IEEE Information Theory Society Newsletter

Vol. 70, No. 2, June 2020

EDITOR: Salim El Rouayheb

President's Column

The last time I wrote to you was in a different lifetime. In the past three months, we have witnessed a pandemic with devastating impact that had cost lives and disrupted life as we know it, in every way we can imagine. The pandemic is still far from under control in much of the world, and we do not have a date that we can expect to have some normalcy; of course everyone is hoping for sooner than later. I still feel like I entered the twilight zone, but have reluctantly accepted that this is not a bad dream as I originally thought, but is the new normal (at least for sometime). In difficult times like these, humanity is often at its best (of course there are always exceptions); one quickly converges to what really matters

in life and all of a sudden set backs that seemed monumental before become minutia. The pandemic will no doubt have long-term impact on our profession, and by extension our professional organization.

Despite the somewhat depressing tone of the beginning of this column, I would like to say that our society's operations are in full force, and we are very much on track with the goals set at the beginning of the year. Like every other aspect of our lives, we needed to quickly adapt to virtualization and adjusted our operations accordingly. This is not to say there are no challenges in virtualization, though we also should acknowledge that the adaptation has been with a pace that is uncharacteristically fast for all of us, including our umbrella organization IEEE. We have even seen some positive impacts that would have been more challenging to achieve in the previous normal.

Our new journal JSAIT under the leadership of Andrea Goldsmith has published its first issue, and has exceeded the already high expectations set by the society and the IEEE both in terms of attracting a large number of high quality submissions and financially. The second issue is nearing its completion; the first five issues are now set with their editorial teams and timelines. We owe tremendous gratitude to Prof. Goldsmith and the guest editors who work tirelessly to ensure timely publication of outstanding papers that show the impact of information theoretic thinking in fields such as learning, quantum, security and others. I hope that you will find this new member benefit a valuable resource for your research and professional development.

We are now preparing to launch our new magazine IEEE BITS. Like JSAIT, this new publication is also several years in the making with diligent efforts of the magazine committee under the leadership of Christina Fragouli. The magazine will start publishing in 2021 under the leadership of Rob Calderbank. We thank Prof. Fragouli and the committee for

spearheading this effort and Prof. Calderbank for accepting this pioneering role for our society.

Speaking of member benefits, I would like to mention a couple of additional initiatives we have started with the goal of improving our membership numbers and retention. First, in partnership with IEEE, we are running a half-year membership campaign targeting IEEE members who are not members of our society, but have expressed interest in their technical profile. Instead of the usual half of the yearly dues, this year (due to the special circumstances) we are able to offer this for free. I am pleased to report that we are about 25% up from where we were in mid-May, and we are now over 3500 strong.

We also have worked with IEEE to adjust our dues for 2021. I am delighted to announce that in 2021, our student members will be able to sign up for our society for one dollar. Our regular membership fee is also reduced to twenty-five dollars.

As part of adapting to our new normal, our board of governors has passed a record number of motions to accommodate the changing landscape in March and April. We have posted all the changes in a dedicated web page (https://www

(continued on page 22)





Aylin Yener



ISSN 1059-2362

From the Editor

I hope everyone is doing well during these challenging times. We start with the president's column updating us on different issues in our society. This issue features a technical contribution on a new update to the Information Theoretic Inequality Prover (ITIP). We continue with a report on the 2020 Eduard Rhein Technology Award. We also have the minutes from the Board of Governors meeting in San Diego past February.

This May witnessed the first issue of our new journal, the IEEE Journal on Selected Areas in Information Theory (JSAIT), which focuses on deep learning. You can find here the front cover and table of contents of JSAIT's first issue. With sadness, we conclude this issue with tribute to Vera Pless who passed away in March 2020.

Salim El Rouayheb

As a reminder, announcements, news, and events intended for both the printed newsletter and the website, such as award announcements, calls for nominations, and upcoming conferences, can be submitted at the IT Society website http://www.itsoc.org. Articles and columns can be e-mailed to me at salim.elrouayheb@rutgers.edu with a subject line that includes the words "IT newsletter."

The next few deadlines are:

July 10, 2020 for the issue of September 2020.

October 10, 2020 for the issue of December 2020.

January 10, 2021 for the issue of March 2021.

Please submit plain text, LaTeX, or Word source files; do not worry about fonts or layout as this will be taken care of by IEEE layout specialists. Electronic photos and graphics should be in high resolution and sent as separate files.

Salim El Rouayheb

IEEE Information Theory Society Newsletter

IEEE Information Theory Society Newsletter (USPS 360-350) is published quarterly by the Information Theory Society of the Institute of Electrical and Electronics Engineers, Inc.

Headquarters: 3 Park Avenue, 17th Floor, New York, NY 10016-5997.

Cost is \$1.00 per member per year (included in Society fee) for each member of the Information Theory Society. Printed in the U.S.A. Periodicals postage paid at New York, NY and at additional mailing offices.

Postmaster: Send address changes to IEEE Information Theory Society Newsletter, IEEE, 445 Hoes Lane, Piscataway, NJ 08854.

© 2020 IEEE. Information contained in this newsletter may be copied without permission provided that the copies are not made or distributed for direct commercial advantage, and the title of the publication and its date appear.

IEEE prohibits discrimination, harassment, and bullying. For more information, visit http://www.ieee.org/web/aboutus/ whatis/policies/p9-26.html.



Table of Contents

President's Column 1
From the Editor 2
AITIP: Automated Information Theoretic Inequality Prover
Awards
IEEE Information Theory Society Board of Governors Meeting 11
A Tribute to Vera Pless (1931–2020)
JSAIT
Recent Publications
Call for Papers
Conference Calendar



AITIP: Automated Information Theoretic Inequality Prover

Chee Wei Tan[†], Lin Ling[†], Siu-Wai Ho^{*}, and Raymond W. Yeung[‡] City University of Hong Kong[†], University of Adelaide^{*}, The Chinese University of Hong Kong[‡]

1 Introduction

Computers as a form of learning machine to study the principles of reasoning and valid logical inference of mathematical statements have been recognized by C. E. Shannon in the early 1950's [1]. Since then, computers have become an indispensable tool in automated theorem proving, being instrumental in achieving significant milestones in mathematics such as validating or proving important mathematical results in the Principia Mathematica [2] and the Four Color Theorem in graph theory [3]. It is therefore to be expected that automated reasoning and logical inference by computers can be instrumental to the development of the mathematical subject of information theory and its related field of coding theory.

Very often, in order to prove converse theorems in information theory and coding theory, we may need to verify the correctness of a given information theoretic inequality, and obtain a proof or a counterexample, but doing this manually can be tedious when the inequality involves more than a few random variables. Luckily, there are well-known software packages such as ITIP (Information Theoretic Inequality Prover) [4] and Xitip [5] that can be used for to verify the given information theoretic inequality. The ITIP is a Matlab software package while the Xitip is an implementation of the ITIP using the C programming language. The idea is to leverage the linear programming based framework in [6], and these software packages can verify the given information inequality by simply checking the sign of the optimal objective value in the corresponding linear program.

Despite what their names suggest, ITIP and Xitip are actually only verifiers and are not provers. They can only verify the correctness of a given information inequality (e.g., by outputing "True" or "Not provable by ITIP"). In practice, it is more desirable to have the analytic proofs and disproofs, as these are the formal ways of proving information inequalities, and they can give us further insights of the inequalities of interest. One important insight is about the necessary and sufficient conditions for the equality to hold. Consider the information inequality

$$I(A; B|C, D) + I(B; D|A, C) \leq I(A; B|D) + I(B; D|A) + H(A; B|D),$$
(1)

which can be proved by showing

$$I(A; B|D) + I(B; D|A) + H(AB|D) - I(A; B|C, D) - I(B; D|A, C)$$
(2)

$$= H(B|A, C, D) + H(A|B, C, D) + I(B; C|A) + I(A; B|D) + I(A; C|D)$$
(3)

$$\geq 0,$$

where (3) can be easily verified by expressing all the qualities on both sides in terms of joint

entropies. Then we can further deduce that the equality in (1) holds if and only if all the qualities on the right side of (3) are equal to zero.

To provide a systematic search for analytic proofs or counterexamples, we have developed a theoretical framework based on convex optimization that can generate an analytic proof when the information inequality is indeed true, and provide a set of hints to construct a counterexample when the information inequality is incorrect [7]. *Duality* plays a significant role in our theoretical framework, particularly Lagrange duality in convex optimization [8] and related notions such as sparsity and dual-based methods. We have also created an online web-based platform called AITIP at https://aitip.org that is freely-available and can be readily used by anyone in the world (free from software dependency or backward compatibility in software installation).

2 Proving and Disproving Information Inequalities

In this section, we briefly describe this optimization-theoretic framework. The details are available in [7].

Finding constraints on joint entropy and mutual information, mostly in the form of information inequalities is a subject of interest in information theory, and inequalities that can be proved as such are collectively called Shannon-type inequalities [9]. Consider n random variables (X_1, X_2, \ldots, X_n) and the (joint) entropies of all the non-empty subset of these random variables form a column vector **h**. For example, if n = 3, then

$$\mathbf{h} = [H(X_1) \ H(X_2) \ H(X_3) \ H(X_1, X_2) H(X_2, X_3) \ H(X_1, X_3) \ H(X_1, X_2, X_3)]^T.$$
(4)

The coefficients related to an information inequality can be denoted by a column vector **b**. To illustrate, continue the example of **h** in (4). Then, the information inequality $-H(X_1, X_3) + H(X_1, X_2, X_3) \ge 0$ is denoted by

$$\mathbf{b}^T \mathbf{h} \ge 0$$

with $\mathbf{b} = \begin{bmatrix} 0 & 0 & 0 & 0 & -1 & 1 \end{bmatrix}^T$. Due to the nonnegativity of Shannon's information measures, we know that \mathbf{h} must satisfy certain inequalities. For example,

$$H(X_1) + H(X_2) - H(X_1, X_2) = I(X_1; X_2) \ge 0,$$

$$H(X_1, X_2) - H(X_2) = H(X_1 | X_2) \ge 0.$$

The set of all the inequalities due to the nonnegativity of Shannon's information measures is defined as the *basic inequalities*. Note that this set is not minimal in the sense that some basic inequalities can be implied by others. Let $\mathcal{N} = \{1, 2, ..., n\}$, a minimal subset of the basic inequalities is defined as the *elemental inequalities* [10, P. 340], namely

$$H(X_i|X_{\mathcal{N}-i}) \ge 0,$$

$$I(X_i;X_j|X_{\mathcal{K}}) \ge 0 \text{ where } i \ne j \text{ and } \mathcal{K} \subseteq \mathcal{N} - \{i,j\},$$

and these elemental inequalities are denoted by

$$\mathbf{Dh} \ge \mathbf{0}.\tag{5}$$

Obviously, any vector **h** must satisfy (5). An important property about this set is that all the inequalities due to the nonnegativity of Shannon's information measures, like $H(X_1) \ge 0$,

 $H(X_1, X_2|X_3) \ge 0$, etc., can be obtained as a conic combination (also known as a nonnegative linear combination) of the elemental inequalities. Therefore, an information inequality can be proved by using the nonnegativity of Shannon's information measures if and only if the inequality can be implied by the elemental inequalities. An information inequality, which is implied by the nonnegativity of Shannon's information measures, is called *Shannon-type inequality*.

Very often we want to prove an information inequality $\mathbf{b}^T \mathbf{h} \ge 0$ subject to a given set of equality constraints $\mathbf{E}\mathbf{h} = \mathbf{0}$. When there is no equality constraint, this set is simply empty.

The linear combination of the joint entropies $\mathbf{b}^T \mathbf{h}$ is a valid information inequality if and only if it is always nonnegative [6]. Consider the following linear program:

$$\begin{array}{ll} \text{minimize} & \mathbf{b}^T \mathbf{h} \\ \text{subject to} & \mathbf{D} \mathbf{h} \geq \mathbf{0} \\ & \mathbf{E} \mathbf{h} = \mathbf{0} \end{array} \tag{P-Proof}$$
variables: \mathbf{h} ,

and its Lagrange dual problem (also a linear program):

$$\begin{array}{ll} \text{maximize} & \mathbf{y}^T \mathbf{0} \\ \text{subject to} & \mathbf{D}^T \mathbf{y} = \mathbf{b} + \mathbf{E}^T \boldsymbol{\mu} \\ & \mathbf{y} \ge \mathbf{0} \\ \text{variables:} & \mathbf{y}, \, \boldsymbol{\mu}, \end{array}$$
(D-Proof)

it can be shown that, when the input information inequality is provable, the optimal solution of (D-Proof), \mathbf{y}^* , can be used to construct the analytical proof. The cardinality of the optimal solution, $\|\mathbf{y}^*\|_0$, equals the number of elemental inequalities used in the proof.

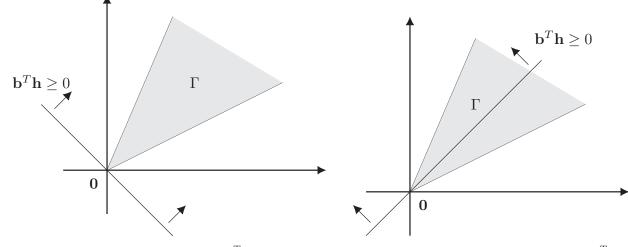
It is particularly interesting to observe that the primal problem (P-Proof) captures the convex cone spanned by entropic vectors and has a geometric interpretation [9] that reduces some network information theory problems to convex optimization or provides impetus to new constraints on the von Neumann entropy in quantum mechanics.

Furthermore, the primal problem (P-Proof) and dual problem (D-Proof) represent the geometric and algebraic aspects of the problem of proving information inequalities, respectively. The optimal value of (P-Proof) is zero if $\mathbf{b}^T \mathbf{h} \ge 0$ is a Shannon-type inequality, and is $-\infty$ otherwise [10, Theorem 14.4]. The two cases are illustrated geometrically in Fig. 1, where Γ represents the feasible region of (P-Proof). Because we are comparing the optimal value of a linear program with 0, the primal problem represents the geometric aspect. The dual constraint in (D-Proof), $\mathbf{D}^T \mathbf{y} = \mathbf{b} + \mathbf{E}^T \boldsymbol{\mu}$, can be interpreted as reconstructing \mathbf{b} as a linear combination of rows in constraint matrices \mathbf{D} and $-\mathbf{E}$ by finding the weights of the rows, and therefore the dual problem is considered the algebraic aspect.

Now, we turn to a reformulation of the linear program that, unlike (P-Proof), is bounded and thus allows both proof and counterexample hints to be determined with a single linear program. Consider

minimize $\mathbf{b}^T \mathbf{h}$ subject to $\mathbf{0} \le \mathbf{D} \mathbf{h} \le \mathbf{1}$ $\mathbf{E} \mathbf{h} = \mathbf{0}$ (P-Merge) variables: \mathbf{h} ,

and its dual problem



(a) Γ is contained in the half-space $\mathbf{b}^T \mathbf{h} \ge 0$. In this case, $\mathbf{b}^T \mathbf{h} \ge 0$ is a Shannon-type inequality.

6

(b) Γ is not contained in the half-space $\mathbf{b}^T \mathbf{h} \geq 0$. In this case, $\mathbf{b}^T \mathbf{h} \geq 0$ is either not true in general or a non-Shannon-type inequality.

Figure 1: Geometric illustration of the relation between the feasible region Γ and the half-space $\mathbf{b}^T \mathbf{h} \geq 0$, assuming that there is no problem-specific constraint, i.e., \mathbf{E} is empty. The figures considering problem-specific constraints can only be drawn in 3-D and can be found in [10, 13.3.2].

$$\begin{array}{ll} \text{maximize} & -\mathbf{1}^T \boldsymbol{\lambda}_{\mathbf{2}} \\ \text{subject to} & \mathbf{b} - \mathbf{D}^T \boldsymbol{\lambda}_1 + \mathbf{D}^T \boldsymbol{\lambda}_2 + \mathbf{E}^T \boldsymbol{\mu} = \mathbf{0} \\ & \boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \geq \mathbf{0} \\ \text{variables:} & \boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \boldsymbol{\mu}, \end{array}$$
(D-Merge)

we have the following results [7].

Theorem 1. Both (P-Merge) and (D-Merge) have finite optimal solutions (i.e., they are "solvable").

Theorem 2. A set of optimal solutions to (D-Merge), $[\lambda_1^{*T} \ \lambda_2^{*T} \ \mu^{*T}]^T$, can be used to construct a proof or hints of counterexample to the information inequality $\mathbf{b}^T \mathbf{h} \geq 0$.

These two theorems are essential as they show that any information inequality (assuming it is not non-Shannon-type) can be proved or disproved by solving *a single* linear program that is guaranteed to be "solvable". The implication is that a unified computational approach to prove or disprove an information inequality can be developed. Hence, in developing optimization algorithms to solve the linear programs (P-Merge) and (D-Merge), we seek to find an optimal dual solution with the smallest cardinality, corresponding to searching for the shortest proof or the smallest counterexample. We refer the readers to [7] for more details on designing fast optimization algorithms based on the recently-popularized alternating direction method of multipliers [11].

3 AITIP Web Service Overview

The core of the AITIP software is a command line tool written in C++ and Python, and the source code is available at https://github.com/convexsoft/AITIP. The command line tool

comes with a basic CPU solver and an accelerated GPU solver, and users can invoke either of them depending on their needs. The AITIP web service at https://aitip.org is a hosted version of the command line tool offering an easy to use interface as a free service to anyone without the hassles of software installation and dependencies management. Currently, this AITIP web service is hosted on a cloud server without a GPU, and can typically handle a problem with around fifteen random variables or less. The AITIP web service thus enhances usability and convenience to a larger number of users via a software-as-a-service paradigm. For problems of bigger size, in order to get the optimal performance, we recommend downloading the source code and run the tool locally on a GPU-enabled machine for proving large scale information inequalities.

Here we show some representative examples to demonstrate the usage of AITIP.

Example 3.1.

Suppose we want to prove the data-processing inequality

 $I(X;Y) \ge I(X;Z)$ if X, Y and Z form a Markov chain.

In the web service, we can type in $I(X;Y) \ge I(X;Z)$ as the objective function and $X \longrightarrow Y \longrightarrow Z$ as the user-defined constraint. With the command line tool, the same inequality can be proved by invoking

python3 main.py -i "I(X;Y) >= I(X;Z)" -u "X -> Y -> Z".

Optionally, by passing in an extra flag --gpu, we can invoke the GPU solver which offers better performance for large scale information inequalities. With both the web service and the command line tool, AITIP can generate the following proof for the above inequality

Input: H(X) + H(Y) - H(X,Y) - H(X) - H(Z) + H(X,Z) >= 0.0 User constraints: H(X,Y) + H(Y,Z) - H(X,Y,Z) - H(Y) = 0.0 The objective can be written as: H(Y) - H(X,Y) - H(Z) + H(X,Z)=[-H(Z) + H(X,Z) + H(Y,Z) - H(X,Y,Z)] -{-H(Y) + H(X,Y) + H(Y,Z) - H(X,Y,Z)} >=0 where expressions in [] are non-negative due to elemental inequalities, and expressions in {} are zero due to the user specified constraints.

Example 3.2.

The Shannon's perfect secrecy theorem is a classic result in information theory, and it can be represented as the following information inequality

$$H(U) \le H(R)$$
 if $I(U; X) = 0$ and $H(U|R, X) = 0$.

To prove it with the AITIP web service, we can type in $H(U) \leq H(R)$ as the objective function and I(U;X) = 0 and H(U|R,X) = 0 as user-defined constraints in two separate lines. To prove it with the command line tool, we can invoke the following command python3 main.py -i " $H(U) \le H(R)$ " -u "I(U;X) = O/H(U|R,X) = 0".

Notice that multiple user-defined constraints can be separated by / in the command line parameter -u. The proof generated by AITIP is given below

```
Input: -H(U) + H(R) >= 0.0
User constraints:
H(U) + H(X) - H(U,X) = 0.0
H(R,U,X) - H(R,X) = 0.0
The objective can be written as:
H(R) - H(U)
=[-H(U,X) + H(R,U,X)]
+[H(R) + H(X) - H(R,X)]
-{H(U) + H(X) - H(U,X)}
-{-H(R,X) + H(R,U,X)}
>=0
```

where expressions in [] are non-negative due to elemental inequalities, and expressions in {} are zero due to the user specified constraints.

Example 3.3.

Now consider the following (untrue) information inequality

 $I(X;Y) \ge H(X|Y).$

By typing in I(X;Y) >= H(X|Y) as the objective function in the web service or invoking

python3 main.py -i "I(X;Y) >= H(X|Y)"

in the command line, we can obtain some hints given by AITIP

```
Input: H(X) + H(Y) - H(X,Y) - H(X,Y) + H(Y) \ge 0.0
Canonical form: H(X) + 2.0H(Y) - 2.0H(X,Y) \ge 0
We cannot prove the given inequality, which means it is one of these two cases
1) The inequality is a non-Shannon-type inequality.
2) The inequality is not true.
If it is case 2), a disproof can be constructed using the following hints:
A counter example can be constructed as a probability distribution satisfying all of the following conditions
-H(X) + H(X,Y) = 0
H(X) + H(Y) - H(X,Y) = 0
H(X,Y) = 1
```

8

From the hints, we can deduce that a probability distribution satisfying H(X) = 1 and H(Y) = 0 can be used as a counterexample. Indeed, it is easy to verify that in this case I(X;Y) = 0 and H(X|Y) = 1.

4 Open Issues

Our paper in [7] can be viewed as a case study of the "automated reasoning by convex optimization" approach [12] to automate the tasks of reasoning and logical deduction of information inequalities. The theoretical framework in [7] and the AITIP web service can be further improved. Let us list down several open issues.

The current version of AITIP attempts to prove a given information inequality by checking whether it can be represented as a conic combination of the set of *elemental inequalities*. This strategy however fails when the input is a non-Shannon-type inequality, because *absence of evidence is not evidence of absence*. Indeed, since the discovery by Z. Zhang and R. W. Yeung in 1998 of the first non-Shannon-type information inequality, which is a linear inequality for entropies of four random variables that cannot be reduced to the basic Shannon inequalities [10, Chapter 15]):

H(X,U) + H(X,V) + 3(H(U,V) + H(V,Y) + H(U,Y)) $\geq 2H(U) + 2H(V) + H(Y) + H(X,Y) + H(U,V,X) + 4H(U,V,Y),$

there has been many more non-Shannon-type inequalities being discovered. If a non-Shannon type inequality is used as input, the current version of AITIP would report that it is not provable. It is interesting to generalize our framework to handle both Shannon and non-Shannon type information inequalities.

This can be improved by expanding the 'knowledge' of AITIP from a set of elemental inequalities to include all the known non-Shannon-type inequalities. Then the ability of AITIP would depend on the characterization of the non-Shannon-type information inequalities which is still an important open problem.

If an information inequality cannot be represented as a conic combination of the set of elemental inequalities, it may be not true in general. If this is the case, a counterexample can be searched to disprove the information inequality being queried. As can be seen from the example in Section 3, the current version of AITIP can only give hints instead of an explicit counterexample to disprove the inequality. In some cases, careful inspection from trained human eyes is needed to construct a correct counterexample from the hints given by AITIP. How to automatically generate counterexamples from the hints is an interesting open problem. This would be the next step to making the AITIP web service a fully automated information theoretic inequality prover.

There are also several open issues related to the development of convex optimization-based algorithms for proof search in large-scale problems. Firstly, solving the linear program in [7] remains a huge challenge as its dimension increases exponentially with the number of random variables. An information inequality involving many random variables results in a highly-degenerate linear program that can be numerically ill-conditioned. Secondly, the logical correctness in mathematical reasoning cannot be susceptible to computational issues such as inaccurate numerical approximation or floating-point errors. Thirdly, distributed computation for solving the high-dimensional optimization problems are needed, requiring highly specialized optimization algorithms to be integrated with powerful hardware accelerators, e.g., dedicated graphic-processing unit (GPU). Last but not least, an end-to-end method to explore the proof space, refine problemspecific constraints and to automatically construct a formal proof or valid counterexample requires more in-depth investigation.

References

- C. E. Shannon, "Computers and automata," *Proceedings of IRE*, vol. 41, pp. 1234–1241, 1953.
- H. Wang, "Computer theorem proving and artificial intelligence," Automated Theorem Proving: After 25 years, American Mathematical Society, Contemporary Mathematics, vol. 29, pp. 49–70, 1984.
- [3] A. Kenneth and H. Wolfgang, "Every planar map is four-colorable," Contemporary Mathematics, With the collaboration of J. Koch., American Mathematical Society, vol. 98, 1989.
- [4] R. W. Yeung and Y. O. Yan, Information Theoretic Inequality Prover (ITIP), Matlab program software package available at: http://home.ie.cuhk.edu.hk/ ITIP, 1999.
- [5] R. Pulikkoonattu and S. Diggavi, *ITIP-based C program software package, available at:* http://xitip.epfl.ch, 2006.
- [6] R. W. Yeung, "A framework for linear information inequalities," *IEEE Trans. on Informa*tion Theory, vol. 43, no. 11, pp. 1924–1934, 1997.
- [7] S.-W. Ho, L. Ling, C. W. Tan, and R. W. Yeung, "Proving and disproving information inequalities: Theory and scalable algorithms," *IEEE Trans. on Information Theory*, 2020.
- [8] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.
- [9] R. W. Yeung, "Facets of entropy," *IEEE Information Theory Society Newsletter*, vol. 62, no. 8, 2012.
- [10] —, Information Theory and Network Coding. Springer, 2008.
- [11] N. Parikh and S. Boyd, "Proximal algorithms," Foundations and Trends in Optimization, vol. 1, no. 3, pp. 127–239, 2014.
- [12] C. W. Tan and L. Ling, "Automated reasoning by convex optimization: Proof simplicity, duality and sparsity," in 54th Annual Conference on Information Sciences and Systems (CISS). IEEE, 2020.

Awards

2020 Eduard Rhein Technology Award for Neal Koblitz and Victor Miller

Neal Koblitz and Victor Miller

are the recipients of the 2020 Ed-

uard Rhein Technology Award

for the invention of ellipticcurve cryptography. Their core

idea was to replace the "multi-

plicative group of a finite field"

with the "group of points on an

elliptic curve over a finite field".

This idea was practically impor-

tant because problems such as

computing discrete logarithms

seem to be significantly more

difficult in the second group

than the first. This means, e.g.,

that elliptic-curve cryptogra-



Neil Koblitz, PhD

phy requires only 283-bit keys to achieve the same level of security as the 3000-bit keys of earlier methods. Furthermore, the ten-fold reduction in key length lets cryptographic devices operate with higher speed, smaller memory, and less energy.

In 2013, the U.S. National Institute of Standards and Technology (NIST) recommended elliptic curve cryptography for key exchange through an algorithm called Elliptic Curve Diffie Hellman (ECDH), and for digital signatures through an algorithm called the Elliptic Curve Digital Signature Algorithm (ECDSA). Furthermore, the U.S. National Security Agency allowed using these algorithms to protect information classified up to top secret with 384-bit keys. Today, elliptic curves are used by applications such as Bitcoin, Transport Layer Security (TLS) based web browsing, and many others.

Neil Koblitz received a Bachelor of Arts from Harvard University in 1969 and a Ph.D. from Princeton University in 1974. He has been with the University of Washington since 1979. Shortly before inventing elliptic curve cryptography, in 1984 he published the textbook "Introduction to Elliptic Curves and Modular Forms" with, in his words, down-to-earth examples that aim to make the material readable and interesting. He has received several recognitions for his work, including an RSA Excellence in Mathematics Award in 2009 together with Victor Miller.



Victor Miller was born in Brooklvn, New York, and he learned about elliptic curves as a freshman in college in 1964 when these objects were, in his words, an interesting but arcane piece of mathematics. He studied mathematics at Columbia University and Harvard from 1964-75. He joined the University of Massachusetts in 1973, IBM in Yorktown Heights in 1978, and the Center for Communications Research (CCR) of the Institute for Defense Analyses in Princeton, New Jersey, in 1993.

Victor S. Miller, PhD

Through their invention of elliptic curve cryptography, Neal Koblitz and Victor Miller have had a lasting impact on digital technology that is sure to grow over time. Their application of fundamental mathematics to a problem of great engineering and social relevance has made possible a secure and efficient communication over the internet.

Eduard Rudolph Rhein was born in 1900 in Königswinter and died in 1993 in Cannes. The Eduard Rhein Technology Award has been awarded annually since 1979. The award ceremony will be held in the Hall of Fame of the Deutsches Museum in Munich in November.

IEEE Information Theory Society Board of Governors Meeting

Location: San Diego, CA

Date: February 2nd, 2020

Time: The meeting convened at 1:00 pm PST; the meeting adjourned at 6:45 pm PST

Meeting Chair: Aylin Yener

Minutes taken by: Lara Dolecek

Meeting Attendees: Erik Agrell, Jeff Andrews, Matthieu Bloch, Suhas Diggavi (*), Alex Dimakis, Lara Dolecek, Stark Draper (*), Elza Erkip, Christina Fragouli (*), Andrea Goldsmith, Babak Hassibi (#,*), Syed Jafar (#), Sid Jaggi (*), Tara Javidi, Jeorg Kliewer (#), Vijay Kumar, Brian Kurkoski (*), Matt LaFleur (#), Olgica Milenkovic (*), Prakash Narayan, Alon Orlitsky (#), Henry Pfister (*), Vince Poor (*), Joachim Rosenthal, Parastoo Sadeghi, Anand Sarwate (#), Igal Sason, Daniela Tuninetti, Aaron Wagner, Aylin Yener, Wei Yu

Remote attendees are denoted by (*); non-voting attendees are denoted by (#).

Business conducted between meetings: The following votes were conducted by email between the Oct. 2019 Information Theory Society (ITSoc) Board of Governors (BoG) meetings and this meeting:

11

- 1) In December 2019, BoG approved the meeting minutes from the last meeting.
- 2) In January 2020, The N&A committee nominated Stark Draper as the chair of the Diversity and Inclusion Committee. BoG voted and elected Stark Draper.

At 1:00 pm local time, ITSoc president Aylin Yener called the meeting to order.

Attendees introduced themselves. President Yener thanked everyone for joining the meeting.

Motion: A motion was made to approve the agenda.

The motion passed.

President's Report-Aylin Yener

President Yener started by first thanking everyone for their service, welcoming new members, and congratulating members on their distinguished awards. She extended thanks first to Frank Kschischang, who served in multiple roles, including the positions of Senior Past President (SPP), Chair of the Constitutions and Bylaws Committee, and the Chair of the Nominations & Appointments Committee Chair. She extended special thanks to Frank for his major Bylaws effort last year and for stepping in for the position of the Junior Past President (JPP) in 2018. She next thanked Emina Soljanin for her ongoing service, who has also served in multiple roles, including as the Society's President in 2019, the Chair of Shannon and Wyner award committees, Ex-officio on several others, and as the JPP in 2020. President Yener next thanked Elza Erkip for her ongoing service, which has included the position of the JPP in 2019, major efforts for the extensive bylaws revisions last year, a member and then the chair of the Nominations and Appointments committee, chair of the Diversity and Inclusion committee, and the Senior Past President in 2020. President Yener next thanked former BoG members: Sasha Barg, Andrew Barron, Steven Hanly, Michele Wigger, and Greg Wornell, for their service. She next thanked all the members of the following committees: Nominations and Appointments Committee: Gerhard Kramer; Conference Committee: Brian Kurkoski and Alfonso Martinez; Paper Awards Committee: Sae-Young Chung, Alex Dimakis, Negar Kiyavash, Khrishna Narayanan, Antonia Tulino, and Michele Wigger; Shannon Committee: Janos Korner and David Tse; Wyner Committee: Bruce Hajek and Muriel Medard; Massey Committee: Erdal Arıkan, Tom Fuja (chair), and Tara Javidi; Cover Committee: Yossi Steinberg; Fellows Committee: Ning Cai and Max Costa.

Next, president Yener welcomed new BoG members: Erik Agrell (Region 8), Meir Feder (Region 8), Camilla Hollanti (Region 8), Sid Jaggi (Region 10), Alex Dimakis (re-elected), Tara Javidi (re-elected), and Joachim Rosenthal (Region 8). She also thanked many new volunteers on a number of committees. She reported that the current BoG composition is 11 female and 15 male members, and that there are 6 members from Region 8, and 3 members from Region 10, indicating significantly improved geographic diversity.

President Yener next stated that Stark Draper has been elected as the New Diversity and Inclusion Committee Chair, based on the nomination by the N&A committee and email BoG vote conducted in January 2020. She also extended special thanks to inaugural members of this committee since 2018, who were Elza Erkip (chair), Stark Draper, Sid Jaggi, Tara Javidi, Muriel Medard, and Emanuele Viterbo. Next, President Yener stated that Lara Dolecek and Aaron Wagner were reappointed based on the email BoG votes into their positions as the Society's Secretary and Treasurer, respectively.

President Yener next went over the presidential appointments for 2020. Tara Javidi was appointed as the Women in Engineering (WiE) representative. Tara is a Professor of Electrical and Computer Engineering at UCSD, the Founding Co-Director Center for Machine Integrated Computing and Security at UCSD, and also an Elected Board Member ITSoc. Parisa Hassanzadeh was appointed as the Young Professionals (YP) Representative. Parisa is a Research Scientist at J.P. Morgan AI Research. She received her PhD in Electrical Engineering from NYU in 2019.

Next, President Yener congratulated the ITSoc members who were elected IEEE Fellows in Class of 2020. She also congratulated the following members for their technical field awards: Anders Lindquist, Alfred Hero III, Shu Lin, and Balaji Prabhakar.

President Yener next went over the status of new bylaws, stating that the changes were fully approved by the IEEE, and that they are available on-line. She reiterated that the major bylaw overhaul was done by Frank and Elza and that bylaws contain many answers to how the society operates.

She then went over the new avenues of dissemination and recognition. The society now has two flagship journals: Transactions on Information Theory and the Journal on Selected Areas of Information Theory, with the latter providing outreach to fields interfacing information theory. She also stated that the society also has two named lectureships at IT schools, Padovani and Goldsmith, the latter specifically designated for a female young researcher. The inaugural Goldsmith Lecturer is Ayfer Ozgur.

President Yener next stated that ITSoc membership certificates are newly available in 2020. They can be accessed by logging into Collaboratec with own IEEE info, and are then populated with the individual's name. She thanked Matt for facilitating this new operation.

Next, president Yener went over the open calls for awards and recognitions, stating the importance of recognizing colleagues for their outstanding work. She invited society and BoG members to think of one paper or person deserving of an award, invest and to pay it forward, in order to further increase the number of nominations and recognitions. Next, President Yener discussed how certain society volunteers have already done a lot for the community and that the service overload might end up exhausting volunteers. She suggested that it would be a good idea to keep a record of how many different roles one is serving in at the same time so as to better balance the load and influence. President Yener and Matt will work to streamline the record keeping of who is on what committee and in what volunteer positions.

President Yener next discussed the goals for 2020. She highlighted the key theme for the upcoming year: openness and engagement. The goals include better communication between society volunteer committees and operations, better process of informing and equipping volunteer selection, and improvement of membership numbers. She highlighted that being in the IT community means being an active member of the IT Society.

Next, President Yener talked about Inclusiveness and Transparency. She stated that her goals are to continue efforts on improved inclusiveness and transparency. She stated that a more diverse group of the volunteers and members the society has, the richer and broader set of new ideas and perspectives can arise. She said that in this context, the acronym IT stands for both Information Theory as well as Inclusion and Transparency. She concluded her presentation by welcoming the members to the new decade of IT.

Treasurer's Report-Aaron Wagner

Aaron Wagner in his capacity as the Society's Treasurer presented his report. He started by recapping the IEEE accounting practices. He reminded the board that there are fixed boundaries between fiscal years, and that the general operating funds and special funds are disjoint. He stated that the IEEE foundation covers separately the expenses for the Shannon movie and the Padovani Lectureship.

Next, Aaron went over the 2019 general funds. He presented the funds status as a conditional expectation, that increases with each reporting date. Expected budgeted surplus for 2019 is \$46k. The expected budgeted surplus for 2019 at time of ITA 2020 is \$453k. He stated that this amount is due to several factors. Notable sources of deviation include: IT Transactions revenue of \$232k, decrease in IT Transactions cost of \$43k, conference publications revenue increase of \$67k, ISIT 2019 in Paris surplus is up \$52k, and dues are up \$2.6k. Aaron clarified that IEEE runs seasonal promotions to reduce membership cost towards the end of the year so that the membership profit is not just simply the number of members times the membership fee.

Next, Aaron presented trends of the IT Transactions. He first presented the chart available at ISIT 2018 in Vail, when the numbers suggested a cause for concern.

President Aylin Yener explained that bumps in curves were due to switching to light editing and more complicated formula. Aaron stated that Open Access, clicks on articles, and institutional membership all contribute to an increase in the revenue. Next, Aaron discussed the 2019 Special Projects. He went over the budget breakdown, \$120k is due to the 3% rule for the special projects and \$145k is due to the 50% rule for general funds, yielding the available total of \$265k. Aaron provided the list of 10 special projects and their leaders, along with the individual budgets. The total for the 10 special projects was \$264.5k.

Next, Aaron presented the status of the 2020 Special Projects. The total allowed is \$314k, of which \$89k is due to the 3% rule for the special projects and the remaining \$225k is due to the 50% for the general funds. Aaron presented a list of 10 special projects, their organizers and budgets, that are already approved by the officers or BoG. The sum total for these 10 projects is currently \$127k. Aaron encouraged members to submit other ideas as well, given the availability of funds which are subject to use it or lose it rules. He also reminded the members that the receipts must be submitted by December 15, 2020, and that members should also start thinking about the 2021 Special Projects.

Aaron then went over the 2020 General Funds. He stated that the expected surplus is \$243k, and that we should aim to meet this target. He also reminded of the situation we were in 2 years ago, and that while the budget looks much better now, we cautioned that this could be easy come, easy go money. His recommendation is to find ways of using our current surplus to strengthen the Society moving forward, and in particular to try to find ways to use the money to attract new society members.

Aaron next went over the status of the Padovani fund, stating how that Roberto Padovani generously donated \$110K over 5 years, and that the Society is permitted to spend \$10K/year of it on Schools. Moving forward, the payout may be adjusted to allow for spending in timely manner while being in accordance with existing rules.

Aaron then described what constitutes an IEEE New Initiative, and also discussed the financial impact of JSAIT on the society's budget. He stated that the projection is having 4 issues per year, with \$55k in expenses and the net deficit of \$1k.

Publications Committee: Transactions on Information Theory—Igal Sason

Next presentation was given by Igal Sason in his capacity as the Editor-in-Chief of the IT Transactions.

Igal first provided the overview of the editorial areas and the current number of associate editors per area as of Jan. 2020. He explained that the "At Large" category refers to editors who are typically asked to handle mathematical papers that are not explicitly assigned to a given technical area. He also stated that he and the Executive Editor Erdal Arıkan exchange around 300 emails monthly in regards to the operations of the IT transactions. He also stated that the editorial load is about 1.4 new papers monthly plus revisions.

Next he went over considerations for selecting associate editors (AEs). He stated that it is expected that the prospective AEs have demonstrated academic excellence (e.g., being tenured if in academia), and that they demonstrated a high level of performance as reviewers. He stated that it is also the aim to improve diversity on the editorial board among different dimensions: by having editors from industry as well as academia (2 are now from industry); by improving gender diversity (11 out of 55 current editors are female); and by increasing geographic diversity.

Igal then went over the submission numbers. There were 1364 regular submissions form July 1st 2018 to December 31st 2019. He presented the chart organized by area. For example, for coding theory and techniques there were 12 editors and 350 submissions. He also presented statistics regarding the average monthly number of new paper assignments per AE area. AEs At Large have 2, creating the need to solicit an additional AE At Large. Coding Theory and Techniques area has the average of 1.8, also higher than the overall average of 1.4.

Igal then presented the time duration from submission to first decision, including mean and median. He stated that 55 weeks is the median time from submission to the electronic publication. The average time from the submission to the first decision is 27 weeks and it includes fast rejects which is 8–10% of the submissions.

Next, Igal overviewed the work done by the Editor-in-Chief (EiC) and by the Executive Editor (EE). He stated that the professional compatibility of the EE and EiC compatibility and close cooperation on a daily basis is very important for the functionality of the journal. He provided a list of various issues that are done in full coordination between the EE and EiC, including fast rejects, and resubmitted papers whose technical area is not apparent. Igal then stated that the work done separately by the EE is to assign new submissions to the AEs, communicate with the IEEE, and the Publications Committee. He also stated that the separate work by the EiC is to provide advice to AEs; take care of overdue reviews and overview AE decisions; handle appeals; read decision letters; edit tentative fast-rejection letters; edit each issue of the IEEE Transactions on IT including table of contents; interact with IEEE administration, BoG, and Publications Committee.

Igal then presented the Executive editorial board which consists of the following members: Sasha Barg, Frank Kschischang, Amos Lapidoth, and Prakash Narayan. He then discussed the status of the Invited Papers. One invited cross-cutting article has already appeared as the leading article in the January 2020 issue; the paper is a survey on communication for generating correlation. Two more invited papers are in review one is on cyberphysical systems and one is on deep neural networks. Igal stated that the invited papers are subject to thorough reviews and are handled by Prakash Narayan as AE. Igal stated that Prakash invited these papers for submission when he served as the EiC, and he is now handling them as an AE.

Next, Igal discussed the impact factor of the journal. He noted that the Transactions are back in the Q1 category and that the impact factor improved significantly in 2018.

He stated that it is important to cite papers by their Transactions appearance once it becomes available rather than cite the initial ArXiv paper, and to also cite the Transactions paper instead of its ISIT or ITW pre-cursors, when it is appropriate.

Igal also stated that in 2018 and 2019, the number of submissions was 923 and 966 papers, respectively. He also stated that the page budget for 2020 is 8100 pages. 1287 pages were used for the Jan. and Feb. 2020 issues (15.9 % of total budget). In addition to 12 regular issues, there is also an additional special issue dedicated to the memory of Vladimir I. Levenshtein, titled: From Deletion Correction to Graph Reconstruction. Guest EiC for this special issue is Olgica Milenkovic, and there are 7 Guest Associate Editors.

A BoG member asked and Igal clarified that the Executive Editorial board consists of 3 former EiCs, and Amos, and that the board was selected by Igal.

BoG congratulated IT Transactions leadership for bringing down sub-to-pub time. There was a brief discussion on how to reduce this time frame further. Igal stated that he gets monthly reports and follows up with tardy reviewers. A BoG member suggested to reach out to other EiCs in related fields and get input on their own strategies.

Igal next stated that 9 AEs have terms that are ending in March 2020. He presented the list of proposed new AEs. Biographies of the candidates are available online. After a brief discussion regarding the list of candidates, the following 8 motions were made, while an additional motion was withdrawn after discussion.

Motion: to vote on the election of the following candidates for AEs: Amos Beimel, Thomas Courtade, Marco Dalai, Camilla Hollanti, Tobias Koch, Vincent Tan, Ramji Venkatanaram, and Marcelo Weinberger.

These motions passed.

EiC of the Journal on Selected Areas in IT—Andrea Goldsmith

Next presentation was given by Andrea Goldsmith in her capacity as the EiC of the Journal on Selected Areas in IT.

Andrea first presented the executive summary of JSAIT, including the launch timeline, finalization of the senior editorial and industrial advisory board, number of issues per year, and the scope of the forthcoming issues. She went over the JSAIT leadership structure, editorial board membership, industrial advisory board, and the working list of possible topics for future issues. Topics for issues 1, 2, and 3 are fixed. There are several suggestions made and the board will select topics for the issues 4, 5, 6 based on this list. She reiterated that ideas on future special issues from the IT community are most welcome. Andrea thanked the steering committee who did a lot of work to successfully launch the journal. She said that JSAIT will follow a strict timeline of 5 months from paper deadline to final decision. She also stated that the website for the journal has already been launched.

Andrea next went over the details of the inaugural issue, which is titled "Deep Learning: Mathematical Foundations and Applications to Information Science." Alex Dimakis is the lead guest editor, along with 4 other guest editors. Andrea thanked Alex and other editors for doing a great job with a large number of submissions; she in particular thanked Negar Kiyavash who stepped in to replace a non-responsive editor. Deadline for this issue was in October 2019, and the notifications will be sent in March 2020.

Andrea then discussed the status of the second special issue. This issue will be on Quantum Information Science. The deadline for submission is extended to February 15, 2020. Lead guest editors for this journal are Emina Soljanin and Andreas Winter. There are 5 additional guest editors. It is expected that many papers will be submitted to this timely topic.

Next, Andrea went over the status of the third special issues. This issue will be on Statistical Inference and Estimation. The lead guest editor is Devavrat Shah and there are 6 additional guest editors. Paper submission is in May 2020. Expected publication date in November/ December 2020.

Next, Andrea went over possible colors and styles for JSAIT, and asked that the members provide her with feedback regarding the cover appearance.

Andrea concluded her presentation by stating that launch was successful, that 3 special issues will appear in 2020, which may end up being published in 4 volumes; that the guest editorial teams are working great; and that have been no major issues yet. She requested from the BoG members to send her suggestions on future topics and to advertise CFPs.

A BoG member asked and Andrea clarified that there is no hard limit on the acceptance rate, rather the goal is to accommodate all high quality papers. She also clarified that the page limit is 15, with first 10 printed free of charge, and that supplementary material may be uploaded for free on ieeexplore as a separate pdf.

After a short break, the meeting resumed.

Constitution and bylaws committee-Elza Erkip

Next presentation was given by Elza Erkip on behalf of the Constitution and Bylaws Committee. Members of the committee are SPP Elza Erkip and JPP Emina Soljanin. Elza stated that the bylaws were extensively revised in 2019. She thanked Frank Kschischang for leading this effort. She stated that the changes this year are relatively minor, and she encouraged IT members to inform the committee if bylaws are ambiguous.

As SPP, Elza is also the Chair of the Publications Committee. In this capacity, she went over the oversight of the IT Society publications. She stated that JSAIT and Magazine have Steering Committees. As a discussion item for the board members, she asked if there should be a steering committee for IT Transactions as done for JSAIT and Magazine.

Some BoG member expressed opposition to this idea, stating that there doesn't appear to be a need for it. Other BoG members supported the idea stating the current role of the executive committee moving forward is not clear.

IT Magazine-Elza Erkip

Elza was the presenter of the next item of the agenda, which was on the status of the new IT Magazine. Elza went over the presentation for the TAB Periodicals Committee. The presentation included the status of the magazine title; launch timeline of March 2021; target of 4 issues per year and an annual increase in the number of pages; scope of the publication; need for it that was passed on the polled survey; overlap and complementarities with peer publications; examples of paper sources; roles and responsibilities of the magazine oversight committee, steering committee, EiC, senior editors, and area editors. Financials indicated that the deficit of 50k\$ will decrease over time, and that IEEE magazines typically lose money but are member benefit and to enlarge pool of members and to promote the field.

Elza then went over the Steering Committee, which consists of Dan Costello, Elza Erkip, Christina Fragouli (chair), Ubli Mitra, and Wojtek Szpankowski. She next went over the timeline stating that in November 2019, "IEEE BITS: The Information Theory Magazine," as the name of the magazine was approved by PSPB. She also stated that Phase I submission discussed by the Periodicals Committee at the Technical Activities Board was rejected in November 2019, but that the committee will consider Phase I and II jointly in February 2020. She stated that in January 2020, budget was approved by the Finance Committee and that Phase II was submitted.

Elza clarified that Phase I was likely rejected due to some minor issues and the presentation not being clear in the ppt format. She stated that she will present in person at the next meeting.

The following motion was issued:

Motion: to approve the budget for the magazine.

The motion passed.

The next motion was then issued:

Motion: to approve Phase II proposal.

The motion passed.

The last motion was the following:

Motion: Approve Open Call for EiC (once Phase II proposal is approved by the IEEE).

The motion passed.

Online committee—Brian Kurkoski

Next presentation was given by Brian Kurkoski on behalf of the Online Committee.

Brian went over the current status, and motivated the need to move from Plone to Drupal since expenses are rising and there are problems with the webpage. He informationally presented dollar amounts, and will be making a budget request to BoG in June to support this transition.

Nominations and Appointments Committee-Elza Erkip

Next presentation was given by Elza Erkip on behalf of the Nominations and Appointments Committee. She first went over the committee scope and current members. She then stated committee's goals for this year: 1) to diversify society's committees and positions; 2) to enlarge the pool of volunteers; and 3) to start drafting best practices including how many committees to tap a person for.

She then went over the timeline positions on various committees were filled or being filled. Chair of the 2020 Diversity and Inclusion Committee is Stark Draper, and Emina Soljanin is a member (as JPP). Chair of the 2020 Shannon Award Committee is Aylin Yener (as society's president). Committee has 7 other members, several of whom are former award winners. Chair of the 2020 Wyner Award Committee is Aylin Yener (as society's president). Committee has 4 other members, two of whom are former award winners. The chair of the 2020 Cover Award Committee is Christina Fragouli. Committee has 4 other members. The chair of the 2020 IEEE Fellows Evaluation Committee is Antonia Tulino. Committee has 6 other members. Members of the committee are IEEE Fellows. The chair of the Massey Committee is Tara Javidi, and the committee has 4 more members.

Elza next stated that she is working on putting together the Paper Awards Committee, which needs 6 new members, and 2 need to be BoG members. A BoG member asked and Elza clarified that these committees are to be staffed early since awards deadlines are in spring.

Conference Committee-Vijay Kumar

Next presentation was given by Vijay Kumar as the Chair of the Conference Committee. Vijay started by thanking outgoing members Brian Kurkoski and Alfonso Martinez for their service. He next went over the 2020 committee, which consists of: Vijay Kumar, Emina Soljanin, Aylin Yener, Aaron Wagner, Salman Avestimehr, Chen Li, and Daniela Tuninetti.

He then went over the role of the liaison for ISIT 2020, and thanked Aylin for volunteering for this role. Next, Vijay went over the status of the upcoming ISIT conferences, which were as follows: 2020 Los Angeles—to provide an update in the meeting; 2021 Melbourne—to provide an update in the meeting; 2022—Helsinki—to provide an update in the meeting; 2023 Taipei—nothing to report; 2024 New York (proposed) brief presentation to follow. ISIT 2020 update was provided by Giuseppe Caire. It was stated that the conference will be using CMS submission system, and that there were 771 submissions.

ISIT 2021 update was provided by Parastoo Sadeghi. It was stated that the contract between IEEE and ICSMA (Professional Organizer of the conference) has been executed, that the contract between IEEE and Melbourne Convention Centre will be signed shortly, and that the contract between IEEE and Melbourne Convention Bureau was reviewed and approved by the IT Society (Aylin). It was also state that the plan is to distribute first CFP at ITA 2020.

ISIT 2022 was provided by Camilla Hollanti. It was stated that the organizing committee is awaiting tenders from management companies and EDAs; that it is likely the committee will go with EDAS; and that the process of launching a webpage for ISIT 2022 and plans to discuss Plenary Speaker will be undertaken soon.

Vijay stated that the ISIT 2024 pre-proposal will be to made today. He then reviewed the status of the upcoming ITW events. 2020 ITW in Riva del Garda, Italy, will be presented shortly; 2021 ITW in Kanazawa, Japan, has nothing to report; and 2022 ITW in Goa, India, reported that a visit to check out potential sites is planned for March. 2022 ITW preproposal was approved, and is on track to become a full proposal.

More details were then provided regarding the status of ITW 2020. Co-chairs are Marco Dalai and Enrico Paolini; budget was approved by IEEE Finance; website is active and progressively updated-www.itw2020.it; contract between IEEE and Congress Center was signed; submission and review process will be done via EDAS. The workshop TPC membership status is : 71 invited; 33 accepted; 8 declined; 30 not yet responded, 6 plenary speakers are confirmed: Nina Balcan, Giuseppe Caire, Andreas Krause, Gabor Lugosi, Andrea Montanari, and Emina Soljanin; 5 invited sessions are confirmed: Gergely Neu (Machine Learning), Florent Krzakala (Stat Physics), Ryan Gabrys and Eitan Yaakobi (New Directions in Coding Theory), Yury Poliyanskiy and Giuseppe Durisi (Wireless), and David Tse (Blockchain); and 2 Sunday tutorials are confirmed: Eric Chitambar and Nati Srebro.

Next, Vijay presented items for discussion. He stated that a request was made for informal approval for Information-Theoretic Cryptography Conference, which was initiated and supported by Matthieu Bloch and Vinod Prabhakaran. He also stated that a request from Organizers of 17th International workshop on Algebraic and Combinatorial Coding Theory (ACCT2020) for approval for having accepted manuscripts appear in IEEE Xplore.

ISIT 2024—Joerg Kliewer

After Vijay, Joerg presented a proposal for ISIT 2024 in New York, prepared by him and Anand Sarwate. He motivated the choice for New York as being a major tourist destination, having a strong IT sector, and being easily accessible. He then went over the organizing committee. Next, Joerg presented hotel options. The first option presented was Sheraton Times Square, the second option was Hilton Midtown, and the third option was Kimmel Center at NYU. Joerg next compared the options in terms of the projected budget surplus, reminding that the numbers are still preliminary. He also presented pros and cons of Sheraton and Hilton.

He then presented a list of questions requesting feedback from BoG: Should they continue working on the New York proposal? What is the venue preference? Is there a surplus issue? Can BoG assist in getting potential sponsors? Is there any feedback from BoG?

A BoG member suggested Brooklyn Marriott. Anand clarified that they did contact them but hotel said they are too small to hold ISIT. Some BoG members suggested a combination of a hotel and a university campus for the conference. It was also stated that the proposed date of the 4th of July week is actually cheaper. Regarding the hotel occupancy, BoG members said that occupancy of 300 rooms would not be hard to meet. Regarding the surplus, it was also stated that the dollar amount is more important that the percentage. A BoG member suggested to the organizers to reach out to other IEEE conferences held in New York and get their input. It was also suggested that Brooklyn be considered instead of Manhattan.

Crypto conference-Matthieu Bloch

Matthieu then presented slides regarding a conference on information theoretic cryptography. The conference organizers seek to revive it and are looking for blessing from IT Society, without a formal binding, to increase interaction between crypto and information theory disciplines.

It was recognized by the BoG that engagement with the crypto community would be great, but that the proper mechanism needs to be established first; President Aylin Yener stated that the approval cannot be issued at this time since we need to consult with the IEEE first.

ISIT 2020 Los Angeles—Babak Hassibi

Next presentation was given by Babak Hassibi, on behalf of the ISIT 2020 organizing committee. Babak went over the venue details, program, including the list of plenary speakers, and the banquet details. It was stated that the awards luncheon will be held on Tuesday and the banquet will be on Wednesday at Universal Studios. Closing day will be Friday, it perhaps being half a day. Wednesday banquet ticket will also include a day pass to the Universal Studios theme park. Next, Babak went over the submission numbers of this and past conferences. It was recognized that the numbers of submissions are in decline. Babak clarified that instead of a fixed percentage, TPC committee will use "technically correct and novel" standard in making paper acceptance decisions. He also clarified that the conference needs 650 attendees to break even. A BoG member commented that even as number of papers went down the attendance went up, at least for ISIT 2019 in Paris.

Movie Committee-Alon Orlitsky

Next presentation was given by Alon Orlitsky who provided an update on The Bit Player movie, on behalf of the Movie Committee, whose members are Christina Fragouli, Daniela Tunitteti, Alon Orlitsky.

Alon provided the website for the movie: thebitplayer.com. He also stated that the poster for the movie also had hidden phrases in it. Movie premiere was at the World Science Festival in New York on May 29, 2019, where the movie screening was followed by a panel. There were 267 people in attendance at the premiere despite heavy rain in New York that day. Alon stated that the movie was also shown at the World Congress of Science Journalists, held in July 2019 in Lausanne, Switzerland, and at movie festivals in Paris and in Netherlands. The movie received the Best in Show recognition at MIPCOM 2019. Another screening was held at the Computer History Museum in Cupertino, CA, and it was organized by Andrea Goldsmith. Another west coast screening was held in San Francisco and it was sponsored by Intel, at the cost of 25k-30k\$. Alon also went over the list of other screenings. He then discussed festival status of the movie, and stated that they tried for major festivals but got only into minor festivals. Next, Alon discussed the distribution, for which the requests are made through the website. There are 40 requests and charge is 300–400\$ per screening, including an educational sciences series. For the international distribution company hired is called Off the Fence. Next, Alon stated that Nova and Netflix declined to show the movie, and that the potential alternatives include american public television, amazon prime, and educational channels. In terms of moving forward, Alon ask for feedback on replacing Argot, compensation for Mark, putting movie on YouTube, and any other suggestions. Alon also clarified that the movie is doing okay, but not great. He said that they raised over 1M\$, of which a portion was spent so far, and that the rest can be use towards outreach and promotion. President Aylin Yener said she will work with Alon and the Board on how to proceed, and whether to try YouTube or something else.

A Tribute to Vera Pless (1931-2020)

W. Cary Huffman, Professor Emeritus, Department of Mathematics and Statistics, Loyola University of Chicago whuffma@luc.edu

Vera Stepen Pless passed away at her home in Oak Park, Illinois on March 2, 2020, a few days short of her 89th birthday. She was a leading expert in the theory of error-correcting codes, being one of the very few women doing research in coding theory in its early years.

Vera Stepen was born in Chicago, Illinois on March 5, 1931, the daughter of Russian Jewish immigrants. She left high school after two years to pursue a "great books" program at the University of Chicago, graduating in three years. In 1952 she married Irwin Pless and completed an M.A. also from the University of Chicago. Subsequently she joined a physics group at the university but soon afterwards received a fellowship from Northwestern University. Vera moved

with her husband to Boston and completed her Ph.D. long-distance as a ring theory student of Alex Rosenberg, defending her dissertation [10], [11] two weeks before the birth of her first child.

In 1963 Vera joined the Air Force Cambridge Research Laboratory (AFCRL) to work in the new research area of error-correcting codes and continued to work there for ten years, resigning after the Department of Defense was prohibited from doing pure research. Upon leaving the AFCRL, she became a research associate at the Massachusetts Institute of Technology. In 1975 Vera was appointed full professor in the Department of Mathematics, Statistics and Computer Science at the University of Illinois Chicago where she taught until her retirement in 2006.

Vera Pless made significant, original, and lasting contributions to the study of error-correcting codes. In 1963, she published her first major work [12] in coding theory presenting what are now called the *Pless power moments* relating the weight distributions of a linear code to that of its dual. These power moments are equivalent to the *MacWilliams identities* published by F. Jessie MacWilliams [9] in the same year. Over the next few years, she helped establish the uniqueness of the Golay codes [14] and discovered what are now called the *Pless symmetry codes* [16].

Vera was among the first to explore the classification of maximal self-orthogonal and self-dual codes with her presentation of these binary codes up to length 20 in [15]. She followed this with the classification of self-dual codes of moderate lengths over various fields in succeeding publications, some with authors such as John H. Conway and Neil J. A. Sloane; see for example [3]. She developed mass formulas [13] that verify completeness of the classifications; she even modified the GROUP computer system to create the Combinatorial and Algebraic Machine Aided Computation (CAMAC) system [17] to assist in the computations.

In addition to the Pless symmetry codes, she discovered generalizations of quadratic residue codes called *duadic codes* [8] and *Q-codes* [18]. Vera together with Richard A. Brualdi developed *greedy codes*



[2], a generalization of lexicodes. Vera even delved into codes over rings studying cyclic codes over \mathbb{Z}_4 with Patrick Solé and her Ph.D. student Zhongqiang Qian in [21], [22]. Vera also tackled questions as diverse as covering radius (e.g., [1]), formally self-dual codes (e.g., [4]), additive codes (e.g., [5]), and decoding (e.g., [7]).

Teaching both research specialists and aspiring coding theory students was important to Vera. In 1982, she published her first coding theory book *Introduction to the Theory of Error-Correcting Codes* [19], currently in its third edition, which provided a gentle introduction to the field. In 1992 Vera began work as co-editor of the two volume *Handbook of Coding Theory* [20]. This 25 chapter, 33 author *Handbook*,

which covered a wide range of topics on the frontiers of research, was published six years after the project began. Upon its completion, the co-editors decided it would be appropriate to co-author an extensive textbook that could provide in part a bridge to the *Handbook*. The result was *Fundamentals of Error-Correcting Codes* [6] published in 2003.

During the mid 1980s Vera served on the Board of Governors of the Information Theory Society. In 2012 she became a fellow of the American Mathematical Society. During her career she published over 120 journal articles, 21 appearing in *IEEE Transactions on Information Theory*.

Vera is survived by her three children Naomi, Daniel, and Ben along with four grandchildren Lilah, Evie, Rebecca, and Jesse.

On a personal note, I had the privilege of working with Vera for over 30 years as our universities were only a subway ride (with one transfer) apart. Vera was always inspirational with her wealth of knowledge and intuitive insight into coding problems. In a very informal way, she taught me much coding theory as we sat in her office, probably not realizing how influential these conversations were. Vera loved classical music and reading; she loved her children and grandchildren. And she loved her students. On my visits, we would often go to lunch, usually at Vera's favorite Thai restaurant, inviting one or two students; you could never move fast enough as she would quickly pick up the check. I served on the Ph.D. committees of a number of her students. When members would ask the student a question, Vera could barely restrain herself (and often did not) from answering for them-she so much wanted her students to succeed. In the days following her passing, I received emails from coding theorists whose research careers were nudged, and even re-directed, along new paths based on interactions with Vera. Her presence will be greatly missed.

References

[1] E. F. Assmus, Jr. and V. S. Pless. On the covering radius of extremal self-dual codes. *IEEE Trans. Inform. Theory*, 29:359–363, 1983. [2] E. R. Berlekamp, editor. *Key Papers in the Development of Coding Theory*. IEEE Press, New York, 1974.

[3] I. F. Blake, editor. *Algebraic Coding Theory History and Development*. Dowden, Hutchinson, & Ross, Inc. Stroudsburg, PA, USA, 1973.

[4] R. A. Brualdi and V. S. Pless. Greedy codes. J. Combin. Theory Ser. A, 64:10–30, 1993.

[5] J. H. Conway, V. S. Pless, and N. J. A. Sloane. Self-dual codes over GF(3) and GF(4) of length not exceeding 16. *IEEE Trans. Inform. Theory*, 25:312–322, 1979.

[6] J. E. Fields, P. Gaborit, W. C. Huffman, and V. S. Pless. On the classification of extremal even formally self-dual codes of lengths 20 and 22. *Discrete Appl. Math.*, 111:75–86, 2001.

[7] P. Gaborit, W. C. Huffman, J.-L. Kim, and V. S. Pless. On additive GF(4) codes. In *Codes and Association Schemes (Piscataway, NJ,* 1999), volume 56 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 135–149. Amer. Math. Soc., Providence, RI, 2001.

[8] W. C. Huffman and V. S. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Cambridge, 2003.

[9] J.-L. Kim and V. S. Pless. Decoding some doubly-even self-dual [32, 16, 8] codes by hand. In *Codes and Designs (Columbus, OH,* 2000), volume 10 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 165–178. de Gruyter, Berlin, 2002.

[10] J. S. Leon, J. M. Masley, and V. S. Pless. Duadic codes. *IEEE Trans. Inform. Theory*, 30:709–714, 1984.

[11] F. J. MacWilliams. A theorem on the distribution of weights in a systematic code. *Bell System Tech. J.*, 42:79–94, 1963. (Also reprinted in [?] pages 261–265 and [?] pages 241–257).

[12] V. S. Pless. *Quotient Rings of Continuous Transformation Rings*. PhD thesis, North-western University, 1957; available at ProQuest LLC, Ann Arbor, MI.

[13] V. S. Pless. The continuous transformation ring of biorthogonal bases spaces. *Duke Math. J.*, 25:365–371, 1958.

[14] V. S. Pless. Power moment identities on weight distributions in error correcting codes. *Inform. and Control*, 6:147–152, 1963. (Also reprinted in [?] pages 266–267 and [?] pages 257–262).

[15] V. S. Pless. The number of isotropic subspaces in a finite geometry. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat.* (8), 39:418– 421, 1965.

[16] V. S. Pless. On the uniqueness of the Golay codes. *J. Combin. Theory*, 5:215–228, 1968.

[17] V. S. Pless. A classification of self-orthogonal codes over GF(2). *Discrete Math.*, 3:209–246, 1972.

[18] V. S. Pless. Symmetry codes over GF(3) and new five-designs. *J. Combin. Theory Ser. A*, 12:119–142, 1972.

[19] V. S. Pless. CAMAC—Combinatorial and Algebraic Machine Aided Computation. In *Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1975),* pages 505–511. Congressus Numerantium, No,. XIV, 1975.

[20] V. S. Pless. Q-codes. J. Combin. Theory Ser. A, 43:258–276, 1986.

[21] V. S. Pless. *Introduction to the Theory of Error-Correcting Codes*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons, Inc., New York, 3rd edition, 1998.

[22] V. S. Pless and W. C. Huffman, editors. *Handbook of Coding Theory, Vol. I, II*. North-Holland, Amsterdam, 1998.

[23] V. S. Pless and Z. Qian. Cyclic codes and quadratic residue codes over \mathbb{Z}_4 . *IEEE Trans. Inform. Theory*, 42:1594–1600, 1996.

[24] V. S. Pless, P. Solé, and Z. Qian. Cyclic self-dual \mathbb{Z}_4 -codes. *Finite Fields Appl.*, 3:48–69, 1997.

SELECTED AREAS IN INFORMATION THEORY

MAY 2020

VOLUME 1

NUMBER 1

IJSTL5

(ISSN 2641-8770)

Issue on Deep Learning: Mathematical Foundations and Applications to Information Science



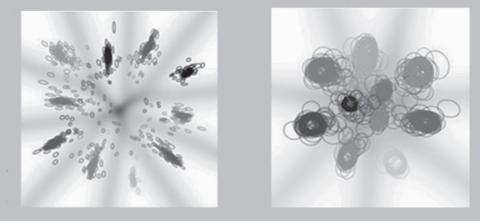


Fig. 4 from "The Information Bottleneck Problem and Its Applications in Machine Learning," by Goldfeld and Polyanskiy, p.19.



A PUBLICATION OF THE IEEE INFORMATION THEORY SOCIETY



SELECTED AREAS IN INFORMATION THEORY

MAY 2020

VOLUME 1

NUMBER 1

IJSTL5

(ISSN 2641-8770)

ISSUE ON DEEP LEARNING: MATHEMATICAL FOUNDATIONS AND APPLICATIONS TO INFORMATION SCIENCE

EDITORIAL

Welcome to the IEEE JOURNAL ON SELECTED AREAS IN INFORMATION THEORY (JSAIT)A. J. Goldsmith 000

GUEST EDITORIAL

PAPERS

PAPERS	
Physical Layer Communication via Deep Learning	000
The Information Bottleneck Problem and Its Applications in Machine LearningZ. Goldfeld and Y. Polyanskiy	000
Deep Learning Techniques for Inverse Problems in Imaging	
G. Ongie, A. Jalal, C. A. Metzler, R. G. Baraniuk, A. G. Dimakis, and R. Willett	000
Expression of Fractals Through Neural Network FunctionsN. Dym, B. Sober, and I. Daubechies	000
Harmless Interpolation of Noisy Data in Regression	
V. Muthukumar, K. Vodrahalli, V. Subramanian, and A. Sahai	000
Toward Moderate Overparameterization: Global Convergence Guarantees for Training Shallow Neural Networks	
S. Oymak and M. Soltanolkotabi	000
Sample Compression, Support Vectors, and Generalization in Deep LearningC. Snyder and S. Vishwanath	000
Tightening Mutual Information-Based Bounds on Generalization ErrorY. Bu, S. Zou, and V. V. Veeravalli	000
Extracting Robust and Accurate Features via a Robust Information BottleneckA. Pensia, V. Jog, and PL. Loh	000
A Fourier-Based Approach to Generalization and Optimization in Deep Learning	
	000
An Information-Theoretic Approach to Unsupervised Feature Selection for High-Dimensional Data	
	000
MaxiMin Active Learning in Overparameterized Model Classes	000
DeepJSCC-f: Deep Joint Source-Channel Coding of Images With FeedbackD. B. Kurka and D. Gündüz	000
Deepcode: Feedback Codes via Deep LearningH. Kim, Y. Jiang, S. Kannan, S. Oh, and P. Viswanath	000
LEARN Codes: Inventing Low-Latency Codes via Recurrent Neural Networks	
Y. Jiang, H. Kim, H. Asnani, S. Kannan, S. Oh, and P. Viswanath	000
Qsparse-Local-SGD: Distributed SGD With Quantization, Sparsification, and Local Computations	
D. Basu, D. Data, C. Karakus, and S. N. Diggavi	000

(Contents Continued on Page 22)



A PUBLICATION OF THE IEEE INFORMATION THEORY SOCIETY



(Contents Continued from Page 21)

00
00
00
00
00
00
00
00
00
00

President's Column (continued from page 1)

.itsoc.org/covid) and informed the membership accordingly. Some events needed to be postponed and others needed to go virtual. Each of these decisions has been made in concert with the requests of the organizers in accordance with the best course of action in each case, given the state at that point in time. So far, all of the decisions turned out to be right ones, given the present state we are in. The IEEE has an event emergency response team that we worked with in each of these changes, so contracts in place could be modified or canceled. Although normally such changes incur some costs due to prior commitments and deposit requirements, all of our events so far have been able to avoid any financial penalties. I would like to thank all of the organizers of the schools and conferences who worked diligently to ensure our society stayed financially strong despite this challenging year.

Most of our 2020 schools have requested to delay by a year, with the exception of the European school which postponed to fall 2020. We are currently in the process of determining the best action. ITW 2020 has been delayed to spring 2021. Our distinguished lecture program has been suspended given the travel restrictions. And perhaps most dramatically, our annual symposium ISIT 2020 has transitioned to virtual. For those of you who have had papers at ISIT, this entailed preparing a video presentation, and for all of you who participated, tuning into the live events, and listening to other paper presentations. For the organizers, it was a very different story. The preparation of an ISIT typically is a five-year process. The organizers start putting together a proposal scouting potential venues and preparing a detailed proposal (including the budget) that is presented to the board of governors, often competing with other teams. Typically, ISITs are chosen at least four years ahead of time. So, the LA organizers have been working hard for in excess of four years to perfect ISIT, when COVID-19 hit. They have opted not to postpone or cancel (thankfully), and instead set out to redesign and reimagine the entire conference in just three months. This took an enormous effort. I doubt they slept much, to ensure every little detail was attended to. Importantly, the organizers have devised a financial model that allowed very low registration fees (our non-author members could attend for free!). This ISIT drew close to 50% more participants than any of its predecessors and set an attendance record. We owe a tremendous gratitude to the general chairs, the TPC chairs and all of the organizers of ISIT 2020 for this trailblazing effort.

It is now quite clear that virtual or hybrid events, just like virtual/ hybrid learning, are going to be a major part of our operations going forward. While we miss discussing our latest research results in person, we must recognize that there are advantages to being able to utilize digital means to convene, including having access to content in an asynchronous manner (no more running between the sessions and missing the first two slides). Beyond meetings, going forward, having access to digital content and multimedia resources under our society brand is a clear benefit we can offer to our membership. This brings about the larger question of having a stronger and unified virtual presence as a society. We are now working on this, which I hope to elaborate on in my next column.

Until then, stay well and healthy.

Recent Publications

IEEE Transactions on Information Theory

Table of content for volumes 66(3), 66(4), 66(5)

Vol. 66(3): Mar. 2020.

	CODING THEORY AND TECHNIQUES	
E. Rosnes and M. Helmling	Adaptive Linear Programming Decoding of Nonbinary Linear Codes Over Prime Fields	1281
K. Wan, D. Tuninetti, and P. Piantanida	An Index Coding Approach to Caching With Uncoded Cache Placement	1318
L. Song, C. Fragouli, and T. Zhao	A Pliable Index Coding Approach to Data Shuffling	1333
Q. Zhang, M. Bakshi, and S. Jaggi	Covert Communication With Polynomial Computational Complexity	1354
O. Elishco, R. Gabrys, and E. Yaakobi	Bounds and Constructions of Codes Over Symbol-Pair Read Channels	1385
I. Tamo, M. Ye, and A. Barg	Error Correction Based on Partial Information	1396
H. Hou and P. P. C. Lee	Binary MDS Array Codes With Optimal Repair	1405
D. S. Krotov	The Existence of Perfect Codes in Doob Graphs	1423
N. Cai and M. Hayashi	Secure Network Code for Adaptive and Active Attacks With No-Randomness in Intermediate Nodes	1428
M. Shi, X. Li, A. Neri, and P. Solé	How Many Weights Can a Cyclic Code Have?	1449
	QUANTUM ERROR-CORRECTION	
L. Eldar, M. Ozols, and K. Thompson	The Need for Structure in Quantum LDPC Codes	1460
	SOURCE CODING	
H. Narimani and M. Khosravifard	A New Code for Encoding All Monotone Sources With a Fixed Large Alphabet Size	1474
E. Domanovitz and U. Erez	Achievability Performance Bounds for Integer-Forcing Source Coding	1482
	SHANNON THEORY	
Z. Goldfeld, P. Cuff, and H. H. Permuter	Wiretap Channels With Random States Non-Causally Available at the Encoder	1497
F. Arbabjolfaei and YH. Kim	Generalized Lexicographic Products and the Index Coding Capacity	1520
J. Zhang and X. Wang	Asymptotically Optimal Stochastic Encryption for Quantized Sequential Detection in the Presence of Eavesdroppers	1530
P. Sen and YH. Kim	Homologous Codes for Multiple Access Channels	1549
A. Campello, C. Ling, and JC. Belfiore	Semantically Secure Lattice Codes for Compound MIMO Channels	1572
Y. Jitsumatsu and Y. Oohama	A New Iterative Algorithm for Computing the Correct Decoding Probability Exponent of Discrete Memoryless Channels	1585
M. Tahmasbi, M. R. Bloch, and A. Yener	Learning an Adversary's Actions for Secret Communication	1607
I. Issa, A. B. Wagner, and S. Kamath	An Operational Approach to Information Leakage	1625
A. Painsky and G. W. Wornell	Bregman Divergence Bounds and Universality Properties of the Logarithmic Loss	1658
S. Kuzuoka	On the Conditional Smooth Rényi Entropy and its Applications in Guessing and Source Coding	1674
S. Watanabe and T. S. Han	Interval Algorithm for Random Number Generation: Information Spectrum Approach	1691
	SPARSE RECOVERY, SIGNAL PROCESSING, COMMUNICATION, LEARNING, ESTIMATION	
D. Ryabko	Time-Series Information and Unsupervised Learning of Representations	1702
XY. Liu, S. Aeron, V. Aggarwal, and X. Wang	Low-Tubal-Rank Tensor Completion Using Alternating Minimization	1714
D. Zou, R. Balan, and M. Singh	On Lipschitz Bounds of General Convolutional Neural Networks	1738
Y. Li, D. Shah, D. Song, and C. L. Yu	Nearest Neighbors for Matrix Estimation Interpreted as Blind Regression for Latent Variable Model	1760
Q. Qu, Y. Zhang, Y. C. Eldar, and J. Wright	Convolutional Phase Retrieval via Gradient Descent	1785
	COMMUNICATIONS	
W. Xu, H. A. J. Alshamary, T. Al-Naffouri, and A. Zaib	Optimal Joint Channel Estimation and Data Detection for Massive SIMO Wireless Systems: A Polynomial Complexity Solution	1822
Q. Li, P. de Kerret, D. Gesbert, and N. Gresset	Robust Regularized ZF in Cooperative Broadcast Channel Under Distributed CSIT	1845
M. U. Baig, L. Yu, Z. Xiong, A. Høst-Madsen, H. Li, and W. Li	On the Energy-Delay Tradeoff in Streaming Data: Finite Blocklength Analysis	1861

COMMUNICATION NETWORKS

Q. He, D. Yuan, and A. Ephremides A. M. Daniel and W. Yu	Optimal Scheduling for Emptying a Wireless Network: Solution Characterization, Applications, Including Deadline Constraints Optimization of Heterogeneous Coded Caching	1882 1893
Q. Yu, M. A. Maddah-Ali, and A. S. Avestimehr	Straggler Mitigation in Distributed Matrix Multiplication: Fundamental Limits and Optimal Coding	1920
	CRYPTOGRAPHY	
S. Kim, K. Yoon, J. Kwon, YH. Park, and S. Hong	New Hybrid Method for Isogeny-Based Cryptosystems Using Edwards Curves	1934
	SEQUENCES	
H. Aly and A. Winterhof	A Note on Hall's Sextic Residue Sequence: Correlation Measure of Order k and Related Measures of Pseudorandomness	1944
	COMMENTS AND CORRECTIONS	
A. Høst-Madsen	Corrections to "The Wideband Slope of Interference Channels: The Small Bandwidth Case"	1948

SHANNON THEORY

M. Diaz, H. Wang, F. P. Calmon, and L. Sankar	On the Robustness of Information-Theoretic Privacy Measures and Mechanisms	1949
M. Tahmasbi, A. Savard, and M. R. Bloch	Covert Capacity of Non-Coherent Rayleigh-Fading Channels	1979
A. Dytso, S. Yagli, H. V. Poor, and S. Shamai (Shitz)	The Capacity Achieving Distribution for the Amplitude Constrained Additive Gaussian Channel: An Upper Bound on the Number of Mass Points	2006
YP. Wei and S. Ulukus	The Capacity of Private Information Retrieval With Private Side Information Under Storage Constraints	2023
S. Kadhe, B. Garcia, A. Heidarzadeh, S. El Rouayheb, and A. Sprintson	Private Information Retrieval With Side Information	2032
S. Sreekumar and D. Gündüz	Distributed Hypothesis Testing Over Discrete Memoryless Channels	2044
N. Merhav	Error Exponents of Typical Random Trellis Codes	2067
S. Tridenski and R. Zamir	Channel Input Adaptation via Natural Type Selection	2078
A. Anshu and P. Yao	On the Compression of Messages in the Multi-Party Setting	2091
J. Chen, L. Xie, Y. Chang, J. Wang, and Y. Wang	Generalized Gaussian Multiterminal Source Coding: The Symmetric Case	2115
	QUANTUM INFORMATION THEORY	
K. Fang, X. Wang, M. Tomamichel, and M. Berta	Quantum Channel Simulation and the Channel's Smooth Max-Information	2129
F. Salek, A. Anshu, MH. Hsieh, R. Jain, and J. R. Fonollosa	One-Shot Capacity Bounds on the Simultaneous Transmission of Classical and Quantum Information	2141
L. Lami	Completing the Grand Tour of Asymptotic Quantum Coherence Manipulation	2165
	COMMUNICATION	
M. Johnny and M. R. Aref	BIA for the K-User Interference Channel Using Reconfigurable Antenna at Receivers	2184
Y. Pang and M. K. Varanasi	Constant-Gap-to-Capacity and Generalized Degrees of Freedom Regions of the MIMO MAC-IC-MAC	2198
P. Hassanzadeh, A. M. Tulino, J. Llorca, and E. Erkip	Rate-Memory Trade-Off for Caching and Delivery of Correlated Sources	2219
E. Parrinello, A. Ünsal, and P. Elia	Fundamental Limits of Coded Caching With Multiple Antennas, Shared Caches and Uncoded Prefetching	2252
	COMMUNICATION NETWORKS	
Y. Zhang, Y. Chen, YH. Lo, and W. S. Wong	Achieving Zero-Packet-Loss Throughput 1 for a Collision Channel Without Feedback and With Arbitrary Time Offsets	2269
S. Zou, V. V. Veeravalli, J. Li, and D. Towsley	Quickest Detection of Dynamic Events in Networks	2280
	CODING THEORY AND TECHNIQUES	
S. Mesnager and A. Sınak	Several Classes of Minimal Linear Codes With Few Weights From Weakly Regular Plateaued Functions	2296
P. Huang, Y. Liu, X. Zhang, P. H. Siegel, and E. F. Haratsch	Syndrome-Coupled Rate-Compatible Error-Correcting Codes: Theory and Application	2311
A. Lenz, P. H. Siegel, A. Wachter-Zeh, and E. Yaakobi	Coding Over Sets for DNA Storage	2331
V. Guruswami and R. Li	Coding Against Deletions in Oblivious and Online Models	2352
J. Sima, N. Raviv, and J. Bruck	Two Deletion Correcting Codes From Indicator Vectors	2375

25

J. Zhang, D. Wan, and K. Kaipa	Deep Holes of Projective Reed-Solomon Codes	2392
H. Cai, Y. Miao, M. Schwartz, and X. Tang	On Optimal Locally Repairable Codes With Multiple Disjoint Repair Sets	2402
L. Holzbaur, R. Freij-Hollanti, A. Wachter-Zeh, and C. Hollanti	Private Streaming With Convolutional Codes	2417
MC. Chiu	Interleaved Polar (I-Polar) Codes	2430
R. G. L. D'Oliveira and S. El Rouayheb	One-Shot PIR: Refinement and Lifting	2443
M. Shi, D. S. Krotov, and P. Solé	A New Approach to the Kasami Codes of Type 2	2456
	SPARSE RECOVERY, SIGNAL PROCESSING, LEARNING, PROBABILITY AND STATISTICS, ESTIMATION	
Y. Yakimenka and E. Rosnes	Failure Analysis of the Interval-Passing Algorithm for Compressed Sensing	2466
C. Thrampoulidis and A. S. Rawat	The Generalized Lasso for Sub-Gaussian Measurements With Dithered Quantization	2487
D. Amelunxen, M. Lotz, and J. Walvin	Effective Condition Number Bounds for Convex Regularization	2501
M. Ndaoud and A. B. Tsybakov	Optimal Variable Selection and Adaptive Noisy Compressed Sensing	2517
M. Brand	MML Is Not Consistent for Neyman-Scott	2533
A. Padakandla, P. R. Kumar, and W. Szpankowski	The Trade-Off Between Privacy and Fidelity via Ehrhart Theory	2549
L. K. Patra, S. Kayal, and S. Kumar	Measuring Uncertainty Under Prior Information	2570
	SOURCE CODING	
Si. Pae	Binarization Trees and Random Number Generation	2581
	CRYPTOGRAPHY	
Z. Li, S. Ling, C. Xing, and S. L. Yeo	On the Bounded Distance Decoding Problem for Lattices Constructed and Their Cryptographic Applications	2588
	COMMENTS AND CORRECTIONS	
L. Yu and V. Y. F. Tan	Corrections to "Wyner's Common Information Under Rényi Divergence Measures"	2599

Vol. 66(5): May 2020.

CODING THEORY AND TECHNIQUES

P. Huang, E. Yaakobi, and P. H. Siegel	Multi-Erasure Locally Recoverable Codes Over Small Fields: A Tensor Product Approach	2609
M. Karmoose, L. Song, M. Cardone, and C. Fragouli	Privacy in Index Coding: k-Limited-Access Schemes	2625
T. Liu and D. Tuninetti	Tight Information Theoretic Converse Results for Some Pliable Index Coding Problems	2642
Y. Yehezkeally and M. Schwartz	Reconstruction Codes for DNA Sequences With Uniform Tandem-Duplication Errors	2658
Y. M. Chee, H. M. Kiah, A. Vardy, and E. Yaakobi	Explicit and Efficient WOM Codes of Finite Length	2669
K. Reing, G. V. Steeg, and A. Galstyan	Maximizing Multivariate Information With Error-Correcting Codes	2683
S. L. Fong, A. Khisti, B. Li, WT. Tan, X. Zhu, and J. Apostolopoulos	Optimal Streaming Erasure Codes Over the Three-Node Relay Network	2696
T. Honold, M. Kiermaier, S. Kurz, and A. Wassermann	The Lengths of Projective Triply-Even Binary Codes	2713
F. Li, Q. Yue, and Y. Wu	LCD and Self-Orthogonal Group Codes in a Finite Abelian p-Group Algebra	2717
H. A. Inan, P. Kairouz, and A. Özgür	Sparse Combinatorial Group Testing	2729
J. Li and D. Wan	Distance Distribution in Reed-Solomon Codes	2743
M. Araya, M. Harada, and K. Saito	Quaternary Hermitian Linear Complementary Dual Codes	2751
F. Li	Construction of Constant Dimension Subspace Codes by Modifying Linkage Construction	2760
Z. Ye, T. Zhang, X. Zhang, and G. Ge	Some New Results on Splitter Sets	2765
	SHANNON THEORY	
G. Schamberg and T. P. Coleman	Measuring Sample Path Causal Influences With Relative Entropy	2777
L. Yu and V. Y. F. Tan	Exact Channel Synthesis	2799
J. Chen	Secure Communication Over Interference Channel: To Jam or not to Jam?	2819
S. T. Jose and A. A. Kulkarni	Shannon Meets von Neumann: A Minimax Theorem for Channel Coding in the Presence of a Jammer	2842
E. Sula, M. Gastpar, and G. Kramer	Sum-Rate Capacity for Symmetric Gaussian Multiple Access Channels With Feedback	2860
N. De Ponti	Metric Properties of Homogeneous and Spatially Inhomogeneous F-Divergences	2872
R. F. Vigelis, L. H. F. De Andrade, and C. C. Cavalcante	Properties of a Generalized Divergence Related to Tsallis Generalized Divergence	2891
B. Jaye, G. V. Livshyts, G. Paouris, and P. Pivovarov	Remarks on the Rényi Entropy of a Sum of IID Random Variables	2898

June 2020

T. Gur and I. Shinkar	An Entropy Lower Bound for Non-Malleable Extractors	2904
N. Merhav	Guessing Individual Sequences: Generating Randomized Guesses Using Finite–State Machines	2912
	QUANTUM INFORMATION THEORY	
Y. Ouyang and R. Chao	Permutation-Invariant Constant-Excitation Quantum Codes for Amplitude Damping	2921
S. Huber, R. König, and M. Tomamichel	Jointly Constrained Semidefinite Bilinear Programming With an Application to Dobrushin Curves	2934
A. Gonzales and E. Chitambar	Bounds on Instantaneous Nonlocal Quantum Computation	2951
P. J. Brown, S. Ragy, and R. Colbeck	A Framework for Quantum-Secure Device-Independent Randomness Expansion	2964
	COMMUNICATIONS	
C. Hellings and W. Utschick	Improper Signaling Versus Time-Sharing in the Two-User Gaussian Interference Channel With TIN	2988
CH. Chang and CC. Wang	A New Capacity-Approaching Scheme for General 1-to-K Broadcast Packet Erasure Channels With ACK/NACK	3000
M. U. Baig, A. Høst-Madsen, and A. Nosratinia	Discrete Modulation for Interference Mitigation	3026
J. Nam, G. Caire, M. Debbah, and H. V. Poor	Capacity Scaling of Massive MIMO in Strong Spatial Correlation Regimes	3040
	COMMUNICATION NETWORKS	
P. Li, G. J. Puleo, and O. Milenkovic	Motif and Hypergraph Correlation Clustering	3065
	PROBABILITY, STATISTICS AND LEARNING	
K. Gourgoulias, M. A. Katsoulakis, L. Rey-Bellet, and J. Wang	How Biased Is Your Model? Concentration Inequalities, Information and Model Bias	3079
A. Elmahdy and S. Mohajer	On the Fundamental Limits of Coded Data Shuffling for Distributed Machine Learning	3098
C. L. Canonne, I. Diakonikolas, D. M. Kane, and A. Stewart	Testing Bayesian Networks	3132
H. Lou, M. Schwartz, J. Bruck, and F. Farnoud	Evolution of k-Mer Frequencies and Entropy in Duplication and Substitution Mutation Systems	3171
V. Krishnamurthy	Convex Stochastic Dominance in Bayesian Localization, Filtering, and Con- trolled Sensing POMDPs	3187
A. Zhang and M. Wang	Spectral State Compression of Markov Processes	3202
	SIGNAL PROCESSING, DETECTION, AND ESTIMATION	
T. Bendory, D. Edidin, and Y. C. Eldar	Blind Phaseless Short-Time Fourier Transform Recovery	3232
Z. Li, JF. Cai, and K. Wei	Toward the Optimal Construction of a Loss Function Without Spurious Local Minima for Solving Quadratic Equations	3242
S. Daei, F. Haddadi, and A. Amini	Living Near the Edge: A Lower-Bound on the Phase Transition of Total Variation Minimization	3261
N. Merhav	Weak-Noise Modulation-Estimation of Vector Parameters	3268
	CRYPTOGRAPHY	
S. Su	Systematic Methods of Constructing Bent Functions and 2-Rotation Symmetric Bent Functions	3277



2021 IEEE International Symposium on Information Theory

General Co-Chairs Parastoo Sadeghi Emanuele Viterbo

TPC Co-Chairs

Michael Gastpar Stephen Hanly Henry Pfister Emina Soljanin

Publications Bikash Dey

Finance Sarah Johnson

Local Arrangements Margreta Kuijper James Saunderson

Publicity Brian M. Kurkoski

Tutorials Yi Hong

Recent Results Neda Aboutorab

Student Travel Grants Lawrence Ong

Sponsorship Girish Nair

Call for Papers

Fair dinkum, ISIT returns to Australia. In 2021, the IEEE International Symposium on Information Theory (ISIT) will be held 11–16 July at the Melbourne Convention & Exhibition Center in Melbourne, Victoria, Australia. ISIT was last held in Australia in 2005, in Adelaide.

Interested authors are encouraged to submit previously unpublished contributions from a broad range of topics related to information theory, including but not limited to the following areas:

- Communication and Storage Coding
- Coding Theory
- Coded and Distributed Computing
- Combinatorics and Information Theory
- Communication Theory
- Compressed Sensing and Sparsity
- Cryptography and Security
- Detection and Estimation
- Deep Learning for Networks
- Distributed Storage
- Emerging Applications of IT
- Information Theory and Statistics
- Information Theory in Biology

- Information Theory in CS
- Information Theory in Data Science
- Learning Theory
- Network Coding and Applications
- Network Data Analysis
- Network Information Theory
- Pattern Recognition and ML
- Privacy in Information Processing
- Quantum Information Theory
- Shannon Theory
- Signal Processing
- Source Coding and Data Compression
- Wireless Communication

Submitted and published manuscripts should not exceed 5 pages in length plus an optional extra page containing references only. Submitted manuscripts should be of sufficient detail to be evaluated by expert reviewers in the field. Full information about paper submission will be posted on the conference web site.

http://isit2021.org/

Paper submission deadline: January 10, 2021

Notification of acceptance: March 26, 2021

Accepted papers must be presented by an author in person. International attendees wishing to attend ISIT 2021 must be aware of Australian visa requirements. Attendees requiring a visa are advised to begin the visa application process immediately after acceptance notification.

We look forward to welcoming you to ISIT 2021 in Melbourne.



27

Lead Guest Editor H. Vincent Poor

Guest Editors

Matthieu Bloch Onur Günlü Frédérique Oggier Lalitha Sankar Rafael F. Schaefer Aylin Yener

2020 IEEE JSAIT - Special Issue on Privacy and Security of Information Systems

This special issue will focus on exploring the intersection of privacy and security with information and coding theory, as well as applications in communication theory, cryptography, computer science, machine learning, and hardware security. The early work of Shannon on perfect secrecy systems paved the way for the development of information-theoretic security and has led to deep insights regarding the role played by coding for security. Information-theoretic security now encompasses a broad range of security notions, from secrecy, authentication, covertness and privacy, applied to a wide variety of models, including wiretap channels, source and channel models for key generation, context-aware privacy models, secure and private learning, as well as distributed storage and computations systems. This special issue aims to attract contributions further exploring informationtheoretic security and privacy and investigating fundamental limits or practical code constructions/algorithms in contexts including but not limited to: secret message transmission, secret key agreement, authentication, identification, data anonymization, private retrieval, and privacy-preserving machine learning.

IEEE Journal on Selected Areas in Information Theory (JSAIT) Editor-in-Chief: Andrea Goldsmith (Stanford University)

Call for Papers

Previously unpublished contributions in security and privacy methods for biometrics, 6G, machine learning, IoT, and database search based on information- and coding-theoretic methods are solicited, including but not limited to:

- Biometric secrecy systems and physical unclonable functions
- Secrecy capacity and secret-key capacity of wireless channels
- New attack models and information theoretic defense mechanisms
- Covert and stealthy communication
- Code constructions for security and privacy
- Differential privacy and privacy-preserving mechanisms
- Code designs for physical layer security in emerging applications
- Private information retrieval
- Secure multi-party computation, private computation
- Privacy amplification with extractors and hash functions
- Security and privacy guarantees in distributed and federated learning

Important Dates

Paper Submission Deadline	August 15, 2020
Acceptance Notification	January 15, 2021
Camera-ready Version due	February 5, 2021
Expected Publication	February/March 2021

Submission Guidelines

Submitted papers should be of sufficient length and detail for review by experts in the field. Prospective authors must follow the *IEEE Journal on Selected Areas in Information Theory* manuscript submission guidelines in <u>JSAIT Author Information</u> webpage. All papers should be submitted through <u>https://mc.manuscriptcentral.com/jsait-ieee</u>

IEEE Journal on Selected Areas in Information Theory Special Issue on

Sequential, active, and reinforcement learning



There has been a long history of the interplay between information theory and sequential data analysis in the context of sequential estimation, hypothesis testing, and change-point detection. Recently, sequential methods have become hugely popular in domains such as reinforcement learning, multi-armed bandits, online convex optimization, and active learning. These methods have assumed tremendous importance due to the wide availability of large amounts of data, including data acquired in real time by advanced sensing technologies, and audio-visual content available on social media platforms. Although many practical algorithms have been developed for making accurate decisions on-the-fly, there is also a strong need for understanding the fundamental performance limits of these algorithms designed for the sequential learning tasks. Herein lies an excellent opportunity for information theory to employ the vast array of techniques in its arsenal to answer these fundamental questions. Simultaneously, sequential learning has already started to motivate new problems and insights in information theory and has led to new perspectives. This special issue seeks to fertilize new topics at the intersection of information theory and sequential, active, and reinforcement learning, and to promote synergies across these areas of research.

Topics

Prospective authors are invited to submit original manuscripts on topics including, but not limited to:

(a) Multi-armed bandits;

Important Dates

- (c) Bayesian optimization;
- (e) Stochastic optimization methods;
- (g) Sequential estimation, hypothesis testing, and tracking;
- (b) Reinforcement learning;(d) Change-point detection, anomaly detection;
- (f) Active learning;
- (h) Sequential experimental design.

Acceptance Notification: March 15, 2021 Expected Publication: April/May 2021

Senior Editors

Manuscript Due: October 1, 2020

Final to Publisher: April 10, 2021

Robert Nowak (University of Wisconsin Madison)

David Tse (Stanford University)

Guest Editors

- (a) Yao Xie (Georgia Tech, Lead)
- (c) Mengdi Wang (Princeton University)
- (e) George Moustakides (University of Patras)
- (g) Zheng Wen (DeepMind)

- (b) Vincent Tan (National University of Singapore, Lead)
- (d) Venugopal Veeravalli (UIUC)
- (f) Csaba Szepesvari (University of Alberta)

IEEE Membership Can Help You **Reach Your Personal** and Professional Goals



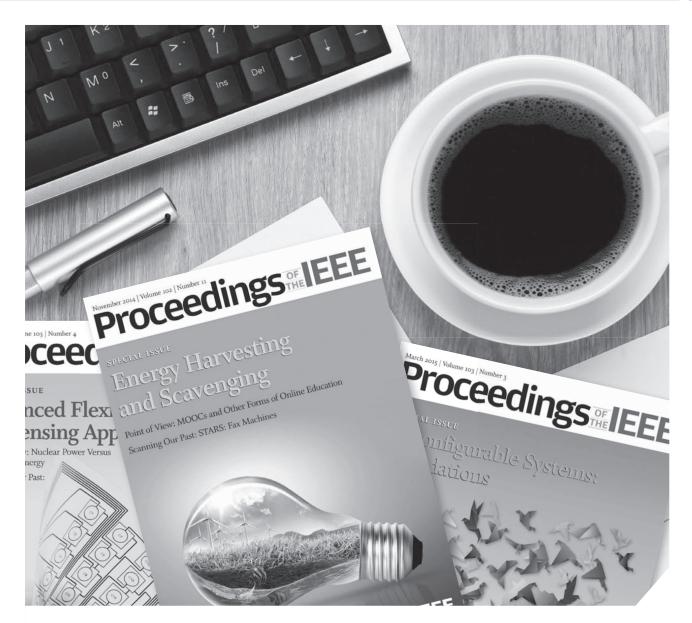
Gain access to the latest IEEE news, publications and digital library. Give and receive personal mentoring. Network locally and globally with IEEE members. And that's only the beginning. Discover how IEEE can help jumpstart your career.

Visit **www.ieee.org/join** today.

"Participating in IEEE has developed me as a well-rounded engineer and helped me shine during networking events."

-Likhitha Patha Electrical Engineering Student, IEEE Brand President, Virginia Polytechnic Institute and State University





One of the most influential reference resources for engineers around the world.

For over 100 years, *Proceedings of the IEEE* has been the leading journal for engineers looking for in-depth tutorial, survey, and review coverage of the technical developments that shape our world. Offering practical, fully referenced articles, *Proceedings of the IEEE* serves as a bridge to help readers understand important technologies in the areas of electrical engineering and computer science.



To learn more and start your subscription today, visit ieee.org/proceedings-subscribe



32

Conference Calendar

DATE	CONFERENCE	LOCATION	WEB PAGE	DUE DATE
June 15–19, 2020	The International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless (WiOpt)	Virtual	http://wi-opt.org	Passed
June 21–26, 2020	IEEE International Symposium on Information Theory	Virtual	https://2020.ieee-isit.org	Passed
June 22–26, 2020	52nd Annual ACM Symposium on the Theory of Computing (STOC)	Virtual	http://acm-stoc.org/ stoc2020/	Passed
June 29–July 1, 2020	IEEE Conference on Communications and Network Security	Virtual	https://cns2020.ieee-cns.org	Passed
November 16–19, 2020	61st Annual IEEE Symposium on Foundations of Computer Science (FOCS)	Durham, North Carolina, USA	https://focs2020.cs.duke.edu	Passed
December 7–11, 2020	IEEE Global Communications Conference (GLOBECOM)	Taipei, Taiwan	https://globecom2020.ieee- globecom.org	passed
Major COMSOC conferences: http://www.comsoc.org/confs/index.html				

IEEE Information Theory Society Newsletter