Perspectives

Our models go considerably beyond Shannon's transmission model and the model of identification. They will greatly enlarge the body of information theory. We substantiate here this belief by a brief discussion of how already the identification model alone had a significant impact.

Right now the most visible influences are new approximation problems (like approximation of output statistics [14] or entropy approximations based on Schur-convexity [10] etc.), a new emphasis on random number generation [1] and, above all, an understanding of the concept of common randomness [9], in identification [10, 11, 13], cryptography [7], and classical transmission problems of arbitrarily varying channels [3, 5, 12], and the paper [6], with a novel capacity formula, which could not be derived before.

It is also fascinating to discover how transmission problems and identification problems in multi-user theory show often some kind of duality. Often identification problems are mathematically more complex and in other cases we encounter the opposite: there is a rather *complete* capacity theory for identification via multi-way channels in case of complete feedback [10, Lecture 3], whereas for transmission with feedback we don't even understand the multiple access channel.

We conclude with three more recently encountered directions of research.

1 Comparison of Identification Rate and Common Randomness Capacity: Identification Rate can Exceed Common Randomness Capacity and Vice Versa

One of the observations of [9] (chapter "Identification in the Presence of Feedback: A Discovery of New Capacity Formulas") was that random experiments, to whom the communicators have access, essentially influence the value of the identification

R. Ahlswede, *Identification and Other Probabilistic Models*,
Foundations in Signal Processing, Communications and Networking 16,
https://doi.org/10.1007/978-3-030-65072-8_13

capacity $C_{pol}ID$. We introduce now *common randomness capacity*, which was called mystery number in [10] (chapter "On Identification via Multi-Way Channels with Feedback: Mystery Numbers"), and has subsequently been called by us in lectures and papers by its present name.

The common randomness capacity $C_{pol}CR$ is the maximal number ν such, that for a constant $c > 0$ and for all $\epsilon > 0$, $\delta > 0$ and for all n sufficiently large there exists a permissible pair (K, L) of RV's for length n on a set $\mathcal{K}$ with $|\mathcal{K}| < e^{cn}$ with

$$\Pr\{K \neq L\} < \epsilon \qquad \text{and} \qquad \frac{H(K)}{n} > \nu - \delta.$$

Actually, if sender and receiver have a common randomness capacity $C_{pol}CR$ then by the so called $\sqrt{n}$-trick of chapter "Identification in the Presence of Feedback: A Discovery of New Capacity Formulas", that is, the transformator lemma (discussed in [4]), always

$$C_{pol}ID \geq C_{pol}CR \text{ if } C_{pol}ID > 0. \tag{1}$$

For many channels (see [7, 9]), in particular for channels with feedback [9, 10], equality has been proved.

It seemed therefore plausible, that this is always the case, and that the theory of identification is basically understood, when common randomness capacities are known.

We report here a result, which shows that this expected unification is not valid in general—*there remain two theories*.

Example In [15] one can find also an example with $0 < C_{pol}ID < C_{pol}CR$)

Example We will now prove the existence of a sequence of channels (not a sequence of discrete memoryless channels) with $C_{pol}ID = 1, C_{pol}CR = 0$.

We use a Gilbert type construction of error correcting codes with constant weight words. This was done for certain parameters in [8] (see chapter "Identification via Channels", Part I). The same arguments give for parameters needed here the following auxiliary result.

Proposition 126 *Let $\mathcal{Z}$ be a finite set and let $\lambda \in (0, 1/2)$ be given. For $(2^{3/\lambda})^{-1} < \varepsilon < (2^{2/\lambda} + 1)^{-1}$ a family $A_1, \ldots, A_N$ of subsets of $\mathcal{Z}$ exists with the properties*

$$|A_i| = \varepsilon|\mathcal{Z}|, \qquad |A_i \cap A_j| < \lambda\varepsilon|\mathcal{Z}| \qquad (i \neq j)$$

and

$$N \geq |\mathcal{Z}|^{-1} 2^{\lfloor \varepsilon|\mathcal{Z}| \rfloor} - 1.$$

Notice that $\lambda \log\left(\frac{1}{\varepsilon} - 1\right) > 2$ and that for ℓ with $2^{-\ell} = \varepsilon$ necessarily $\ell > \frac{2}{\lambda}$.

Choose now $\mathcal{Z} = \{0,1\}^n$, $\varepsilon = 2^{-\ell}$ and A_i's as in the Proposition. Thus $|A_i| = 2^{n-\ell}$, $N(n,\lambda) = 2^{-n}2^{2^{n-\ell}} - 1$ and $|A_i \cap A_j| < \lambda 2^{n-\ell}$.

Consider now a discrete channel $(W^n)_{n=1}^{\infty}$, where the input alphabets $\mathcal{X}_t = \{1, 2, \ldots, N(t,\lambda)\}$ are increasing, $\mathcal{X}^n = \prod_{t=1}^{n} \mathcal{X}_t$ are the input words of length n, $\mathcal{Y}^n = \{0,1\}^n$ are the output words and $W^n : \mathcal{X}^n \rightsquigarrow \mathcal{Y}^n$ is defined by

$$W^n(\cdot|i_1 i_2 \ldots i_n) = W^n(\cdot|i_n)$$

and $W^n(\cdot|i)$ is the uniform distribution on A_i for $1 \leq i \leq N(n,\lambda)$.

By Proposition 126 and $3/\lambda > \ell > 2/\lambda$

$$N(n,\lambda) \geq 2^{-n}2^{2^{n-3/\lambda}}$$

and

$$C_{pol}ID \geq \liminf_{n\to\infty} \frac{1}{n} \log\log N(n,\lambda) \geq 1.$$

However, for transmission every decoding set is contained in some A_i and for error probability λ must have cardinality $(1-\lambda)|A_i| = (1-\lambda)2^{n-\ell}$.

Therefore $M(n,\lambda) \leq \frac{2^n}{(1-\lambda)2^{n-\ell}} \leq 2^{\ell+1}$, if $\lambda < 1/2$, and $\frac{1}{n}\log M(n,\lambda) \leq \frac{\ell+1}{n} \leq \frac{3/\lambda+1}{n} \to 0 (n \to \infty)$. *The transmission capacity is* 0. Consequently also $C_{pol}CR = 0$. ▲

Remark The case of bounded input alphabets remains to be analyzed. What are "natural" candidates for equality of $C_{pol}ID$ and $C_{pol}CR$?

Remark For infinite alphabets one should work out conditions for finiteness of the identification capacity.

2 Robustness, Common Randomness and Identification

It is understood now [6, 7] how the theory of AV-channels is *intimately* related to the concept of robust common randomness. A key tool is the balanced hypergraph coloring [2]. We sketch now another direction concerning robustness and identification.

For more robust channel models, for instance in jamming situations, where the jammer knows the word to be sent (c.f. AV-channels with maximal error criterion), the communicators are forced to use the maximal error concept. In case of identification this makes the randomization in the encoding (see [8, Lecture 1]) superfluous. Now, for a DMC W it was mentioned in chapter "Identification via Channels" that in the absence of randomization the identification capacity, say

$C_I^*(W)$, equals the logarithm of the number of different row-vectors in W. This is easy to show, however, a formidable problem arises if the DMC W is replaced by the AVC $\mathcal{W}$. In fact, for 0-1-matrices only in $\mathcal{W}$ we are—exactly as for transmission—led to the equivalent Shannon-zero-capacity problem. But for general $\mathcal{W}$ the identification problem is quite different from the transmission problem.

In so far there is a lower bound on $C_I^*(\mathcal{W})$, which implies for

$$\mathcal{W} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \delta & 1-\delta \end{pmatrix} \right\}, \qquad \delta \in (0,1)$$

that $C_I^*(\mathcal{W}) = 1$, which is obviously tight. It exceeds the known capacity for transmission. The capacity for

$$\mathcal{W} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1-\delta & \delta \\ \delta & 1-\delta \end{pmatrix} \right\}$$

is unknown.

3 Beyond Information Theory: Identification as a New Concept of Solution for Probabilistic Algorithms

Finally we mention as the perhaps most promising direction the study of probabilistic algorithms with identification as *concept of solution*. (For example: for any i, is there a root of a polynomial in interval i or not?)

The algorithm should be fast and have small error probabilities. Every algorithmic problem can be thus considered. This goes far beyond information theory. Of course, like in general information transfer also here a more general set of questions can be considered. As usual in complexity theory one may try to classify problems.

What rich treasures do we have in the much wider areas of information transfer?!

References

1. R. Ahlswede, The capacity region of a channel with two senders and two receivers. Ann. Probab. **2**(5), 805–814 (1974)
2. R. Ahlswede, Coloring hypergraphs: a new approach to multi–user source coding. Part I, J. Comb. Inf. Syst. Sci. **1**, 76–115 (1979). Part II **5**(3), 220–268 (1980)
3. R. Ahlswede, General theory of information transfer, in *Preprint 97–118, SFB 343 Diskrete Strukturen in der Mathematik* (Universität Bielefeld, Bielefeld, 1997)
4. R. Ahlswede, Towards a general theory of information transfer, in *Shannon Lecture at ISIT in Seattle 13th July 2006*. IEEE Information Theory Society Newsletter (2007)
5. R. Ahlswede, N. Cai, Arbitrarily varying multiple–access channels, in *Part I: Ericson's Symmetrizability is Adequate, Gubner's Conjecture is True, Preprint 96–068, SFB Diskrete*

Strukturen in der Mathematik (Universität Bielefeld, Bielefeld). *Part II: Correlated Sender's Side Information, Correlated Messages and Ambiguous Transmission*. Preprint 97–006, SFB 343 Diskrete Strukturen in der Mathematik, Universität Bielefeld. IEEE Trans. Inf. Theory, vol. 45(2), 749–756 (1999)

6. R. Ahlswede, N. Cai, The AVC with noiseless feedback and maximal error probability: a capacity formula with a trichotomy. Preprint 96–064, SFB 343 Diskrete Strukturen in der Mathematik, Universität Bielefeld, Numbers, Information and Complexity, Special volume in honour of R. Ahlswede on occasion of his 60th birthday, editors I. Althöfer, N. Cai, G. Dueck, L.H. Khachatrian, M. Pinsker, A. Sárközy, I. Wegener, Z. Zhang (Kluwer Acad. Publication, Boston, Dordrecht, London), pp. 151–176 (1996)
7. R. Ahlswede, I. Csiszár, Common randomness in information theory and cryptography, Part I: Secret sharing. IEEE Trans. Inf. Theory **39**(4), 1121–1132 (1993). R. Ahlswede, I. Csiszár, Common randomness in information theory and cryptography, Part II: CR capacity. IEEE Trans. Inf. Theory **44**(1), 225–240 (1998)
8. R. Ahlswede, G. Dueck, Identification via channels. IEEE Trans. Inf. Theory **35**, 15–29 (1989)
9. R. Ahlswede, G. Dueck, Identification in the presence of feedback—a discovery of new capacity formulas. IEEE Trans. Inf. Theory **35**, 30–39 (1989)
10. R. Ahlswede, B. Verboven, On identification via multi–way channels with feedback. IEEE Trans. Inf. Theory **37**(5), 1519–1526 (1991)
11. R. Ahlswede, Z. Zhang, New directions in the theory of identification via channels, in *SFB 343 Diskrete Strukturen in der Mathematik, Bielefeld, Preprint 94–010* (1994). IEEE Trans. Inf. Theory **41**(4), 1040–1050 (1995)
12. R. Ahlswede, B. Balkenhol, C. Kleinewächter, Identification for Sources, in *General Theory of Information Transfer and Combinatorics* (eds.) by R. Ahlswede, et al. Lecture Notes in Computer Science, vol. 4123 (2006)
13. T.S. Han, *Information-spectrum Methods in Information Theory*, vol. 50 (Springer, Berlin, 2013)
14. T.S. Han, S. Verdú, Approximation theory of output statistics. IEEE Trans. Inf. Theory **39**(3), 752–772 (1993)
15. C. Kleinewächter, On identification, in *General Theory of Information Transfer and Combinatorics*. Lecture Notes in Computer Science, vol. 4123 (Springer, New York, 2006), pp. 62–83