Discrete Applied Mathematics 161 (2013) 1072–1084

Contents lists available at SciVerse ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Finding lower bounds on the complexity of secret sharing schemes by linear programming[☆]

Carles Padró [a], Leonor Vázquez [b], An Yang [a,*]

[a] School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore

[b] ORIONEARTH, Oil Reservoir Integration on Earth, Mexico

ARTICLE INFO

Article history:
Received 14 August 2012
Accepted 16 October 2012
Available online 10 November 2012

Keywords:
Secret sharing
Linear programming
Polymatroid
Non-Shannon information inequalities

ABSTRACT

Optimizing the maximum, or average, length of the shares in relation to the length of the secret for every given access structure is a difficult and long-standing open problem in cryptology. Most of the known lower bounds on these parameters have been obtained by implicitly or explicitly using that every secret sharing scheme defines a polymatroid related to the access structure. The best bounds that can be obtained by this combinatorial method can be determined by using linear programming, and this can be effectively done for access structures on a small number of participants.

By applying this linear programming approach, we improve some of the known lower bounds for the access structures on five participants and the graph access structures on six participants for which these parameters were still undetermined. Nevertheless, the lower bounds that are obtained by this combinatorial method are not tight in general. For some access structures, they can be improved by adding to the linear program non-Shannon information inequalities as new constraints. We obtain in this way new separation results for some graph access structures on eight participants and for some ports of non-representable matroids. Finally, we prove that, for two access structures on five participants, the combinatorial lower bound cannot be attained by any linear secret sharing scheme.

© 2012 Elsevier B.V. All rights reserved.

1. Introduction

Secret sharing, which was independently introduced by Blakley [7] and Shamir [36], deals with methods to distribute a *secret value* among a set of participants, in such a way that only some *qualified subsets* can recover the secret value. In this work we consider only *unconditionally secure perfect secret sharing schemes*, in which the shares of the participants in an unqualified set do not provide any information about the secret. The collection of qualified subsets is called the *access structure* of the secret sharing scheme. The reader that is unfamiliar with secret sharing will find more information about the topic in the surveys by Stinson [37] and by Beimel [2]. In addition, some of the concepts appearing in this paper are described in more detail in [27].

[☆] A previous version of this paper appeared in the Proceedings of LATIN 2010 (Padró and Vázquez, 2010) [34]. Several new results have been added to the current version, as the ones in Sections 6 and 7. Moreover, the overall presentation of the paper has been greatly improved. This work was partially done while the first and second authors were with Universitat Politècnica de Catalunya, Barcelona. Their work was partially supported by the Spanish Ministry of Education and Science under project MTM2009-07694. The work of the first and third authors is supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

[*] Corresponding author. Fax: +65 6515 8213.
E-mail addresses: carlespl@ntu.edu.sg (C. Padró), leobaki@hotmail.com (L. Vázquez), yang0246@ntu.edu.sg (A. Yang).

0166-218X/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2012.10.020

The length of the shares, when compared to the length of the secret value, is usually considered as a measure of the efficiency of a secret sharing scheme. Specifically, the *complexity*, or *information ratio*, of a secret sharing scheme is defined as the ratio between the maximum length of the shares and the length of the secret. The *average complexity*, or *average information ratio*, is defined analogously from the average length of the shares. In every secret sharing scheme, the length of every share is at least the length of the secret [26]. A secret sharing scheme is said to be *ideal* if all shares have the same length as the secret. The *optimal complexity* $\sigma(\Gamma)$ of an access structure Γ is defined as the infimum of the complexities of all secret sharing schemes for Γ. The *optimal average complexity* $\widetilde{\sigma}(\Gamma)$ is defined analogously. Clearly, $1 \leq \widetilde{\sigma}(\Gamma) \leq \sigma(\Gamma)$.

Determining the values of these parameters is one of the main open problems in secret sharing. Even though many partial results have been found, important questions remain unsolved. In particular, the asymptotic behavior of these parameters is unknown and there is a huge gap between the best known upper and lower bounds. Because of the difficulty of finding general results, this problem has been considered for several particular families of access structures in [8,13–15,39,19,25,28] among other works. And a great achievement has been obtained recently by Csirmaz and Tardos [15] by determining the optimal complexity of all access structures defined by trees.

In a *linear secret sharing scheme*, the secret value and the shares are vectors over some finite field, and every share is the value of a given linear map on some random vector. The homomorphic properties of linear secret sharing schemes are very important for some of the main applications of secret sharing as, for instance, secure multiparty computation. On the other hand, linear secret sharing schemes are obtained when applying the best known techniques to construct efficient schemes, as the decomposition method by Stinson [38]. Because of that, it is also interesting to consider the parameters $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$, the infimum of the (average) complexities of all *linear* secret sharing schemes for Γ. Obviously, $\sigma(\Gamma) \leq \lambda(\Gamma)$. In fact, almost all known upper bounds on the optimal complexity are upper bounds on λ, and the same applies to the corresponding parameters for the average optimal complexity. Even though non-linear secret sharing schemes have been proved to be in general more efficient than the linear ones [3,6], not many examples of access structures with $\sigma(\Gamma) < \lambda(\Gamma)$ are known.

On the other hand, Csirmaz [12] explained how most of the known lower bounds on the optimal complexity have been found by implicitly or explicitly using a combinatorial method based on the connection between the Shannon entropy and polymatroids presented by Fujishige [20]. The best known asymptotic lower bound [12] was obtained by using this method. The parameter $\kappa(\Gamma)$ was introduced in [27] to denote the best lower bound on $\sigma(\Gamma)$ that can be obtained by this method. We introduce here the corresponding parameter $\widetilde{\kappa}(\Gamma)$ for the combinatorial lower bounds on the optimal average complexity.

As far as we know, $\kappa(\Gamma) = \lambda(\Gamma)$ for all access structures whose optimal complexity $\sigma(\Gamma)$ has been determined. This is due of course to the techniques that have been most used until now. Namely, the combinatorial method, which provide lower bounds on κ, and several decomposition methods, which provide almost always linear secret sharing schemes, and hence upper bounds on λ. In particular, these are the methods used by Jackson and Martin [25] to determine the optimal (average) complexities of almost all 180 non-isomorphic access structures on five participants. The same techniques were used by van Dijk [39] to find the optimal complexities of almost all 112 non-isomorphic graph access structures on six participants. Some improvements in the upper bounds for the unsolved cases were presented in [11,42].

Determining the values of $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ for a given access structure Γ is a linear program. Both the number of variables and of constraints grow exponentially in the number of participants. Moreover, Csirmaz [14, Section 1.2] pointed out that the system of constraints is overdetermined. Nevertheless, linear programming can be used to compute $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ for access structures on a small number of participants. This method has been applied on access structures with four minimal qualified subsets [28] and on bipartite access structures [19].

The use of linear programming, whenever it is possible, to compute $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ has two useful advantages. First, it does not only provide a lower bound on the optimal (average) complexity, but the best bound that can be obtained by using that combinatorial method. That is, other techniques are needed if the obtained lower bound is not tight. And second, after solving the linear program, a polymatroid attaining the optimal value of $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ is given, which may facilitate the search for optimal secret sharing schemes.

In this paper, we present the results of such a computation on the access structures on five participants and the graph access structures on six participants whose optimal complexities have not been previously determined. Several known lower bounds are improved and, in a few cases, the value of the optimal (average) complexity is determined. After the publication of the previous version of this paper [34], Gharahi and Dehkordi [21] presented lower bounds on the optimal complexities of some graph access structures. Their bounds coincide with the values of $\kappa(\Gamma)$ that we computed by linear programming, but a different proof is given. For one of those access structures, an upper bound is given in [21] that makes it possible to determine $\sigma(\Gamma)$.

The lower bound $\kappa(\Gamma)$ on the optimal complexity is not tight in general. The first found examples of access structures with $\kappa(\Gamma) < \sigma(\Gamma)$ were the ports of the Vamos matroid [4]. An infinite family of graph access structures with $\kappa(\Gamma) < \lambda(\Gamma)$ was presented by Csirmaz [14]. These results are proved, respectively, by using the non-Shannon information inequality by Zhang and Yeung [43] and the Ingleton inequality [22]. These and other known information inequalities, as for instance the ones in [16,31,17,18], are linear inequalities, and hence they can be added as constraints to the linear program computing $\kappa(\Gamma)$. For some access structures, better lower bounds on $\sigma(\Gamma)$ (or on $\lambda(\Gamma)$ if the Ingleton inequality is used) are obtained in this way. Nevertheless, Beimel and Orlov [5] proved that all known non-Shannon information inequalities cannot improve our knowledge on the asymptotic behavior of the optimal (average) complexity.

We checked that, for the aforementioned access structures on five participants and graph access structures on six participants, no better lower bounds on $\lambda(\Gamma)$ can be obtained by adding the Ingleton inequality to the linear program.

Download English Version:

https://daneshyari.com/en/article/418373

Download Persian Version:

https://daneshyari.com/article/418373

Daneshyari.com