,Y,Z) is in the range of the maximum value. Then by letting $\{v_j : 1\le j\le M_1\} = \mathcal{T}_Y^n$, $\mathcal{D}_i = \mathcal{T}_{Z|X,\delta}^n(u_i) \setminus \bigcup_{i'\neq i}\mathcal{T}_{Z|X,\delta}^n(u_{i'})$ (δ is suitable) $\mathcal{E}_j = \varnothing$ and by independently randomly selecting u_i, $i = 1,2,\ldots,\lfloor 2^{n(I(X\wedge Z)-\delta')}\rfloor$ on $\mathcal{T}_X^n$ one can get the desired code. We omit the details. □

Remarks

1. Inspection of our results shows that we answered a basic question for the interference channel. We found the capacity region if one of the two channels is noiseless. Until now experts could not tell us whether this is known as a special case of complicated characterizations using several auxiliary RV's.

3 Further Results and Perspectives

IV. Screening design of experiments
Motivated by the original parent concept with no distinction between men and women we look at the special MAC with equal input alphabets $\mathcal{X} = \mathcal{Y} = Q$ and symmetric transmission probabilities

$$W(z|x,y) = W(z|y,x) \text{ for all } z \in \mathcal{Z} \text{ and } x, y \in Q$$

and at the situation where the codes $\mathcal{U}$ and $\mathcal{V}$ are equal. This communication situation came up for the first time in the theory of screening design of experiments (see the survey [11]), but now we look at the semicodes analogue to the above with $\mathcal{E}_i = \mathcal{D}_i$ for $i = 1, \ldots, M = M_1 = M_2$ and obtain the analogue to Theorem 1.

V. Semicodes for AVMAC
Next we tighten our models so that they give insight into the original problem. We replace the MAC by the AVMAC, the arbitrarily varying MAC, defined by a set of stochastic matrices $\mathcal{W} = \{w(\cdot|\cdot,\cdot,s) : s \in \mathcal{S}\}$ where $W(\cdot|\cdot,\cdot,s) : \mathcal{X} \times \mathcal{Y} \rightsquigarrow \mathcal{Z}$ and $s \in \mathcal{S}$.

We proved in [4] that its capacity region $\mathcal{R}(\mathcal{W})$ has the property:
$\mathcal{R}(\mathcal{W}) = \varnothing$ if and only if one of the following three conditions holds

(i) $\mathcal{W}$ is $(\mathcal{X}, \mathcal{Y})$–symmetrizable, that is for a stochastic $\sigma : \mathcal{X} \times \mathcal{Y} \to \mathcal{S}$

$$\sum_s W(z|x,y,x)\sigma(s|x',y') = \sum_s W(z|x',y',s)\sigma(s|x,y)$$

for all $x, x' \in \mathcal{X}, y, y' \in \mathcal{Y}$ and $z \in \mathcal{Z}$.

(ii) $\mathcal{W}$ is $\mathcal{X}$–symmetrizable, that is for a stochastic $\sigma_1 : \mathcal{X} \to \mathcal{S}$

$$\sum_s W(z|x,y,s)\sigma_1(s|x') = \sum_s W(z|x',y,s)\sigma_1(s|x)$$

for all $x, x' \in \mathcal{X}, y \in \mathcal{U}$ and $z \in \mathcal{Z}$.

(iii) $\mathcal{W}$ is $\mathcal{Y}$–symmetrizable, that is for a stochastic $\sigma_2 : \mathcal{Y} \to \mathcal{S}$

$$\sum_s W(z|x,y,s)\sigma_2(s,y') = \sum_s W(z|x,y',s)\sigma_2(s|y)$$

for all $x \in \mathcal{X}, y, y' \in \mathcal{Y}$ and $z \in \mathcal{Z}$.

VI. Robust screening design of experiments
We can establish the analogue for the one code-set ($\mathcal{U} = \mathcal{V}$) situation and of course also the capacity formula.

VIII. For certain termites females can give birth to males without mating and to females after mating. This gives another structure of relatedness, which can be studied with respect to the identifiability property.

References

1. R. Ahlswede, Multi–way communication channels, Proceedings of 2nd International Symposium on Information Theory, Thakadsor, Armenian SSR, Sept. 1971, Akademiai Kiado, Budapest, 23–52, 1973.
2. R. Ahlswede, The capacity region of a channel with two senders and two receivers, Ann. Probability, Vol. 2, No. 5, 805–814, 1974.
3. R. Ahlswede, An elementary proof of the strong converse theorem for the multiple–access channel, J. Combinatorics, Information and System Sciences, Vol. 7, No. 3, 216–230, 1982.
4. R. Ahlswede and N. Cai, Arbitrarily varying multiple–access channels, Part I. Ericson's symmetrizability is adequate, Gubner's conjecture is true, IEEE Trans. Inf. Theory, Vol. 45, No. 2, 742–749, 1999.
5. R. Ahlswede and G. Dueck, Every bad code has a good subcode: a local converse to the coding theorem, Z. Wahrscheinlichkeitstheorie und verw. Geb., Vol. 34, 179–182, 1976.
6. R. Ahlswede, P. Gács, and J. Körner, Bounds on conditional probabilities with applications in multiuser communication, Z. Wahrscheinlichkeitstheorie und verw. Geb., Vol. 34, 157–177, 1976.
7. I. Csiszár and J. Körner, Information Theory: Coding Theorems for Discrete Memoryless Systems, Academic Press, 1981.
8. G. Dueck, The strong converse to the coding theorem for the multiple–access channel, J. Combinatorics, Information & System Science, 187–196, 1981.
9. H.D.L. Hollmann, J.H. van Lint, J.P. Linnartz, and L.M.G.M. Tolhuizen, On codes with the identifiable parent property, J. Combin. Theory Ser. A 82, No. 2, 121–133, 1998.
10. J. Körner and K. Marton, Images of a set via two channels and their role in multi–user comunication, IEEE Transactions on Information Theory, Vol. 23, 751–761, 1977.
11. J. Viemeister, Die Theorie Selektierender Versuche und Multiple–Access–Kanäle, Diplomarbeit, Universität Bielefeld, 1981.