IEEE Information Theory Society Newsletter

Vol. 62, No. 5, March 2012 Editor: Tara Javidi ISSN 1059-2362

Editorial committee: Helmut Bölcskei, Giuseppe Caire, Meir Feder, Tracey Ho, Joerg Kliewer, Anand Sarwate, and Andy Singer

President's Column

It is an honor and delight to address you for the first time as your new president. I am surrounded by a wonderful and supportive cadre of vice-presidents (Gerhard Kramer and Abbas El Gamal) as well as past presidents (Giuseppe Caire and Frank Kschischang). I would like to thank Giuseppe on behalf of the Society for his outstanding service and extend personal thanks to him for help with the transition. Giuseppe has guided the Society with warmth, sure judgment and energy. I am fortunate to have such a predecessor.

Apart from a new president, our Society also has some other transitions of officers. Andrea Goldsmith transitions off the officer roster as senior past president. Her leadership and enthusiasm have benefited the Society greatly, with such initiatives as the Student Committee, which has provided wonderful opportunities for our students with workshops, panels, as well as the very popular and well-attended Summer School. Tara Javidi replaces as Newsletter editor Tracey Ho, who finishes her term. Aylin Yener, who has performed so excellently on the Student Committee, replaces Nihar Jindal as treasurer. Many thanks to Tracey and Nihar for a job well done—the quality of the Newsletter and the health of our finances are very important to our Society. We are indebted to Tara and Aylin for agreeing to take on these important jobs.

We have an exciting year ahead of us with the upcoming IEEE review of the Society, which will take place at the TAB meeting in February (for publications only) and the TAB meeting in November (for the other activities). I have had the opportunity to observe these reviews at the TAB meeting last November and found them quite interesting. I think the exercise may prove to be a useful one in which to engage as a Society. This will be an opportunity for us to initiate a discussion about our Society's current accomplishments, operations and challenges. More importantly, it will allow us to consider collectively our vision and strategy for the future. I shall rely on the Board of Governors and on the Society as a whole for help in this important task.

In the context of seeding this conversation in our Society, I would like to offer as a topic of reflection the intellectual role our Society plays in the context not only of IEEE, but of engineering writ large. Our Society has had considerable successes in many aspects of engineering, such as progresses in physical layer communications. We have had many opportunities to reflect on those contributions. For instance, the 2004 Shannon Lecture of Bob McEliece led us through an insightful (and even musical) retrospective of the contributions of Shannon (who stood in for coding) versus those of Newton (who stood in for physics) in the context of space communications. The Society has also been at the forefront of many other developments in the physical layer space. One example among a great many is the study of MIMO systems and associated coding approaches, such as space-time codes.

However, the Society's contributions extend far beyond physical layer communications. The Society has had a central role in incubating varied domains, with considerable thematic ins(,t of Ib[(HTMs Tws1(Socicodes37(A)55(l) r)1)1(cOne exampxt o, sucher i

to the NRC, Section 07 Executive and Peer Committees, member of the Committee on Tactical Battle Management, Committee on National Communications Systems Initiative, and U.S. National Committee for the International Union of Radio Science.

Jack was not only an outstanding researcher but also a dedicated and wonderful educator. He was passionate about teaching, and he had a gift for expressing in simple and clear terms even the most difficult subjects. He brought to the classroom a wealth of practical experience gained through his many years of consulting and employment in the telecommunications and storage industries. Using his unique perspective, Jack inspired his students by successfully linking elegant theory with exciting technological applications. In 2000, Jack's excellence in teaching was recognized with the UCSD Distinguished Teaching Award.

Jack maintained a close relationship with his alma mater, the University of Pennsylvania. In fact, studying at Penn was somewhat

wxr a dae clo aTJ 0 T8(oarrnn wammuniobut alsnternation it generwith .ir)18(Tw 0 -123ng A)74(w a giperdae clo ahar Co-)]Tmadivehil wi his m

Erdal Arikan
Bilkent University Ankara

for contributions to coding theory

Martin Bossert
Ulm University

for contributions to reliable data transmission including code constructions and soft decision decoding

The Historian's Column

It is crisis-time in the world today: crisis in the financial world, turmoil in the world economy, disorder in Society, and soul-searching in Science. Periodically such phenomena of agony, doubt, concern, and pessimism tend to emerge and dominate and then subside or go into a sleep-mode. Over the years, we have observed such a

Second Order Analysis Based on Information Spectrum

Abstract – In this letter, we explain the importance of the 2nd-order asymptotic theory for channel coding and its mathematical

In the first step, the optimum asymptotic performance is derived for a given information source or a given channel without any condition, e.g., the independent and identical distributed (i.i.d.) condition or the Markovian condition. The optimum asymptotic performance is represented by a limiting value defined by the logarithmic likelihood or the logarithmic likelihood ratio. Such quantities are called information spectrum quantities. Since these values represent no concrete values, only this step cannot resolve the problem.

In the second step, we calculate the information spectrum quantities concretely in the respective cases, e.g., the i.i.d. case or the Markovian case. Fortunately, it is easy to calculate these values in the i.i.d. case and the Markovian case. Only the first step depends on the type of the information process. The second step depends on the type of information sources or channels, but does not depend on the type of the information process. Especially, when variable types of information process give the same the information spectrum quantity as their optimal performance, the existing calculation can be recycled in the second step.

On the other hand, the first step for the first order asymptotics can be directly applied that for the second order asymptotics. That is, as soon as this problem is mathematically formulated, the solution has been already given [10]. Such a story is too convenient for researchers. Therefore, only the second step is required for the second order asymptotic theory. It can be also resolved only by application of the central limit theorem except for channel coding. only the impossibility part (the converse part) for channel coding cannot be resolved in the above simple

where $W^n_x(y) := W^n(y|x)$ and $W^n_{P^n}(y) := \sum_x P^n(x) W^n(y|x)$.

When we fix the size $|\psi_n|$ for a respective integer n, the minimum average error probability is given as

$$C_n(L|W^n) := \min_{(\psi_n,\phi_n)} \{\epsilon_n(\psi_n,\phi_n) | \log|\phi_n| \geq L\}. \tag{10}$$

Then, we can obtain the following formula:

$$\begin{aligned} \lim_{\gamma\to+0} \inf_{\bar{P}} \underline{P}_I(R_1 - \gamma|\bar{P},\bar{W}) &\leq \liminf_{n\to\infty} C_n(R_1 n|W^n) \\ &\leq \lim_{\gamma\to+0} \inf_{\bar{P}} \underline{P}_I(R_1 + \gamma|\bar{P},\bar{W}) \end{aligned} \tag{11}$$

$$\begin{aligned} \lim_{\gamma\to+0} \inf_{\bar{P}} \overline{P}_I(R_1 - \gamma|\bar{P},\bar{W}) &\leq \limsup_{n\to\infty} C_n(R_1 n|W^n) \\ &\leq \lim_{\gamma\to+0} \inf_{\bar{P}} \overline{P}_I(R_1 + \gamma|\bar{P},\bar{W}). \end{aligned} \tag{12}$$

In particular, when four quantities $\lim_{\gamma\to+0}\inf_{\bar{P}}\underline{P}_I(R_1 - \gamma|\bar{P},\bar{W})$, $\lim_{\gamma\to+0}\inf_{\bar{P}}\underline{P}_I(R_1 + \gamma|\bar{P},\bar{W})$, $\lim_{\gamma\to+0}\inf_{\bar{P}}\overline{P}_I(R_1 - \gamma|\bar{P},\bar{W})$, $\lim_{\gamma\to+0}\inf_{\bar{P}}\overline{P}_I(R_1 + \gamma|\bar{P},\bar{W})$ coincide, the limit $\lim_{n\to\infty} C_n(R_1 n|W^n)$ exits and coincides with them, i.e.,

$$\lim_{n\to\infty} C_n(R_1 n|W^n) = \lim_{\gamma\to+0} \inf_{\bar{P}} \underline{P}_I(R_1 - \gamma|\bar{P},\bar{W}). \tag{13}$$

Therefore, we can evaluate the limits $\liminf_{n\to\infty} C_n(R_1 n|W^n)$ and $\limsup_{n\to\infty} C_n(R_1 n|W^n)$ by using the above four quantities for any sequence of channels. These formulas do not provide explicit bounds for these limits. Hence, their meaning is not as clear as entropy.

However, in the case of discrete memoryless, as is shown via slightly complicated calculation, the above four quantities coincide and are written by using the capacity $C(W)$ as follows.

$$\inf_{P} \lim_{0} P\ (R_1 \quad \gamma|P,W) \quad \begin{matrix} 1 & \text{if } R_1 > C(W) \\ 0 & \text{if } R_1 < C(W). \end{matrix}$$

.49.196. - .4299321(g 0.372 T- 0 2480.41747379558431 27(,, 4(:

realizing the minimum average error probability $C_n(R_1 n|W^n)$. Then, we denote a sequence of distribution satisfying the condition in Lemma 2 by $\bar{P} = \{P^n(x)\}$. Choosing $M_n = 2^{(R_1 \quad)n}$

We have easily shown the above theorem, however, it is not so clear whether the normalized KL-divergence should be used as the criteria for the uniform random number.

If the variation distance between the uniform distribution and the distribution of the generated random number does not go to zero, we can distinguish the generated random number from the uniform random number. So, in order to claim that the generated random number is close to the uniform random number, we should show that the above variation distance goes to zero. Alternatively, we should show that the KL-divergence goes to zero because the convergence concerning the KL-divergence is stronger than the convergence concerning the variational distance due to Pinsker's inequality [21].

If we focus on the first order asymptotics, we cannot deny the existence of a code such that the variational distance from the uniform random number goes to zero and the average error probability for the data compression goes to zero. This is because there exists a common possible rate $H(P^X)$ for both conditions. However, the second order asymptotics denies the existence of such a code because there exist no rate for the second order asymptotics satisfying both conditions due to (26) and (27). That is, in order that the variational distance goes to zero, the second rate R_2 must be $-\infty$, and in order that the average error for data compression goes to zero, the second rate R_2 must be $+\infty$. As is illustrated in Fig. 3, It is impossible to satisfy the both conditions. Therefore, when the data can be correctly recovered in the data compression, the compressed data cannot go to the uniform distribution in the sense of the variational distance [10][2]. The above fact means that the second order analysis discovers the detail behavior behind of the first order asymptotics.

VII. Application to Security

The second order asymptotics reveals the problem for traditional information-theoretical security analysis based on the first order asymptotics. The previous section discusses the relation between the compressed random number and the uniform random number. This topic relates to the generation of the secret random number as well as the uniform random number. Now, we consider how to distill secret random number from a random number A leaked to the eavesdropper as a partially correlated random number E.

In this case, applying Hash function to the random number A, we can distill a random number B that is almost independent of the other random number E. This process is called privacy amplification, and has been studied from the community cryptography theory. On the other hand, due to Slepian-Wolf theorem [22], if the additional side information E is available, the random number A can be compressed up to the conditional entropy rate $H(A|E)$. Let B be the random number obtained by the compression up to the conditional entropy rate $H(A|E)$ based on the leaking information E Then, if the folklore in source coding is valid and the random number A can be decoded from B with E, B looks the uniform distribution for respective values of E. That is, the eavesdropper cannot obtain any information concerning B from E.

However, the folklore in source coding is valid only under the normalized KL-divergence criterion. It is not valid under the non-normalized KL-divergence criterion. This fact can be extended to the case when the additional information E exists [23]. Therefore, the compressed random number B has no correlation with E under the normalized mutual information criterion. However, we cannot say that it has no correlation with E under the non-normalized mutual information criterion.

Employing the separation coding by Slepian-Wolf [22], Ahlswede, Csiszar [24] and Muramatsu [25] treated the secret key distillation from two correlated random variables A and A' that are partially eavesdropped as another random variable E. For a simplicity, in the following, we consider the case $A = A'$, i.e., the case when the error correction is not required. Under this limited case, their method proposed is simplified as follows. We convert the initial random number A to the pair of the final random number B and the dummy random number C. In their method, we keep B as the final random number.

Assume that the random number A can be perfectly recovered from the pair of B and E and $H(C) = H(C|B) = I(A{:}E)$, which is equivalent with the condition that the random number C can be perfectly recovered from the random number E

Thus, such a higher analysis is not required for analysis of the convergence of the mutual information.

Using the second order analysis, we can show that the method via error correction for C cannot generate the secure random number under the non-normalized mutual information. Hence, we need to directly evaluate the variational distance from the uniform distribution or the non-normalized mutual information without the error correction for C.

While the method via the error correction for C is familiar to researchers in information theory, the direct evaluation for the variational distance or the non-normalized mutual information requires a completely new method. As for a method directly evaluating these values, the privacy amplification theorem has been studied from the community of cryptography theory. Initially, this theorem has been established with the Renyi entropy with order 2 [26], [27]. Renner and his collaborators extended it to the version with the smooth min entropy [29], [28]. Recently, the author extended it to the version with Renyi entropy with order $1+s$, which directly yields the exponential decreasing rate of the mutual information when the generation rate is less than the conditional entropy rate [30], [31].

The same problem happens for the security analysis in wire-tap channel. When the normalized mutual information is adopted as the security criterion, the security can be shown via the error correction for the dummy random variable C. However, it is impossible to show the the security under the non-normalized mutual information criterion, i.e., the strong security based on this method because the mutual information behaves as the order $\sqrt{n}$ [32]. As such a method guaranteeing the strong security, the author and the collaborator proposed an application of privacy amplification theorem or channel resolvability [33] to wire-tap channel [30], [31], [34], [35], [36], [37], [38], [39], [40]^3. Therefore, the second order asymptotics enables us to evaluate the detail order analysis that cannot be treated by the traditional the first order asymptotics. That is, the second order asymptotics reveals a kind of security hole behind of the traditional approach. We can expect further reveals of the problem caused by the first order asymptotics.

IX. Conclusions

We have explained the second order asymptotics theory for the channel coding, fixed-length data compression, and the uniform random number generation. They can be treated from a unified viewpoint by employing the method of information spectrum due to the generality of information spectrum.

The method of information spectrum can be applied not only to the second order asymptotics but also to other topics. For example, it is known that in the case of quantum communication with coherent states, the number of transmittable bits increases up to infinity even if the total energy is fixed when the number of used modes increases up to infinity. Such a phenomena does not happen in the classical case. The method of information spectrum enables us to resolve the asymptotic analysis for such a case [46]. Hence, we can expect a further and wider variety of applications of the method of information spectrum.

X. Acknowledgments

The author is grateful to Professors Te Sun Han, Hiroshi Nagaoka for explaining information spectrum. He is also grateful to Professors Tomohiko Uyematsu and Ryutaroh Matsumoto for informing the reference [8] and the references [23], [32], [20], respectively. He is also grateful to anonymous referees and editors of the papers [9], [10] for helpful comments. He also thanks Dr. Ke Li, Dr. Akihito Soeda, and Mr. Wataru Kumagai for helpful comments. This study was partially supported by MEXT through a Grant-in-Aid for Scientific Research on Priority A

up to infa eTj s so17eases
up to iw8uI. KontoyianJ ts fixed when the n7iori3(6):1189181 N71a24.3rse

Ants and Bits

Plenary talk presented at the 2011 IEEE International Symposium of Information Theory, St. Petersburg, Russia.

Abstract. Ants have always been helping people to solve various problems. Everybody remembers how they sorted seeds for Cinderella. For the IT community, ants have helped to show that Information Theory is not only an excellent mathematical theory but that many of its results can be considered laws of Nature. Reciprocally, we helped ants to be distinguished among other "intellectuals" such as counting primates, crows and parrots as one of the smartest species [1, 2]. Our long-term experimental study on ant "language" and intelligence were fully based on fundamental ideas of Information Theory, such as the Shannon entropy, the Kolmogorov complexity, and the Shannon's equation connecting the length of a message l and its frequency of occurrence p, i.e., $l = -\log p$. This approach enabled us to discover a developed symbolic "language" in highly social ant species based on their ability to transfer the abstract information about remote events and to estimate the rate of information transmission. We also succeeded to reveal important properties of ants' intelligence. These insects appeared to be able to grasp regularities and to use them for "compression" of data they communicate to each other. They can also transfer to each other the information about the number of objects and can even add and subtract small numbers in order to optimize their messages.

Introduction

From time immemorial, people have been dreaming about understanding animal "languages"- a dream with which many legends are associated. The title of the book of the famous ethologist Konrad Lorenz, King Solomon's Ring (1952), refers to the legend about King Solomon who possessed a magical ring that gave him the power of speaking with animals. However, decoding the function and meaning of animal communications is a notoriously difficult problem. A bottleneck here is the low repeatability of standard living situations, which could give keys for cracking animals' species-specific codes. Up to now, there are only two types of natural communication systems that have been partly deciphered: the fragments of honeybees' "dance language", and acoustic signalization in vervet monkeys and several other species (see [3] for a review). In both types of communications, expressive and distinctive signals correspond to repeatable and frequently occurring situations in the context of animals' life. The problem of cracking animals' codes have become especially attractive since the great "linguistic" potential was discovered in several highly social and intelligent species by means of intermediary artificial languages. Being applied to apes, dolphins and gray parrots, this method has revealed astonishing mental skills in the subjects [4, 5, 6]. However, surprisingly little is known yet about natural communication systems of those species that were involved in language-training experiments based on adopted human languages. Explorers of animal "languages" thus have met a complex problem of resolving found to include teams of constant membership which consisted of one scout and three to eight recruits (foragers): the scout mobilized only members of its team to the food. The composition of the teams was revealed during special run-up experiments. During the main course of experiments, in each trial one of the scouts was placed on a certain leaf of the binary tree that contained a trough with the food, and then it returned to the nest by itself. Returning to the group of foragers, the scout contacted one to four foragers in turn (Fig. 2). The duration of the contacts was measured every time.

All experiments were so devised as to eliminate all possible cues that could help the ants to find the food, except their information contact with the scout. To avoid the use of an odor track, the experimental set-up was replaced by an identical one when the scout was in the nest or on the arena contacting its group (see Fig. 3). All troughs in the fresh maze contained only water to avoid the possible influence of the smell of syrup. If the group reached the correct point, they were immediately presented with the food. The scout had to make up to four trips before it was able to mobilize its group of foragers. After the scout had contacted its team, it was isolated in a separate container for a while, and the foragers had to search for the food by themselves.

The experiments based on Shannon entropy present a situation in which, in order to obtain food, the ants have to transmit certain information which is quantitatively known to the researcher. This information concerns the sequence of turns towards a trough with syrup. The laboratory maze "binary tree" is used where each "leaf" of the tree ends with an empty trough with the exception of one filled with syrup. The leaf on which to place the filled trough was chosen randomly by tossing a coin for each fork in the path. The simplest design is a tree with one fork and two leaves, that is, a Y-shaped maze. It represents one binary choice which corresponds to one bit of information. In this situation a scouting animal should transmit one bit of information to other individuals: to go to the right (R) or to the left (L). In other experiments the number of forks of the binary tree increased to six. Hence, the number of bits necessary to choose the correct way is equal to the number of forks, that is, turns to be taken (Figure 1 shows a labyrinth with 3 forks). In total, 335 scouts along with their teams were used in all experiments with the binary tree, and each scout took part in tens of trials.

The binary tree and ants' language

Before analyzing ants' "linguistic potential" we considered the evidence of information transmission from the scouts to the for-

The scheme was as follows. Ants were offered a horizontal trunk with 30 branches. The experiments were divided into three stages, and at each of them the regularity of placing the trough with syrup on branches with different numbers was changed. At the first stage, the branch containing the trough with syrup was selected randomly, with equal probabilities for all branches. So the probability of the trough with syrup being placed on a particular branch was 1/30. At the second stage we chose two "special" branches A and B (N 7 and N 14; N 10 and N 20; and N 10 and N 19 in different years) on which the trough with syrup occurred during the experiments much more frequently than on the rest - with a probability of 1/3 for "A" and "B", and 1 /84 for each of the other 28 branches. In this way, two "messages" -"the trough is on branch A" and "the trough is on branch B"- had a much higher probability than the remaining 28 messages. In one series of trials we used only one "special" point A (the branch N 15). On this branch the food appeared with the probability of 1/2, and 1/58 for each of the other 29 branches. At the third stage of the experiment, the number of the branch with the trough was chosen at random again.

The obtained data demonstrated that ants appeared to be forced to develop a new code in order to optimize their messages, and the usage of this new code has to be based on simple arithmetic opera-

Panel on "New Perspectives on Information Theory" IEEE Information Theory Workshop, Paraty, October 20, 2011

A video of the panel discussion (including questions from the audience) can be found in http://media.itsoc.org/itw2011/ What follows is an edited transcript.

Verdú *Seventeen years ago at the ITW that was held in Moscow, I organized a similar panel on the future of Information Theory with the participation of Dick Blahut, Imre Csiszár, Dave Forney, Prakash Narayan and Mark Pinsker. In preparation for this panel I have asked our panelists to read the transcript of that panel (published in the December 1994 issue of this newsletter) and discuss the ways in which that panel's predictions were and were not accurate.*

Costa Well, it´s been said that it is difficult to make predictions, specially about the future. The 1994 panel predictions were good in many aspects, but they could not guess those areas that appeared from nowhere and brought completely new tools and perspectives to the field. There was another situation in which this happened. Estill Green, a VP of Bell Labs, also made some bold and courageous predictions on telecommunications, looking from 1961 into that technology in the year 2012. Bob Lucky

Kramer I enjoyed the back-and-forth between the engineers (For-system designers, without always giving the correct credit to the originators. It is sufficient to look at conferences such as SIGCOMM, but sometimes also to ICC and Globecomm, to understand what I am talking about.

Costa Before I address the point, let me make a comment on what Raymond just mentioned. It´s true that some of the proofs of what Shannon could see were not there, like the EPI, for example, the entropy power inequality, that was later proved by Stam and Blachman. But he could have the tremendous insight to see it, and maybe feel that it was essentially the isoperimetric inequality. This amazing insight that Shannon had was also what led him to the random coding argument. I remember a class that Tom Cover gave in a course on Information Theory in which he said: "If I had that idea of the random coding argument, I think I would just go home and sober up." Also to point to the recognition of the work of Shannon, he arrived unexpectedly at the 1985 ISIT in Brighton. Nobody knew that he was going to attend the meeting and there was a big commotion. Bob McEliece is reported to have said that it was just like if in a conference of physicists someone had announced that Newton was present.

Now, we see obituaries of Information Theory come up from time to time. Right now is actually a time that we have a better perspective. Coding theory has also gone through that, and obituaries were announced for coding theory a number of times. One of the early announcements was closely followed by the invention of trellis coded modulation and all the burst of activity that it generated. A few years later, another such obituary was challenged by the creation of turbo codes in 1993, and by the rediscovery of LDPC codes. So it is very risky to make categorical statements regarding the end of an area. Many new things are always coming up to second guess the less optimistic forecaster.

It seems odd to imagine that Information Theory may be perishing when we have just witnessed the dawn of the Information Age. To mention changes that are occurring in a number of schools, the traditional engineering denominations are being replaced by names like information engineering, energy engineering, environmental engineering, and so on. These changes point to the importance of paying attention to the resources, and being resourceful is definitively one of the highlights of Information Theory.

Yeung

Shann.

coding at the level of communication over VLSI buses. So my main point in the context of this discussion is that we should be a little bit humble about why we are so successful—it's not entirely of our own making.

Verdú *Just like in 1994 I think it is futile to try to predict what the disruptive problems that will revolutionize the field in the future. Nevertheless, it is useful to discuss those current topics with the highest chance to have an impact on the future development of Information Theory.*

Kramer I suppose we all have our favorite current topics that we feel are important now and that we can predict will be important in the future. One of my favorites is Information Theory applied to optical channels, including optical fiber (MIMO is hot), free space, non-coherent vs. coherent, quantum, and so forth. A second favorite topic of mine is whether and how one can transfer the substantial progress on understanding relay and interference channel capacity into wireless systems. A third favorite is the same question concerning network coding and its application to distributed storage.

Caire At the risk of being disproved and laughed about by those who will read the transcript of this panel in a few years from now, I am going to try a forecast. What I'd like to see in the next 5–6 years from now is the development of a "communication theory for networks''. We gained an enormous insight about network Information Theory, in understanding interference and relaying. Nevertheless, we are very far from a "plug-and-play'' set of techniques around which novel physical layer architectures can be actually designed. To make an analogy, in point-to-point communications we had Ungerboeck TCM, and now Turbo and LDPC codes followed by some form of bit-interleaving and mapping onto modulation alphabets. These techniques have been widely studied at the point that they have become standard tools around which systems based on point-to-point links can be safely designed. Still, in order to handle interference we rely on orthogonal (or quasi-orthogonal) access, and treating interference as noise, or as "collisions''. We are still very far from the point where a new set of codes in the signal space (lattice codes? polar codes applied to multiuser problems?) can be used as basic building blocks for a robust system design. Of course, the risk of not filling this gap between Information Theory and communication theory (and therefore, practice of system design) is that these areas will remain confined in the purely theoretical domain and they may eventually fade away.

Anantharam As I said in the beginning, much of the success we have had in this field is centered around problems that are in the communication theory arena, but I think there are vast realms out there that are waiting to be conquered by what you might call "information-theoretic thinking". Shannon basically brought information-theoretic thinking to bear on communication theory. But there are aspects of nature, for instance, which have to have been designed with the concept of the optimization of some kind of information content in view. When you have a lot of interacting entities, either entities in nature or entities that you want to design, for instance when you want to design a biological system, which is eventually going to happen, there has to be a thinking, both in the engineered design and in nature as it came up with the designs that we are aware of today, which involves a notion of some information aspect that was optimized in enabling the coordination between the interacting entities. I am not sure on what time scale this will happen, but for instance biology is advancing at an enormous rate, so it could very well be twenty years, maybe longerofe as2 6, hey ewome kimho will rtion of some infor
BunI tft s wetmax-fltw- by-cutotamef10.v*n 1(of) 1(ofairy n1(o is noflryf1

tiles or bricks that form multiple user structures, like broadcast channels, multiple access channels, interference channels and relay channels. I think there will be more development in these areas, and it may be a stretch, it may take a long time, but eventually we will see some conciliation and integration between the approaches of network coding and multiple user Information Theory.

Also source coding is still far from achieving the limits. I must say that I didn't expect to be alive on the day that channel coding limits would be approached as they are, within a small fraction of a dB. I really thought that this would be happening after my time. Now we can ponder that source coding is still not at that point, and hopefully we will still be around when those limits are approached within a fraction of a dB. More effective ways to combine source and channel coding will also became prominent. Improved and new inequalities will continue to extend the power and the scope of Information Theory tools.

I believe there are many fronts in which Information Theory will continue to bring significant contributions, both in practical technologies and in pure scientific and mathematical issues. So rather than thinking that Information Theory will eventually come to some type of blockade, I am more inclined to think that Information Theory will never die.

I would like to quote Karl Popper on something similar to the idea of monkeys trying to reach the moon. My son Bruno is a philosopher and we have some interesting discussions about this sort of thing. This is something that he told me. Karl Popper used to say that we may be very different in the ways we do things and in our abilities and knowledge about things, but in our infinite ignorance we are all alike.

Yeung A few years ago I had a chat with Prakash Narayan who was a panelist 17 years ago. I was pointing out the fact in the control theory community people had been using optimization tools for decades. Prakash made a very interesting point. He said that once the structure of a problem is exposed, what remain are algorithms and optimization. So, I think at least in the context of communications, in the Information Theory community we are going to see more and more of that.

Since we are still on the broad topic of "New Perspectives for Information Theory," I want to pick up a point Sergio mentioned a little while ago, regarding the lack of entropy of topics at ISIT. Personally, this actually bothers me quite a bit. I remember visiting Jim Massey in 2000 at Copenhagen. I was mentioning to Jim that these days research has become so competitive in many areas that if you don't publish something immediately, then very likely 3 months later somebody else will publish the same result. And Jim said, "In that case you shouldn't publish the result." I am not sure whether this is the best way to survive in today's research environment. Ideally we should all be working on problems that we think are important instead of following what the trend is doing all the time. But in the United States in particular, research is pretty much driven by funding. Whatever they call for you have to work on it, although you can do things in disguise. You have to follow the game.

Verdú Looking at my crystal ball, I see going forward: breakthroughs in multiuser Information Theory; intersections of Information Theory with machine learning, with signal processing, with compressed sensing, with theoretical computer science. Maybe one day we will think of the beginning of the XXI century as the era of bad quality: dropped cellphone calls, bad skype connections, lousy youtube video quality. This should put pressure in narrowing the gap between lossy compression theory and practice, and to that end one of the requisites is to learn how we can fool the eye and the ear more effectively than today. New approaches drawn from other fields such as random matrices and statistical physics methods are gaining prominence. And finally, non-asymptotic Information Theory: many practical applications are characterized by short messages or strict delay constraints. In the non-asymptotic regime we do not have the luxury of the closed-form formula, but we can still get very tight bounds as a function of delay.

Anantharam Other modern mathematical tools are also being brought to bear on Information Theory problems, e.g. from additive number theory in problems of interference alignment, and new kinds of concentration inequalities from our improved u39 sensear8 and refined tools. […] Information Theory is firmly integrated in the fabric of neuroscience research, and a progressively wider range of biological research in general, and will continue to play an important role in these disciplines."

Shannon's bandwagon warning notwithstanding, it is probably a safe prediction that this trend – information theoretic-ideas and tools being systematically applied in biology and perhaps in the other sciences – will continue and it will grow. In the reverse direction, another recent –though somewhat less noticeable– trend has been the growing use of information-theoretic concepts in core mathematics research. Although this was advocated by Kolmogorov almost 30 years ago ("Information Theory must precede probability theory and not be based on it. [...] The concepts of Information Theory […] can acquire a certain value in the investigation of the algorithmic side of mathematics as a whole"), progress has perhaps been slower and less flashy than the corresponding successes in, e.g., biology. But there are numerous examples – including Perelman's proof of the Poincaré conjecture and the celebrated Green-Tao theorem on the existence of arithmetic progressions in the primes – where Shannon entropy and the associated "technology" have served as important intellectual guidelines for major mathematical breakthroughs. This is another direction that I believe will continue strong and will gain momentum.

Finally, one of the essential components of our trade has to do with building foundations. Given a new communications scenario – be it a new technology with different physical characteristics, a new biological setting describing the communication between two distinct parts of an organism, or a new type of network model like those we have been studying in recent years arising in social media interactions – we abstract its fundamental characteristics and provide a rigorous "language" for its study. Keeping an open mind – and open doors – towards such new problems virtually guarantees a healthy outlook and a wealth of opportunities. A recent success story in this direction is the area of "compressed sensing." This could well have become a sub-field of statistics or harmonic analysis. The fact that it was embraced by the Information Theory community is a testament to both our open-mindedness and our strength.

I cannot resist one last comment. We really need to figure out how to do lossy compression effectively in practice!

Over 100 participants attended an interdisciplinary workshop on "Counting, Inference, and Optimization on Graphs" at Princeton University, NJ, November 2–5, 2011. The workshop was organized by the authors under the auspices of the Center for Computational Intractability (CCI) at Princeton.

The workshop was originally inspired by the recognition of connections between certain duality results in the theory of codes on graphs and recent work on "holographic" algorithms in theoretical computer science. Ultimately, topics included holographic algorithms, complexity dichotomy theorems, capacity of constrained codes, graphical models and iterative decoding algorithms, and exact and approximate calculation of partition functions of graphical models. The participants had a wide range of backgrounds, including theoretical computer science, information and coding theory, statistical physics, and statistical inference.

The program is listed below. Copies of slides, references to related papers, and videos of some of the talks are available on the conference website at <http://intractability.princeton.edu/blog/2011/05/workshop-counting-inference-and-optimization-on-graphs>.

The participants were enthusiastic about the quality of the talks, the stimulation of various cross-disciplinary dialogues, and the excellent arrangements provided by the Center for Computational Intractability.

Program:

Leslie VrP* [(-0.5 testament to both our)Tj 0 Tw T* [(open-mindedness)1.2

Farzad Parvaresh, “Asymptotic enumeration of binary matrices with bounded row and column weights”

David Forney, “Codes on graphs, normal realizations, and partition functions”

Yongyi Mao, “Normal factor graphs, linear algebra and probabilistic modeling”

Navin Kashyap, “The tree width of a linear code”

Pascal Vontobel, “Should we believe in numbers computed by loopy belief propagation?”

Martin Dyer, “On the complexity of #CSP”

Xi Chen, “Complexity of counting CSP with complex weights”

Alistair Sinclair, “Permanents, determinants, and commutativity”

Leonid Gurvits, “A new entries-dependent lower bound on the permanent of doubly stochastic matrices”

Martin Wainwright, “Learning in graphical models: Missing data and rigorous guarantees with non-convexity”

Yair Weiss, “Convexity: What is it good for?”

Marc Mézard, “Statistical physics-based reconstruction in compressed sensing”

Andrea Montanari, “Sharp thresholds in statistical learning”

Anima Anandkumar, “High-dimensional graphical model selection: Tractable graph families and regimes”

Umesh Vazirani, “Quantum description complexity”

David Poulin, “Belief propagation in the quantum world”

Jonathan Yedidia, “The alternating direction method of multipli-
Umerirl g-passing ss it m(c M´gi(l gMAP18(egimes”)]Tw 0 -2ntiofamndeB(

GOLOMB'S PUZZLE COLUMN™

Powers with Shared Digits

A positive integer which is a square, cube, or higher power of some integer will be called simply a *power*. The infinite sequence of powers begins $\{1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, \ldots\}$.

1) How many powers are there from 1 to 1 million?

2) How many powers are there from 1 to x, for real $x > 4$?

Sometimes, two or more powers will consist of the same k digits, though in different permuted orders. As seen above, there are no such cases with 2

GOLOMB'S PUZZLE COLUMN™

The Sequence n^3-n Solutions

1) The only cases where $n^3 - n = k!$ are: $n = 2, k = 3; n = 3, k = 4; n = 5, k = 5; n = 9, k = 6$

Call for Nominations

IEEE Information Theory Society 2012 Claude E. Shannon Award

The IEEE Information Theory Society Claude E. Shannon Award is given annually for consistent and profound contributions to the field of information theory. Award winners are expected to deliver the Shannon Lecture at the annual IEEE International Symposium on Information Theory held in the year of the award.

NOMINATION PROCEDURE: Nominations and letters of endorsement must be submitted by March 1, 2012 to the current President of the IEEE Information Theory Society, who in 2012 will be Muriel Medard <medard@MIT.edu>. The nomination form is available at http://www.itsoc.org/honors/claude-e.-shannon-award.

(See page 35 for more information).

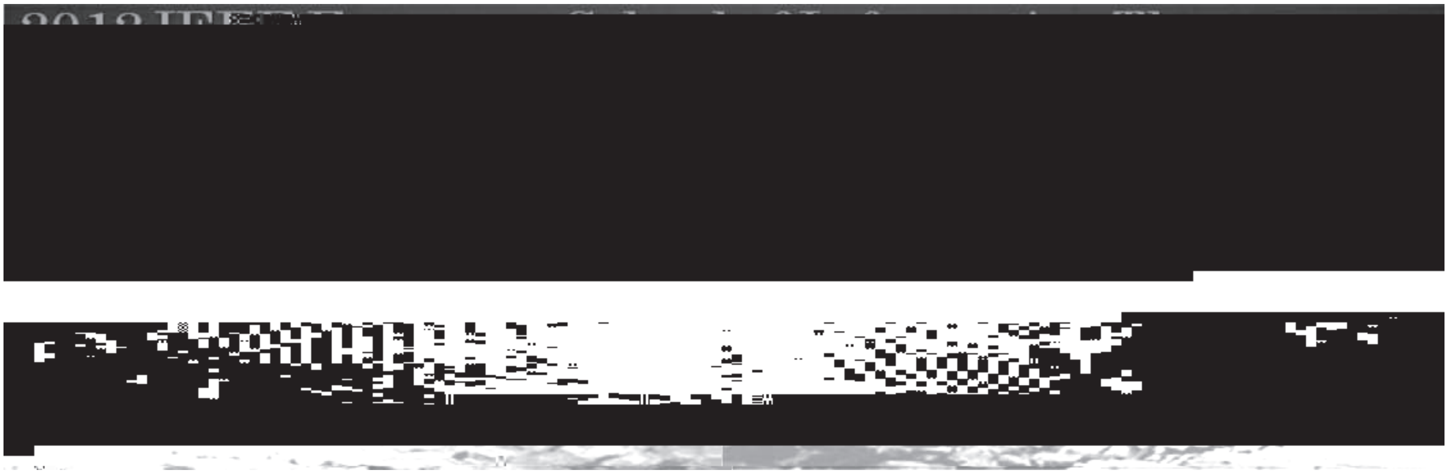
IEEE Information Theory Society 2012 Aaron D. Wyner Distinguished Service Award

The IT Society Aaron D. Wyner Award honors individuals who have shown outstanding leadership in, and provided long standing exceptional service to, the Information Theory community. Each Wyner Award winner receives an ISIT or ITW participation fee waiver, a specially engraved plague, and a certificate. This award was formerly known as the IT Society Distinguished Service Award.

NOMINATION PROCEDURE: Nominations and letters of endorsement must be submitted by March 1, 2012 to the current President of the IEEE Information Theory Society, who in 2012 will be Muriel Medard <medard@MIT.edu>. The nomination form is available at http://www.itsoc.org/honors/wyner.

(See page 35 for more information).

IEEE Information Theory Society 2012 Paper Award



2012 IEEE European School of Information Theory
April 16-20, 2012, Antalya, Turkey

http://www.itsoc.org/european-school

The 2012 IEEE European School of Information Theory will take place in Antalya, Turkey between the 16th and the 20th of April, 2012. The event, organized jointly by CTTC (Spain), TUM (Germany) and Bahcesehir University (Turkey), will offer graduate students and young researchers the opportunity to learn from experts in information theory through half-day tutorials, as well as the chance to present and discuss their own ongoing work.

This is the 12th information theory school in Europe, and we again have a distinguished list of speakers. This year’s instructors and tentative lecture titles are:

* Frans Willems (Eindhoven University of Technology, Netherlands) Introduction to Universal Source Coding and Biometrics

* Sennur Ulukus (University of Maryland, USA) Information Theoretic Security

* Meir Feder (Tel Aviv University, Israel) Efficient Lattice Codes

* Alex Dimakis (University of Southern California, USA) Network Coding for Distributed Storage

* Michael Gastpar (UC Berkeley, USA and EPFL, Switzerland) Algebraic Structure in Network Information Theory

The IEEE Information Theory Society is the main sponsor of the 2012 European School of Information Theory.

General Chairs: Deniz Gunduz (CTTC), Gerhard Kramer (TUM)

Local Organization Chair: Alkan Soysal (Bahcesehir University)

For additional information, see: http://www.itsoc.org/european-school

The Fiftieth Annual Allerton Conference on Communication, Control, and Computing will be held from Monday, October 1 through Friday, October 5, 2012, at Allerton House, the conference center of the University of Illinois. Allerton House is located twenty-six miles southwest of the Urbana-Champaign campus of the University in a wooded area on the Sangamon River. It is part of the fifteen-hundred acre Robert Allerton Park, a complex of natural and man-made beauty designated as a National natural landmark. Allerton Park has twenty miles of well-maintained trails and a living gallery of formal gardens, studded with sculptures collected from around the world.

Papers presenting original research are solicited in the areas of communication systems, communication and computer networks, detection and estimation theory, information theory, error control coding, source coding and data compression, network algorithms, control systems, robust and nonlinear control, adaptive control, optimization, dynamic games, multi-agent systems, large-scale systems, robotics and automation, manufacturing systems, discrete event systems, multivariable control, computer vision-based control, learning theory, cyber-physical systems, security and resilience in networks, VLSI architectures for communications and signal processing, and intelligent transporTl[c)0om)35(-37oc)-34n)33oneei 0.0052 Tc .033 T506-2.304T28[V)30Ac)-1llrs ti Cifese(e)36s)27t)-21is

2012 IEEE COMMUNICATIONS THEORY WORKSHOP

Ka’anapali, Maui, Hawaii, USA
May 14-16, 2012

Sponsored by:

IEEE COMMUNICATION SOCIETY

Shannon Award Call for Nominations

The purpose of the Claude E. Shannon Award is to honor consistent and profound contributions to the field of information theory. The selection is governed by Article V, Section 4.

An honorarium of $10,000 and a suitable memento are awarded to the Claude E. Shannon Award winners. Each Shannon Award winner is expected to present a Shannon Lecture at the IEEE International Symposium on Information Theory of the year of the award. In addition to the honorarium, the Information Theory Society will pay the winner's travel expenses.

The Shannon Lecturers in the years preceding the institution of the Shannon Lecturer Award (1973-1994) shall be considered to be Claude E. Shannon Award winners for the years their respective Shannon Lectures were delivered.

Nominations for the Claude E. Shannon Award can be made by anyone and are made by completing a nomination form (available online) and sending it and all supporting materials to the Society President by March 1st. The committee may consider all possible candidates, not only those for whom nominations have been received.

The 2012 C. E. Shannon Award Selection Committee, whose task is to decide whether to name a C. E. Shannon Award winner for 2013, will consist of the following members:

Aaron D. Wyner Distinguished Service Award Call for Nominations

The purpose of the Aaron D. Wyner Distinguished Service Award is to honor individuals who have shown outstanding leadership in—and provided long-standing exceptional service to—the Information Theory Community. The selection is governed by Article V, Section 9.

Nominations for the Wyner Distinguished Service Award can be made by anyone and are made by completing a nomination form (available online) and sending it and all supporting materials to the Society President by March 1st.

The individual or individuals making the nomination have the primary responsibility for justifying why the nominee should receive this award. The committee may consider all possible candidates, not only those for whom nominations have been received. Current officers and members of the Society Board of Governors are ineligible.

The prize shall be an ISIT or ITW participation fee waiver, a specially engraved plaque and a certificate, and shall be presented at the ISIT meeting held during the Summer following selection of the winner or at an appropriate IEEE IT society activity selected by the recipient.

The 2012 A. D. Wyner Award Selection Committee will consist of the following members:

Conference Calendar

DATE	CONFERENCE	LOCATION	WEB PAGE	DUE DATE
December 5–9, 2011	**2011 IEEE Global Communications Conference (GLOBECOM 2011)**	Houston, TX, USA	http://www.ieee-globecom.org	Passed
December 12–16, 2011	**15th Workshop on Quantum Information Processing (QIP2012)**	Montreal, Quebec, Canada	http://www.iro.umontreal.ca/~qip2012	Passed
February 5–10, 2012	**2012 Information Theory and Applications Workshop**	San Diego, CA, USA	http://ita.ucsd.edu/workshop.php	By Invitation
February 29–March 2, 2012	**2012 International Zurich Seminar on Communications**	Zurich, Switzerland	http://www.izs.etzh.ch/	Passed
March 21–23, 2012	**46th Annual Conference on Information Sciences and Systems (CISS 2012)**	Princeton, NJ, USA	http://ee-ciss.princeton.edu	January 6, 2012
March 25–30, 2012	**IEEE INFOCOM 2012**	Orlando, FL, USA	http://www.ieee-infocom.org	Passed
May 6–9, 2012	**2012 IEEE 75th Vehicular Technology Conference (VTC2012-Spring)**	Yokohama, Japan	http://www.ieeevtc.org/vtc2012spring	Passed
May 14–16, 2012	**2012 IEEE Communication Theory Workshop (CTW 2012)**	Ka'anapali, Maui, HI, USA	http://www.ieee.ctw.org/	March 1, 2012
May 14–18, 2012	**10th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt 2012)**	Paderborn, Germany	http://www.wi-opt.org/	January 6, 2012
June 10–15, 2012	**IEEE International Conference on Communications (ICC 2012)**	Ottawa, Canada	http://www.ieee-icc.org/	Passed
June 29–30, 2012	**International Symposium on Network Coding (NETCOD 2012)**	Cambridge, MA, USA	http://www.netcod2012.org/doku.php	February 24, 2012
July 1–6, 2012	**2012 IEEE International Symposium on Information Theory (ISIT 2012)**	Cambridge, MA, USA	http://isit12.org/	February 3, 2012
August 27–31, 2012	**7th International Symposium on Turbo Codes & Iterative Information Processing**	Gothenberg, Sweden	http://www.ee.kth.se/turbo-symposium-2012/	March 9, 2012
September 3–6, 2012	**2012 IEEE 76th Vehicular Technology Conference (VTC2012-Fall)**	Quebec City, Canada	http://www.ieeevtc.org/vtc2012fall/	February 2012
September 3–7, 2012	**2012 IEEE Information Theory Workshop (ITW 2012)**	Lausanne, Switzerland	http://itw2012.epfl.ch/	April 2, 2012
October 28–31, 2012	**2012 International Symposium on Information Theory and its Applications (ISITA 2012)**	Honolulu, HI, USA	http://www.isita.ieice.org/2012	March 28, 2012

Major COMSOC conferences: http://www.comsoc.org/confs/index.html