Designs, Codes and Cryptography (2023) 91:1951–1971
https://doi.org/10.1007/s10623-023-01187-8

Secret sharing on regular bipartite access structures

Máté Gyarmati[1]

Received: 26 August 2021 / Revised: 12 December 2022 / Accepted: 21 December 2022 /
Published online: 14 February 2023

Abstract
Bipartite secret sharing schemes realize access structures in which the participants are divided into two parts, and all the participants in the same part play an equivalent role. Such a bipartite structure can be described by the collection of its minimal points. The complexity of a scheme is the ratio between the maximum share size given to the participants and the secret size, and the Shannon complexity of a structure is the best lower bound provided by the entropy method. Within this work, we compute the Shannon complexity of regular bipartite structures and provide optimal constructions for some bipartite structures defined by 2 and 3 points.

Keywords Secret sharing · Bipartite access structures · Information ratio · Shannon-complexity

Mathematics Subject Classification 94A62

1 Introduction

Secret sharing is a method to distribute sensitive information amongst participants (P) such that only some predefined coalitions called qualified sets can recover the secret. A secret sharing is *perfect* if the unqualified sets cannot compute any nontrivial information about the secret. In this paper all secret sharing schemes are perfect. The set of qualified sets is monotone and called access structure (Γ). Secret sharing was introduced by Shamir [29] and Blakley [4] independently and is used in many cryptographic protocols, e.g. secure multiparty computation [3, 8, 9], multi-signatures [2], secure aggregations [6], attribute-based encryption [21] and many others, see [1].

Communicated by C. Padro.

Research has been supported by the ÚNKP-20-3 and ÚNKP-21-4 New National Excellence Programs of the Ministry for Innovation and Technology from the source of the National Research, Development and Innovation Fund.

✉ Máté Gyarmati
hairl1@inf.elte.hu

[1] Department of Computeralgebra, Eötvös Loránd University, Budapest, Hungary

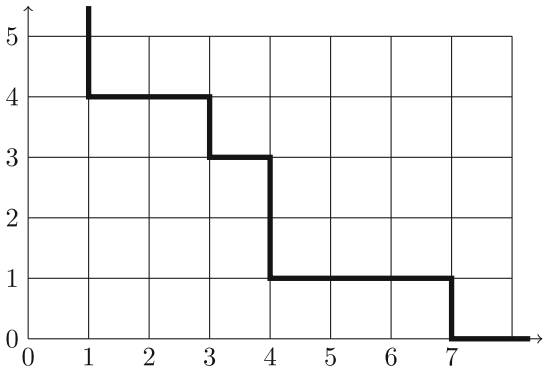


Fig. 1 A staircase defined by four points ($\ell = 4$), (1,4), (3,3), (4,1), (7,0)

We measure the complexity of an access structure with the information ratio, that is, the largest amount of information each participant has to store about the size of the secret. If this value is 1, then the access structure is ideal. Computing the information ratio of an arbitrary access structure is usually a hard problem, the exact value is known only for small structures and specific families, for example, access structures on at most 5 participants [19, 25], some graph based [5, 14, 20, 22, 23, 30, 32], a few bipartite [15, 18] and some ideal access structures [7, 17, 26, 27, 31].

A secret sharing scheme is called k-threshold if the qualified sets are the ones that have at least k elements [4, 29]. All participants in a threshold scheme have the same role, however, in some applications for example in the case of hierarchy we want to provide more control for certain participants, like leaders. A possible generalization is to divide the participants into two parts and a set of participants is qualified if it contains enough elements from each part. Instead of considering only one threshold pair (a threshold for each part), we can consider multiple instances of pairs, for example, a set is qualified if it contains at least 5 participants from the first and 2 from the second, or 3 participants from the first and 6 from the second part. Such access structures are called bipartite [27]. Formally let $P = P_1 \cup P_2$, $P_1 \cap P_2 = \emptyset$ and $n_1 = |P_1|, n_2 = |P_2|$. The bipartite Γ is given by an integer ℓ and two integer sequences

$$0 \le x_1 < x_2 < \ldots < x_\ell \le n_1 \text{ and } n_2 \ge y_1 \ge y_2 \ge \ldots \ge y_\ell \ge 0 \tag{1}$$

such that $A \in \Gamma$ if and only if $|A \cap P_1| \ge x_k$ and $|A \cap P_2| \ge y_k$ for some $1 \le k \le \ell$. The sequence $(x_1, y_1), \ldots, (x_\ell, y_\ell)$ is a staircase in the non-negative grid, see Fig. 1.

It is worth defining the widths $w_k = x_{k+1} - x_k$ and the heights $h_k = y_k - y_{k+1}$ of the staircase as the complexity of the bipartite structure depends on the widths and heights and not the actual coordinates of the points. The widths and heights in Fig. 1 are 2,1,3, and 1,2,1 respectively. The bipartite structure is regular if all widths are the same and all heights are the same.

Padró and Sáez [27] determined all ideal bipartite structures. Csirmaz, Matus, and Padró [15] computed the value of the information ratio of some regular bipartite structures. Assume all widths are w, and all heights are h. In this case, the staircase is regular.

- If $w = h$ then the Shannon complexity of the structure is $2 - 1/w$, that is independent from ℓ.
- If $h = 1$ and all the widths are w then for every ℓ the Shannon complexity of the structure is $1 + \frac{(\ell-1)(w-1)}{\ell+w-2}$.

Our first result is a generalization of these statements. We give a lower bound on the information ratio for every regular staircase, more precisely we compute the Shannon complexity of such access structures.

Farras et. al. [18] and Csirmaz et. al. [15] constructed optimal secret sharing schemes on bipartite access structures given by two points $(x_1, y_1), (x_2, 0)$ and three points $(0, 3)(1, 1), (3, 0)$ respectively.

Our second result is an optimal secret sharing scheme on bipartite access structures defined by three points $(0, x_1), (x_2, y_2), (x_3, 0)$. By duality, this also yields an optimal secret sharing scheme to bipartite access structures defined by two points $(x_1, y_1), (x_2, y_2)$ where $x_1, y_2 \neq 0$. Albeit the case $y_2 = 0$ was already solved by [18] as we mentioned earlier, we provide a different optimal secret sharing scheme for this case too.

The paper is organized as follows. In the next section, we introduce the main concepts and recall some of the results from previous works (focusing on [15]) that are essential for the later sections. In Sects. 3 and 4 we present our results; we compute the Shannon complexity of regular staircases in the former, and present the optimal secret sharing schemes in the latter. Let P be a finite set of participants and $\Gamma \subset 2^P$ be a monotone increasing set system on P. The elements of Γ are called qualified sets, while the other subsets of P are unqualified. There exists a few different definitions of secret sharing, we use the one from [11].

Definition 1 A perfect secret sharing scheme S realizing Γ is a collection of random variables ξ_p for every $p \in P$ and ξ_s with a joint distribution such that

(i) if $A \in \Gamma$, then $\{\xi_p : p \in A\}$ determines ξ_s;
(ii) if $A \notin \Gamma$, then $\{\xi_p : p \in A\}$ is independent of ξ_s.

A secret sharing scheme is linear if the shares of the participants and the secret can be represented as linear subspaces of a vector space.

The complexity of a secret sharing scheme is the ratio between the maximum share size of the participants and the size of the secret. The information ratio measures the complexity of the most efficient secret sharing scheme.

Definition 2 Let Γ be an access structure. Then the information ratio of Γ is

$$\sigma(\Gamma) = \inf_S \max_{p \in P} \frac{H(\xi_p)}{H(\xi_s)}$$

where $H(\cdot)$ is the Shannon entropy and the infimum is taken over all perfect secret sharing schemes S realizing Γ.

The linear complexity of an access structure is

$$\lambda(\Gamma) = \inf_{S \text{ linear}} \max_{p \in P} \frac{H(\xi_p)}{H(\xi_s)},$$

and clearly $\sigma(\Gamma) \leq \lambda(\Gamma)$.

Define f to be the normalized entropy function, i.e. $f : 2^P \mapsto \mathbb{R}$ and $f = H(\xi_p : p \in A)/H(\xi_s)$ where H is the Shannon entropy, $A \subseteq P$ and s is the secret. Using the properties

of the entropy function [16] and the secret sharing we have [10]

$$\begin{aligned}
&(1)\quad f(\emptyset)=0,\ \text{and in general } f(A)\geq 0 && \text{(positivity);}\\
&(2)\quad f(B)\geq f(A) \text{ if } A\subseteq B && \text{(monotonicity);}\\
&(3)\quad f(A)+f(B)\geq f(A\cap B)+f(A\cup B) && \text{(submodularity);}\\
&(4)\quad f(B)\geq f(A)+1 \text{ if } A\subseteq B \text{ and } B \text{ is qualified} && \\
&\qquad \text{but } A \text{ is not} && \text{(strong monotonicity);}\\
&(5)\quad f(A)+f(B)\geq f(A\cap B)+f(A\cup B)+1,\ \text{if} && \\
&\qquad \text{both } A \text{ and } B \text{ are qualified but } A\cap B \text{ is not} && \text{(strong submodularity).}
\end{aligned} \tag{2}$$

Let f be any real-valued function satisfying (2). Then any lower bound given to $\max_{p\in P} f(p)$ is also a lower bound for the information ratio. The value

$$\kappa(\Gamma)=\min_{f}\max_{v\in V} f(v)$$

is called Shannon complexity and can be computed by solving the corresponding LP. Usually, the LP is too large to be solved, and its size is exponential in the number of participants, however, in the case of bipartite structures due to the symmetry the number of inequalities can be decreased drastically. We enlist the reduced version of (2) from [15]. f is now a function on the grid, for more details see [15]. In the strong variants, we use $f^\bullet$ and f° to emphasize that the argument is qualified and unqualified respectively.

$$\begin{aligned}
&f(i,j)\geq 0,\ f(0,0)=0 && \text{non-negativity}\\
&\left.\begin{aligned} f(i+1,j)-f(i,j)\geq 0\\ f(i,j+1)-f(i,j)\geq 0\end{aligned}\right\} && \text{monotonicity}\\
&\left.\begin{aligned} (f(i,j)-f(i-1,j))-(f(i+1,j)-f(i,j)\geq 0\\ (f(i,j)-f(i,j+1))-(f(i,j+1)-f(i,j))\geq 0\end{aligned}\right\} && \text{submodularity - 1}\\
&(f(i+1,j)-f(i,j))-(f(i+1,j+1)-f(i,j+1))\geq 0 && \text{submodularity - 2(3)}\\
&\left.\begin{aligned} f^\bullet(i+1,j)-f^\circ(i,j)\geq 1\\ f^\bullet(i,j+1)-f^\circ(i,j)\geq 1\end{aligned}\right\} && \text{strong monot.}\\
&\left.\begin{aligned} (f^\bullet(i,j)-f^\circ(i-1,j))-(f^\bullet(i+1,j)-f^\bullet(i,j))\geq 1\\ (f^\bullet(i,j)-f^\circ(i,j+1))-(f^\bullet(i,j+1)-f^\bullet(i,j))\geq 1\end{aligned}\right\} && \text{strong submod. - 1}\\
&(f^\bullet(i+1,j)-f^\circ(i,j))-(f^\bullet(i+1,j+1)-f^\bullet(i,j+1))\geq 1 && \text{strong submod. - 2}
\end{aligned}$$

Finally let $H=f(1,0)$, and $V=f(0,1)$. Determining the Shannon complexity is equivalent to the following problem:

$$\kappa(\Gamma)=\inf_{f}\{\max(H,V): f \text{ satisfies (3)}\}. \tag{4}$$

Every submodular function f on the non-negative grid that satisfies (3) yields an upper bound for κ. (3) is only needed to be satisfied for adjacent points on the grid, therefore it is more convenient to give the values of f as the difference between two adjacent points on the grid. We assign the differences to the edges that connect the points (Fig. 2). As $f(0,0)=0$, the values assigned to the edges determine f uniquely. (3) can be reformulated in terms of edge values [15]. We note that an additional property, consistency, has to be satisfied as well.

- Monotonicity - edge values are non-negative.
- Consistency - on each 1×1 square, the sum of the left and top edges

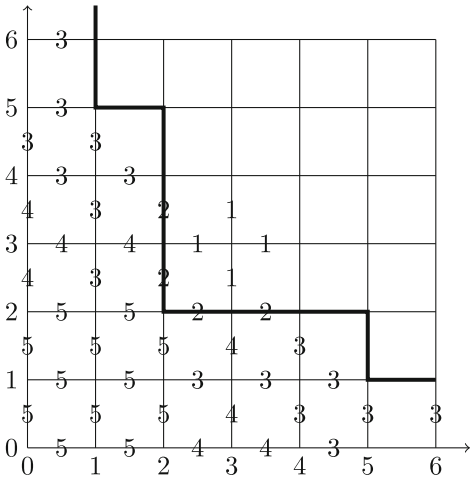


Fig. 2 Non-zero edge values for a submodular function f (the values are multiples of 1/3). The bipartite structure is defined by points (1,5), (2,2), and (5,1). The qualified points are the ones above, to the right or on the solid line. The value of f at any point is the sum of the differences all along any shortest path from the point to the origin

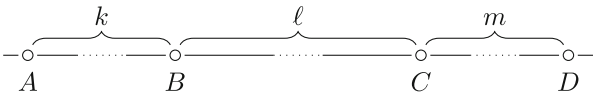


Fig. 3 Lemma 1. The points may be on a vertical line, in the order A, B, C, D from bottom up

equals the sum of bottom and right edges.

- Submodularity - values are decreasing from left to right, and from bottom up (both for vertical and horizontal edges).
- Strong monotonicity - an edge between a qualified and an unqualified vertex has a value at least 1.
- Strong submodularity 1 - the increment between two adjacent horizontal (vertical) edges is at least one if the second edge has two qualified endpoints and the first edge has only one.
- Strong submodularity 2 - in an 1×1 square with three qualified nodes the left edge is at least 1 more than the right edge.

(5)

We do a little abuse of notation as we denote both the point of the grid and the value of f in that point with the same notation such as A, B, A_1, etc. We recall three lemmas from [15]: Lemmas 1, 2 and 3. The first two are used in Sect. 3, to calculate a lower bound on the Shannon complexity while the third is needed in Sect. 4 and it provides a lower bound for the Shannon complexity based on the maximal width.

Lemma 1 *With the notation of Fig. 3*

(a) $\frac{B-A}{k} \geq \frac{C-B}{\ell}$,
(b) $\frac{C-A}{k+\ell} \geq \frac{C-B}{\ell}$,
(c) if A is unqualified, B is qualified, and there are s qualified nodes between A and B (not including B), then $\frac{B-A}{k} \geq \frac{C-B}{\ell} + \frac{k-s}{k}$.

Lemma 2 *Let A, B, A', B' be as in Fig. 4. Then* $B - A \geq B' - A' + \frac{k-V}{k-1}$.

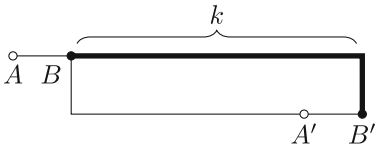


Fig. 4 The arrangement of the points in Lemma 2.

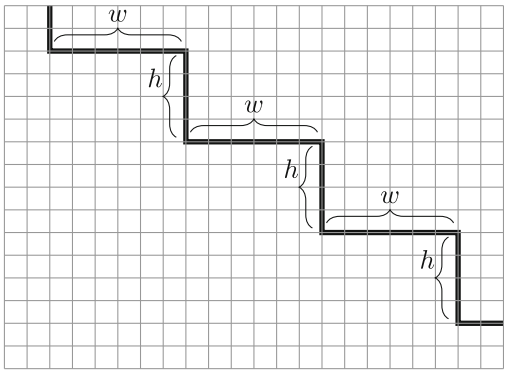


Fig. 5 Regular staircase with width $w = 6$ and height $h = 4$

Lemma 3 *Suppose* Γ *has a step of width* $w = w_k = i_{k+1} - i_k \geq 2$ *such that* $i_k \neq 0$. *Then* $\kappa(\Gamma) \geq 2 - 1/w$.

Finally, we need the concept of duality. The dual of an access structure Γ consists of the complements of the unqualified subsets of Γ, $\Gamma^{\perp} = \{P - A \mid A \notin \Gamma\}$. Especially the minimally qualified elements in $\Gamma^{\perp}$ are the complements of the maximal unqualified elements of Γ. Clearly $(\Gamma^{\perp})^{\perp} = \Gamma$. There is a close relationship between an access structure and its dual as $\lambda(\Gamma) = \lambda(\Gamma^{\perp})$ [24]. We mention that there is a similar connection between the Shannon complexities, $\kappa(\Gamma) = \kappa(\Gamma^{\perp})$ [13], however, it is unknown if the same holds for the information ratio.

2 Shannon-complexity of regular staircases

The main result of this section is the following theorem.

Theorem 1 *Consider the regular staircase* Γ *of width* w, *height* h *and length* ℓ *where* $x_1 \neq 0$ *and* $w \geq h$ *(* (x_1, y_1) *is the leftmost point). Then*

$$\kappa(\Gamma) = \frac{(\ell w - 1)(2w - 1)}{(\ell h - 1)w + (2w + \ell - 2)(w - h)}.$$

The Shannon complexity only depends on if $x_1 \neq 0$, the exact value is not important.

We note that Theorem 1 gives back the values from [15] for the special choice of ℓ and h. If $\ell = 2$ or $h = w$ then clearly the Shannon complexity is $2 - 1/w$ and with the choice $h = 1$, it is $\frac{\ell w - 1}{\ell + w - 2}$.

We prove Theorem 1 in two separate parts. First, we compute a lower bound using the reduced entropy inequalities, then we construct an f function on the grid satisfying (5).

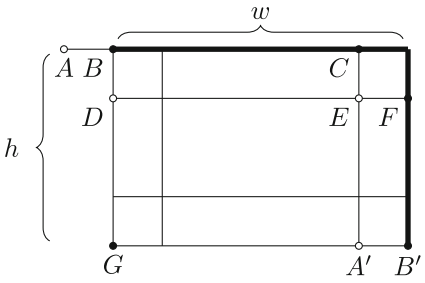


Fig. 6 The arrangement of the points in Lemma 3.

2.1 Lower bound

Theorem 2 *Consider the regular staircase* Γ *of width* w*, height* h *and length* ℓ *where* $x_1 \neq 0$ *and* $w \geq h$ *(*(x_1, y_1) *is the leftmost point). Then*

$$\kappa(\Gamma) \geq \frac{(\ell w - 1)(2w - 1)}{(\ell h - 1)w + (2w + \ell - 2)(w - h)}.$$

Before we start the proof of Theorem 2, we introduce two lemmas that are two different generalizations of Lemma 2. The lemmas estimate the increment of the values in the grid for one step on the staircase at two different places.

Lemma 4 *Let* $A, B, C, D, E, F, G, A', B'$ *be points as in Fig. 6. Then*

$$B - A - (B' - A') \geq \frac{w - V}{w - 1} - \frac{(h - 1)V}{w} + \frac{F - B'}{w}.$$

Proof Recall that $V = f(0, 1)$ is the maximal vertical value. By part (c) of Lemma 1 we have

$$B - A \geq \frac{C - B}{w - 1} + 1. \tag{6}$$

First, use the consistency for the $BCDE$ rectangle, then the strong monotonicity for CE, the (a) part of Lemma 1, and that $B - D$ is at most the vertical maximum V:

$$C - B = (C - E) + (E - D) - (B - D) \geq 1 + \frac{w - 1}{w}(F - D) - V. \tag{7}$$

Substituting (7) in (6) yields

$$B - A \geq \frac{F - D}{w} + \frac{w - V}{w - 1}. \tag{8}$$

Applying the consistency for the $DFGB'$ rectangle, then the (b) part of Lemma 1 and that $D - G$ is at most $h - 1$ times the vertical maximum results in:

$$\begin{aligned} F - D &= (F - B') + (B' - G) - (D - G) \geq \\ &\geq F - B' + w(B' - A') - (h - 1)V. \end{aligned} \tag{9}$$

Finally substituting (9) into (8) yields the statement of the lemma. □

Lemma 5 *With the notation of Fig. 7,*

$$(B - A) - (B' - A') \geq \frac{w - V}{w - 1} - \frac{B - D}{w - 1}.$$

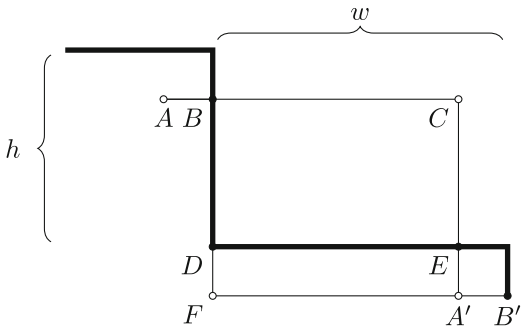


Fig. 7 The arrangement of the points in Lemma 4

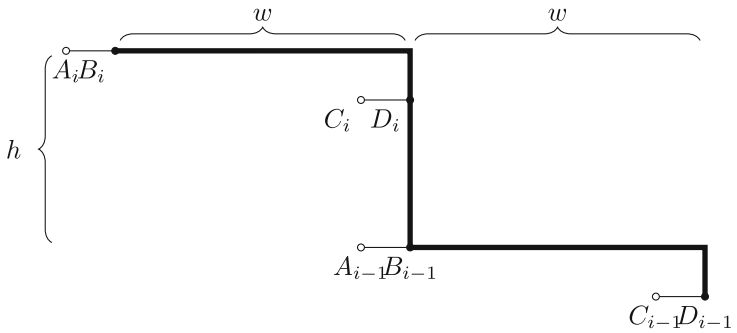


Fig. 8 The points from Lemmas 3 and 4 in the same diagram

Proof By part (c) of Lemma 1,

$$B - A \geq \frac{C - B}{w - 1} + 1, \tag{10}$$

by the consistency of the rectangle $BCDE$ we have

$$C - B = (C - E) + (E - D) - (B - D). \tag{11}$$

$C - E \geq 0$ because of monotonicity. The consistency for the rectangle $DEFA'$ yields $E - D = (E - A') + (A' - F) - (D - F)$. $E - A' \geq 1$ because of strong monotonicity, $A' - F \geq (w - 1)(B' - A')$ by part (a) of Lemma 1, and $D - F \leq V$, thus

$$E - D \geq 1 - V + (w - 1)(B' - A'). \tag{12}$$

Substituting (11) and (12) subsequently into (10) finishes the proof. □

Proof (Theorem 2): Let B_ℓ be the leftmost corner point of the staircase, that is (x_1, y_1) and A_ℓ is the one strictly left to B_ℓ. As $H \geq B_\ell - A_\ell$, our goal is to estimate $B_\ell - A_\ell$ using only w, h, ℓ and V. First, we only restrict our attention to one step on the staircase.

With the notation of Fig. 8 the statement of Lemmas 4 and 5 respectively yield

$$B_i - A_i - (B_{i-1} - A_{i-1}) \geq \frac{w - V}{w - 1} - \frac{(h - 1)V}{w} + \frac{D_i - B_{i-1}}{w}, \tag{13}$$

$$D_i - C_i - (D_{i-1} - C_{i-1}) \geq \frac{w - V}{w - 1} - \frac{D_i - B_{i-1}}{w - 1}. \tag{14}$$

Adding up (13) with $(w-1)/w$ times (14) cancels out the $D_i - B_{i-1}$ part, the remaining is

$$\begin{aligned} &B_i - A_i - (B_{i-1} - A_{i-1}) + \frac{w-1}{w}\left(D_i - C_i - (D_{i-1} - C_{i-1})\right) \\ &\geq \frac{w-V}{w-1} - \frac{(h-1)V}{w} + \frac{w-V}{w} = \frac{2w-1}{w-1} - V\left(\frac{1}{w-1} + \frac{h}{w}\right) = \Delta. \end{aligned} \tag{15}$$

The left-hand side is a telescopic sequence, while the right-hand side contains only fixed values and V. Adding up the inequalities (15) for $i = 2, 3, \ldots, \ell - 1$ we get

$$B_{\ell-1} - A_{\ell-1} - (B_1 - A_1) + \frac{w-1}{w}\left(D_{\ell-1} - C_{\ell-1} - (D_1 - C_1)\right) \geq (\ell-2)\Delta \tag{16}$$

Clearly $B_{\ell-1} - A_{\ell-1} \leq H$, and $D_1 - C_1 \geq 1$. Lemma 2 implies that $B_i - A_i \geq \frac{w-V}{w-1} + D_i - C_i$ for $i = 1$ and $i = \ell - 1$. Thus $B_1 - A_1 \geq \frac{w-V}{w-1} + 1$, and $\frac{w-1}{w}(D_{\ell-1} - C_{\ell-1}) \leq \frac{w-1}{w}H - \frac{w-V}{w}$.

Substituting each of these bounds into the inequality (16) we have

$$\begin{aligned} &H - \frac{w-V}{w-1} - 1 + \left(\frac{w-1}{w}H - \frac{w-V}{w}\right) - \frac{w-1}{w} = \\ &= H\frac{2w-1}{w} + V\left(\frac{1}{w} + \frac{1}{w-1}\right) - 2 - \frac{w-1}{w} - \frac{w}{w-1} = \\ &= H\frac{2w-1}{w} + V\frac{2w-1}{w(w-1)} - \frac{(2w-1)^2}{w(w-1)} \geq (\ell-2)\Delta. \end{aligned}$$

Substituting back the value of Δ yields

$$H(2w^2 - 3w + 1) + V(w(h\ell - 2h + \ell) - h\ell + 2h - 1) \geq (2w-1)(\ell w - 1).$$

The left hand side can be bounded from above by $\max(H, V)(2w^2 - 3w + 1 + w(h\ell - 2h + \ell) - h\ell + 2h - 1)$, therefore

$$\max(H, V) \geq \frac{(\ell w - 1)(2w-1)}{(\ell h - 1)w + (2w + \ell - 2)(w-h)}.$$

□

Theorem 3 *Consider the regular staircase Γ of width w, height h and length ℓ where $x_1 \neq 0$ and $w \geq h$ ((x_1, y_1) is the leftmost point). Then*

$$\kappa(\Gamma) \leq \frac{(\ell w - 1)(2w-1)}{(\ell h - 1)w + (2w + \ell - 2)(w-h)}. \tag{17}$$

Proof We construct the function f, more precisely the non-negative grid satisfying (5). Let w_0 be the minimal number of participants such that all qualified sets have at least w_0 participants from P_1. Similarly, let h_0 be the minimal number of participants such that all qualified sets have at least h_0 participants from P_2. The value of $\kappa(\Gamma)$ does not depend on the exact values of w_0 and h_0, just on the fact whether w_0 and h_0 are zero or not.

Instead of giving values to all edges on the grid, we focus on rectangles of width $2w$ and height h. The four coordinates of the rectangle, denoted by M_i are $(w_0 + (\ell-2-i)w, h_0 + ih)$, $(w_0 + (\ell-i)w, h_0 + ih)$, $(w_0 + (\ell-i)w, h_0 + (i+1)h)$ and $(w_0 + (\ell-2-i)w, h_0 + (i+1)h)$. The value of i goes from 0 to $\ell - 1$. The last rectangle, $M_{\ell-1}$ is shorter if $w_0 < w$.

First, we specify the values of the edges in M_0 (see Fig. 11 for general or Fig. 12 for concrete values), this is the most important part of the proof. Next, we show how to modify

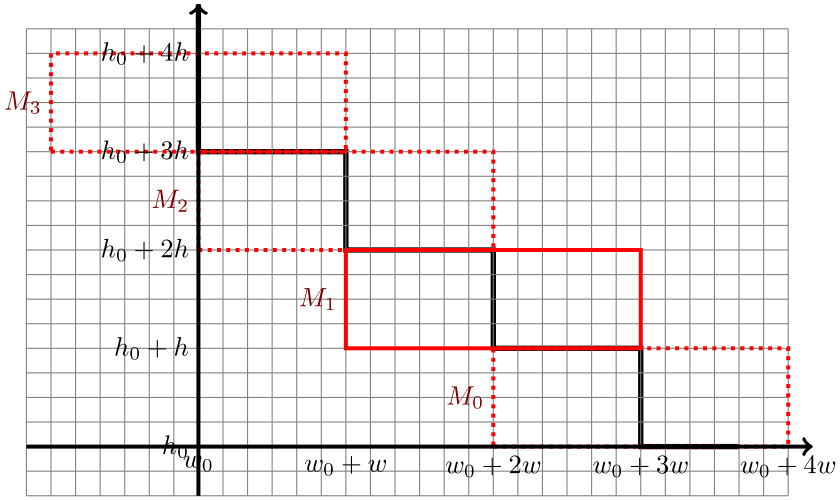


Fig. 9 First we define the values of the grid for rectangles of size $(2w \times h)$, which are marked in red, e.g. M_0,M_1,...,$M_{\ell-1}$ (Color figure online)

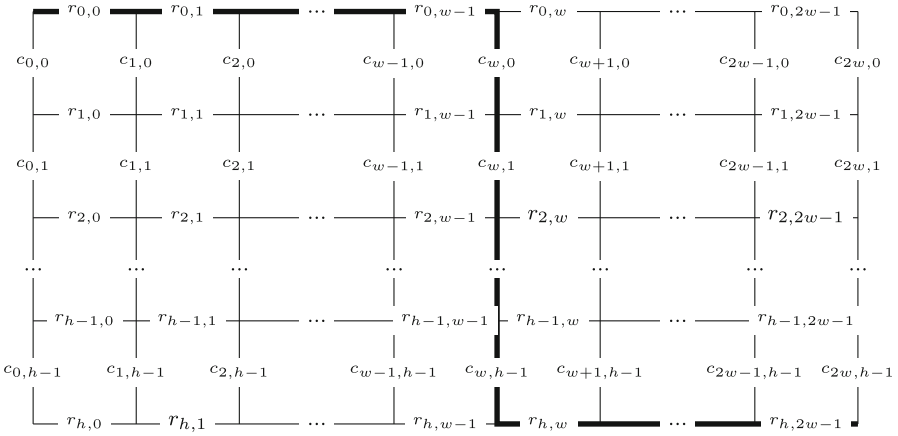


Fig. 10 Row and column values in a rectangle

M_0 to get the edge values in M_i $i = 1, \ldots, \ell - 1$ (see Fig. 12 for example). At this stage, all the edge values are determined inside the union of the rectangles. The last step is to extend the values to the whole grid.

Let V be the right hand side of the inequality in (17) and define $\alpha = \frac{V-1}{w-1}$ and $\beta = \frac{V}{2w-1}$. Denote the jth value in the ith column with $c_{i,j}$ and similarly denote the jth value in the ith row with r_{ij} starting the indexing from 0 as in Fig. 10.

The values $c_{0,0}, c_{1,0}, \ldots, c_{w,0}$ form a linear sequence starting with $c_{0,0,} = V$ and decreasing by α, and $c_{w+1,0}, \ldots, c_{2w,0}$ are all zeros. That is $c_{i,0} = V - i\alpha$ for $i \leq w$ and $c_{i,0} = 0$ if $i > w$. $c_{0,j}, c_{1,j}, \ldots, c_{2w-1,j}$ $j > 0$ is also a linear sequence starting from $c_{0,j} = V$ and decreasing by β. Hence $c_{i,j} = V - i\beta$ if $i \leq 2w - 1$ and $c_{2w,j} = 0$, $j > 0$ in both cases.

The values in the first row are different from the other rows just as in the column case: $r_{0,j} = 1 - \alpha$ if $j \leq w - 1$ and $r_{0,j} = 0$ otherwise. $r_{1,j}, r_{2,j}, \ldots, r_{h,j}$ is a linear sequence

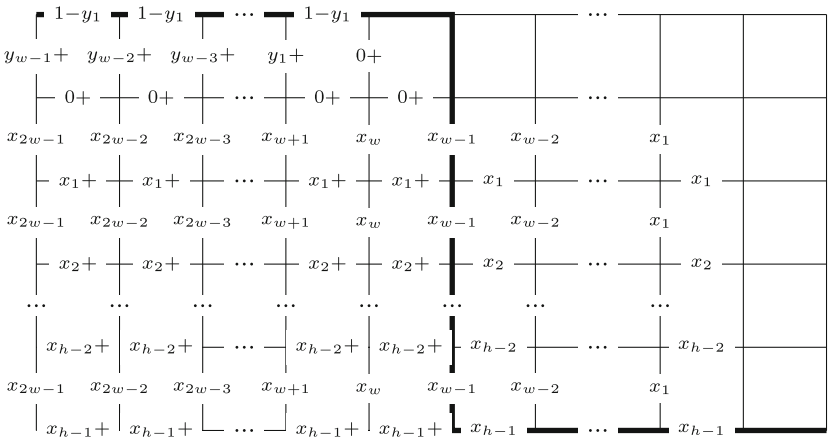


Fig. 11 The values in M_0. The empty edges are 0, $x_i = i\beta$, $y_i = i\alpha$, and $+$ means that we add +1 to the value. E.g. 0+ means $0 + 1 = 1$

for $j = 0, \ldots, 2w$. The only difference is that if $j \leq w$, then the linear sequence starts from $r_{1,j} = 1$ and $r_{i,j} = 1 + (i-1)\beta$, and if $j > w$, then $r_{1,j} = 0$ and $r_{i,j} = (i-1)\beta$.

We note that all elements in a column are identical except the first one. Similarly, except for the first row, the elements in all rows are almost identical, but the elements in the non-qualified part are larger by 1.

Figure 12 presents the values of f in M_0 (bottom), in M_1 (middle) and in M_2 (top) for the case of $\ell = 3$, $w = 4$, $h = 3$. The Shannon complexity is 77/41, $\alpha = 12/41$, $\beta = 11/41$ and $\Delta = 7/41$. For simplicity, we omit the zeros and the denominators. The thick line separates the qualified and the unqualified sets (points on the line are qualified too). The four lower-right edges of M_1 and M_2 have the same value as the four upper-left edges of M_0 and M_1 since these edges are identical.

It is easy to check that the grid satisfies consistency, nonnegativity, monotonicity, and submodularity. It also satisfies strong monotonicity and strong submodularity.

We now construct M_1 from M_0. he column values are identical and the row values are almost the same, the only difference is that we add $\Delta = r_{0,0} - r_{h,w} = (1-\alpha) - (h-1)\beta$ to each row value except the last element of each row, see Fig. 12. $M_2, M_3, \ldots, M_{\ell-2}$ are constructed from M_1 similarly, the columns are unchanged, and in M_i we add $(i-1)\Delta$ to each row values. Finally, in $M_{\ell-1}$ the first value of each column is 0, and the rest is the same as in M_1. The row values are constructed by adding $(\ell-2)\Delta$ to each value, except the first w values of the 0th row. These values are all $(\ell-2)\Delta + 1$, which are equal to the first w values of the first row, see Fig. 12. It is clear that M_i satisfies (5) for $i = 1, \ldots, \ell-1$, too.

Notice that M_i and M_{i+1} have a common line segment of length w. Δ was chosen in a way that the first w row values in the 0th row in M_i (which are $(1 - y + i\Delta, \ldots, 1 - y + i\Delta, i\Delta)$), are equal to the last w row values in the hth (last) row in M_{i+1} (that is $((h-1)\beta + (i+1)\Delta, \ldots, (h-1)\beta + (i+1)\Delta, i\Delta)$), thus these values are equal. (5) remains true if we consider the union of M_i $i = 0, \ldots, \ell-1$. The only non-trivial inequality is the strong submodularity for the column values where M_i and M_{i+1} meet. It is enough to check for M_0 and M_1 because the column values are equal in each rectangle. The values in the ith column are: $V - i\alpha$ in M_0 and $(w-1-i)\beta$ in M_1, thus all we need is that

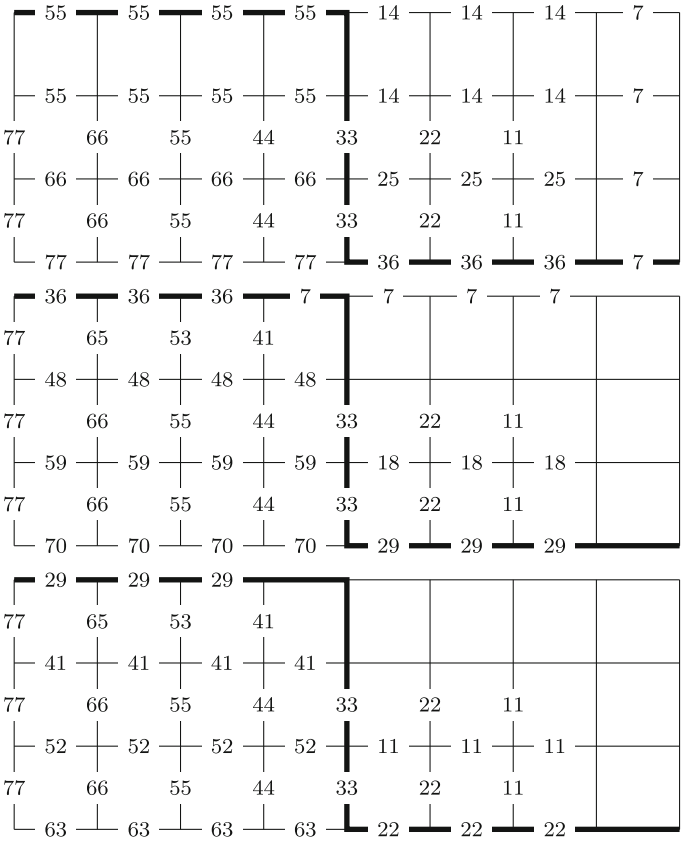


Fig. 12 An example of the edge values on the grid

$a_i = (V - i\alpha) - (w - 1 - i)\beta \geq 1$. $a_0, a_1, \ldots, a_{w-1}$ is a linear sequence, the first element is $V - (w-1)\beta = w\beta > 1$, and the last element is $V - (w-1)\alpha = 1$, hence all elements of the linear sequence is at least 1.

Let $M = \bigcup_{i=0}^{\ell-1} M_i$. We have defined all the edge values in M, we extend these values for the whole grid.

First, we complete the upper right part of the grid. All column values are 0. For the row values, consider the uppermost row values of M, and give the same value to all row values that are above it as in Fig. 14. The column upper border of M is all zero, thus the consistency remains true. The upper bound part clearly inherits the monotonicity and submodularity of M. All points are qualified thus the strong variants need not be checked.

The left lower part can be extended similarly. The column values are now V, and for the row values, consider the lowermost row values of M, and give the same value to all row values that are below it as in Fig. 15. The column lower border of M is all along V, thus the consistency remains true. The lower bound part clearly inherits the monotonicity and submodularity of M. All points are unqualified thus the strong variants need not be checked.

Set the value of all the edges both in columns and rows right from M to zero. Now the only undetermined values are the edges left from $w_0 - w$ (if they exist). Let all row values

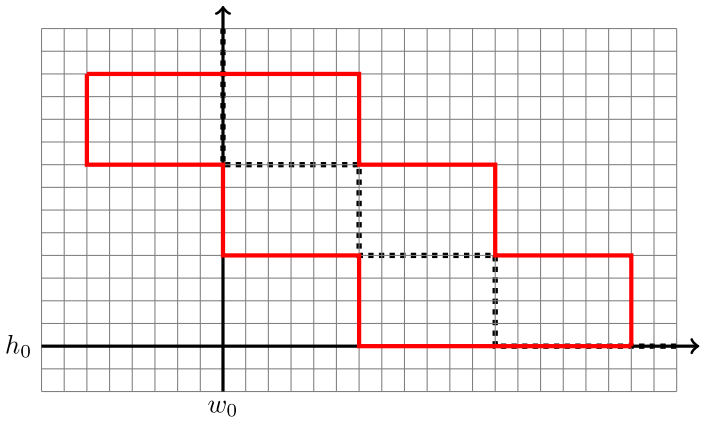


Fig. 13 Values in M (area demarcated in red) are known, we need to extend it to the whole grid (Color figure online)

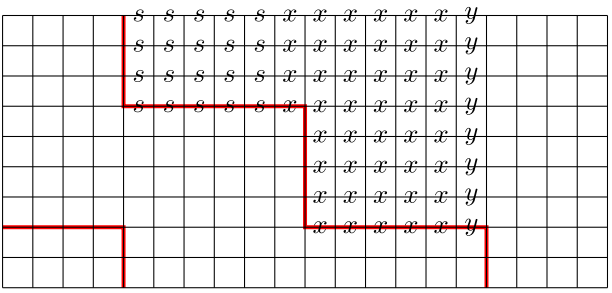
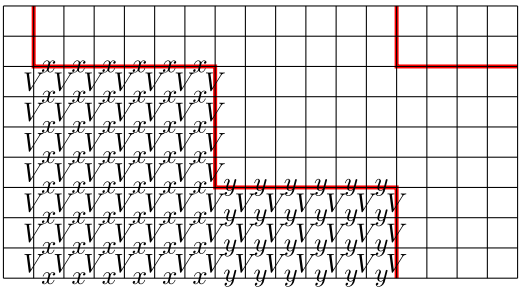


Fig. 14 Above M, the value of every vertical edge is 0, and the value of a horizontal edge is the value of the one strictly below it

Fig. 15 Below M, the value of every vertical edge is V, and the value of a horizontal edge is the value of the one strictly above it



be $1 + (h-1)\beta + (\ell-1)\Delta$ (this is the largest value in $M_{\ell-1}$), all column values below the $y = \ell h - 1$ line be V, and the values above that line be 0.

We have defined the values for the whole grid. The largest column value is clearly V, and the largest row value is $1 + (h-1)\beta + (\ell-1)\Delta$.

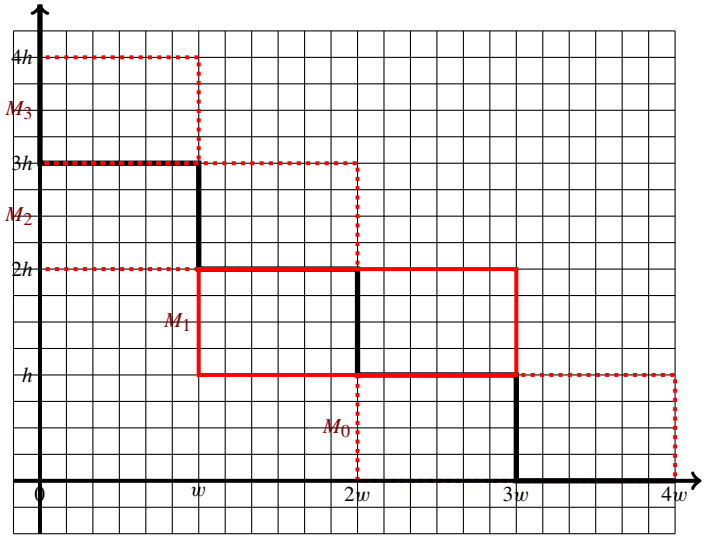
Recall that α, β, and Δ were chosen as $\alpha = \frac{V-1}{w-1}$, $\beta = \frac{V}{2w-1}$, and $\Delta = (1-\alpha)-(h-1)\beta$. It is a routine to check that using V as the bound in (17), $\Delta \geq 0$, and $V = 1+(h-1)\beta+(\ell-1)\Delta)$ indeed, which finishes the proof. □

Theorem 4 *Consider the regular staircase* Γ *of width* w*, height* h *and length* ℓ *with* $x_1 = 0$ *and* $w \geq h$ *(*(x_1, y_1) *is the leftmost point). Then*

$$\kappa(\Gamma) = \frac{((\ell-1)w-1)(2w-1)}{((\ell-1)h-1)w + (2w + (\ell-1) - 2)(w-h)}.$$

Remark: The Shannon complexity of Γ is the same as if we consider the regular staircase of width w, height h, and length $\ell - 1$ for which $x_1 \neq 0$.

Proof A regular staircase of width w, height h and length ℓ contains every other regular staircase with the same width, height, and less length (the containing does not depend if the leftmost point of the staircases is on the y axis or not). Thus the lower bound for $\kappa(\Gamma)$ is trivial.



For the upper bound construct the values for M_0, M_1,…,$M_{\ell-2}$ as in the previous proof. For $M_{\ell-1}$, only the right $w \times h$ part is in the non-negative grid, hence we only need to define the values in that part. Let the right part of $M_{\ell-1}$ be the right part of $M_{\ell-2}$ increased by Δ. The values in the grid can be easily extended to the whole grid.

The largest vertical value is $V = \kappa(\Gamma)$. The largest horizontal values are now in the 0th row of $M_{\ell-2}$ (or equivalently in the hth row of $M_{\ell-1}$), that is $1 + (h-1)\beta + (\ell-2)\Delta$. The same calculation can be applied as before to show that this is equal to $\kappa(\Gamma)$. □

3 An optimal secret sharing scheme

We investigate the bipartite access structure given by the three points, $(0, m+k)$, (ℓ, k), $(n+\ell, 0)$ for $m, k, n, \ell \in \mathbb{N}$. The Shannon-complexity of this access structure is $2 - 1/n$ [15] if $n \geq m$, but it was unknown if this bound can be achieved. We were able to create an optimal secret sharing scheme for this family of bipartite access structures. The optimal secret sharing scheme for the case (m, k), $(m+n, 0)$ was created in [18], we also present a different optimal

scheme. Our schemes are linear: the shares of the participants and the secret are represented as linear subspaces of a vector space. By the duality, our construction yields an optimal secret sharing scheme for bipartite staircases defined by two points if neither of them is on the axes.

It is more convenient to make our constructions over the reals. It does not make any difference because for any vector space V over $\mathbb{R}$ and finitely many vectors $\{v_i \in V : i \in I\}$ there is a vector space W of the same dimension over every finite field $\mathbb{F}$ of large enough characteristic and vectors $\{w_i \in W : i \in I\}$ such that for every $I' \subseteq I$, the dimension of the subspace spanned by $\{v_i : i \in I'$ is the same as the dimension of the subspace spanned by $\{w_i : i \in I'\}$ [28].

An optimal secret sharing scheme for the bipartite staircase defined by points (0,3),(1,1),(3,0) was presented in [15]. That work has served as a starting point for us, our construction uses the same techniques but in a more general way.

Before we start the proof, we would like to introduce an important concept from [15] that will be used in the proof. The construction requires the use of independent values, we refer to these as generic numbers. To be more precise, if we consider all vectors as rows of a huge matrix then any $k \times k$ submatrix that contains a generic entry is non-singular. This can be achieved easily by choosing all unspecified values to be algebraically independent.

We begin our construction for the bipartite access structure defined by the points $(0, m + 1)$, $(1, 1)$, $(n + 1, 0)$. This construction will be the base of our secret sharing schemes, as all the other construction can be obtained from it by only making small modifications.

Proposition 1 *There exists a linear scheme with complexity* $2 - 1/n$ *for the bipartite access structure* Γ *defined by the points* $(0, m + 1), (1, 1), (n + 1, 0)$ *where* $n \geq m$, $n, m \in \mathbb{N}$, $n, m \geq 1$.

Proof Following ideas of [15], we represent the shares of the participants and the secret with a linear subspace of a linear space. The actual shares (and secret) can be computed by orthogonal projection of a random element of the vector space on these subspaces. Denote the subspace assigned to $a \in P_1$, $b \in P_2$ and the secret by E_a, E_b and E_0 respectively. First, we summarize the requirements that the construction has to satisfy.

(a) for every $a \in P_1$ and $b \in P_2$, the linear hull of $E_a \cup E_b$ contains E_0;
(b) For every $n + 1$ participants from P_1, the linear hull of subspaces assigned to them contains E_0.
(c) For every $m + 1$ participants from P_2, the linear hull of subspaces assigned to them contains E_0.
(d) For every n participants from P_1, the linear hull of subspaces assigned to them intersects E_0 trivially.
(e) For every m participants from P_2, the linear hull of subspaces assigned to them intersects E_0 trivially.

Let $N = n^2 + 2n - 1$ be the dimension of the vector space we work in. For every $a \in P_1$ and $b \in P_2$, E_a and E_b are of dimension $2n - 1$, while E_0 is an n dimensional subspace. We define the subspaces with their bases.

The construction uses strings (vectors of length shorter than N) of different lengths. To make it easier to follow we write the length as superscript. For example, v^k denotes a string of length k, e_i^N denotes the string with 1 in the ith coordinate and 0 in every other, 0^k is a string with all k coordinates zero, and finally, α^k is a string of length k with k different generic elements, each chosen independently.

$$E_a = \left(\begin{array}{ccccc|ccccccccc} 1 & \alpha_1 & \alpha_2 & 0 & 0 & \alpha_7 & \alpha_8 & \alpha_9 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \alpha_3 & \alpha_4 & 0 & 0 & 0 & 0 & 0 & \alpha_7 & \alpha_8 & \alpha_9 & 0 & 0 & 0 \\ 1 & \alpha_5 & \alpha_6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_7 & \alpha_8 & \alpha_9 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

$$E_b = \left(\begin{array}{ccccc|ccccccccc} 1 & 0 & 0 & \beta_1 & \beta_2 & \beta_7 & 0 & 0 & \beta_8 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & \beta_3 & \beta_4 & 0 & \beta_7 & 0 & 0 & \beta_8 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & \beta_5 & \beta_6 & 0 & 0 & \beta_7 & 0 & 0 & \beta_8 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

$$E_0 = \left(\begin{array}{ccccc|ccccccccc} s_1 & s_2 & s_3 & s_4 & s_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ s_6 & s_7 & s_8 & s_9 & s_{10} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Fig. 16 E_a, E_b, E_0 in the case of $n = 3, m = 2, \alpha_1, \ldots, \alpha_9, \beta_1, \ldots, \beta_8, s_1, \ldots s_{15}$ are generic values. The basis vectors are in the rows of the matrices.

The secret E_0 can be generated by n vectors. The basis is: $s_i^{2n-1}0^{n^2}$ for $i = 1, \ldots, n$ where s_i^{2n-1} is composed from $2n-1$ generic values. We note that the last n^2 coordinates of $s \in E_0$ are 0.

The vectors that are in the basis of E_a and E_b are composed of two parts. The first $2n-1$ coordinates of E_a and E_b are used to recover the secret (as the secret has non-zero coordinates in only these places), while the goal of the second n^2 part is to provide security if there are at most n participant from P_1 or m from P_2.

The subspace E_a assigned to $a \in P_1$ can be generated by $2n-1$ vectors. It is useful to define $\gamma_i^{n^2} \in \mathbb{R}^{n^2}$ as a concatenation of $n(i-1)$ zeros, α^n, and $n(n-i)$ zeros: $\gamma_i^{n^2} = (0^{n(i-1)}, \alpha^n, 0^{n(n-i)})$. It is important that each $\gamma_i^{n^2}$ uses the same generic α for every $i = 1, \ldots, n$. Now we can present a basis of E_a. There are two types of vectors in E_a, for an example see Fig. 16:

- First type: $x_i^N = (1^1, \alpha_i^{n-1}, 0^{n-1}, \gamma_i^{n^2})$ for $i = 1, \ldots, n$. α_i^{n-1} consists of different generic values for every i.
- Second type: e_i^N for $i = n+1, \ldots, 2n-1$.

The subspace assigned to $b \in P_2$ can be generated by $2n-1$ vectors. $\delta_i^{mn} \in \mathbb{R}^{mn}$ is a vector of length mn, starting with $i-1$ zeros, then $\beta_1, \beta_2, \ldots, \beta_m$ generic values separated with 0^{n-1} each, and finally $n-i$ zeros in the end: $\delta_i^{mn} = (0^{i-1}, \beta_1, 0^{n-1}, \beta_2, 0^{n-1}, \ldots, \beta_{m-1}, 0^{n-1}, \beta_m, 0^{n-i})$. The generic values with the same index are the same for every δ_i^{mn}. The basis of E_b is (see Fig. 16 for an example):

- First type: $y_i^N = (1^1, 0^{n-1}, \rho_i^{n-1}, \delta_i^{mn}0^{(n-m)n})$ for $i = 1, \ldots, n$. ρ_i^{n-1} is composed from $n-1$ generic values, which are chosen independently for each i.
- Second type: e_i^N for $i = 2, \ldots, n$.

We note that with the choice of $m = n = 2$, the bipartite access structure is (0,3),(1,1),(3,0) from [15], and this secret sharing scheme is identical to the one they presented. The proof that conditions (a)–(e) hold is also similar to the one in [15] but it is more complex due to the larger size and more number of vectors. Our goals in (a)–(c) are to show that the subspace corresponding to a qualified set contains $e_1, \ldots, e_{2n-1}$, while in (d)–(e) we show that the intersection of the subspaces assigned to the secret and an unqualified set is trivial.

(a) $e_2^N, \ldots, e_{2n-1}^N$ is in $E_a \cup E_b$, hence we only need to show that e_1^N is in the linear hull of $\in E_a \cup E_b$. There is a non-trivial linear combination of $x_1^N, \ldots, x_n^N, y_1^N, \ldots, y_n^N$ such that the last n^2 coordinates are 0s. If $\alpha^n = (t_1, \ldots, t_n)$, then

$$\sum_{i=1}^{m} \beta_i \gamma_i^{n^2} - \sum_{i=1}^{n} t_i (\delta_i^{mn} 0^{(n-m)n}) = 0^{n^2},$$
$$\sum_{i=1}^{m} \beta_i x_i^N - \sum_{i=1}^{n} t_i y_i^N = \psi^{2n-1} 0^{n^2},$$

where ψ^{2n-1} is $2n-1$ non-zero values, the exact value is not interesting. $\psi^{2n-1}0^{n^2}$ and e_i^N $i = 2, \ldots, 2n-1$ are in the linear hull of $\in E_a \cup E_b$, hence $\psi^1 0^{n^2+2n-2}$ also for some non-zero ψ and so thus e_1^N too is in the linear hull.

(b) First we note that e_i^N for $i = n+1, \ldots 2n-1$ is in the linear hull. Consider x_i^N for all the $n+1$ chosen participants from P_1. These have n non-zero coordinates in the last n^2 coordinates, all in the same positions, hence the vector $(1^1, \psi^{n-1}, 0^{n^2+n-1})$ is in the linear hull of these $n+1$ vectors for some non-zero ψ^{n-1}. Computing these values for $i = 1, \ldots, n$, we get n different vectors with all zeros but the first n coordinates. These are generic, hence these n vectors must be linearly independent and therefore the linear hull of the vectors must contain $e_1^N, \ldots, e_n^N$.

(c) The same works as in (b), the only difference is that there are only $m+1$ participants, but there are only m non-zero values in the last n^2 coordinates, so that is not a problem.

(d) First consider only the n^2 vectors of the first type. The last n^2 coordinates of the vectors in E_0 are zeros, thus a non-trivial linear combination must have the same property. However as α^n is generic, the $n^2 \times n^2$ matrix made from the last n^2 coordinates from all the n^2 vectors of the first type must be non-singular. Therefore there is no non-trivial linear combination of vectors of the first type with zeros in the last n^2 coordinates. The linear hull of $e_{n+1}^N, \ldots e_{2n-1}^N$ intersects E_0 trivially, because E_0 is generic, hence the linear hull of the subspaces intersect E_0 trivially as well.

(e) The proof is essentially the same as for part (d).

□

Theorem 5 *There is a linear scheme with complexity* $2-1/n$ *for the bipartite access structure* Γ *defined by the points* $(0, m+k), (\ell, k), (n+\ell, 0)$ *where* $n \geq m$, $n, m, k, \ell \in \mathbb{N}$, *and* $m, n, k, \ell \geq 1$.

Proof We use the previous construction as a base and slightly modify it. The main idea is that if we add a new coordinate with a generic value to the end of each vector in the previous construction, then a new participant is needed to eliminate this extra coordinate. We need to execute that step independently for all vectors in E_a or E_b if we want to increase the participants needed from P_1 or P_2.

First, we show the constructions for the bipartite structures defined by the points $(0, m+1), (2, 1), (n+2, 0)$ and $(0, m+2), (1, 2), (n+1, 0)$. The construction for $(0, m+k), (\ell, k), (n+\ell, 0)$ can be established by combining the two methods separately multiple times.

$(0, m+1), (2, 1), (n+2, 0)$: Extend each vector with $2n-1$ coordinates. Let ϵ_i^{2n-1} denote a string with a generic value at the ith coordinate, and zeros in the others. The new share of $a \in P_1$ is:

- $(x_i^N, \epsilon_i^{2n-1})$ for $i = 1, \ldots, n$,

$$E_a = \left(\begin{array}{ccc|cccccccc} 1 & \alpha_1 & 0 & \alpha_3 & \alpha_4 & 0 & 0 & \alpha_5 & 0 & 0 \\ 1 & \alpha_2 & 0 & 0 & 0 & \alpha_3 & \alpha_4 & 0 & \alpha_6 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_7 \end{array}\right)$$

$$E_b = \left(\begin{array}{ccc|cccccccc} 1 & 0 & \beta_1 & \beta_3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & \beta_2 & 0 & \beta_3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

$$E_0 = \left(\begin{array}{ccc|cccccccc} s_1 & s_2 & s_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ s_4 & s_5 & s_6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Fig. 17 E_a, E_b, E_0 in the case of $n = 2, m = 1$. We add a generic value to the end of every vector in the base of E_a, while only zeros in the case of E_b and E_0

- $(e_i^N, \epsilon_i^{2n-1})$ for $i = n+1, \ldots, 2n-1$.

The share of $b \in P_2$ and the secret are only changed by adding 0^{2n-1} to the end of all vectors.

$(0, m+2), (1, 2), (n+1, 0)$: The construction is very similar to the previous one. The only difference is that we add ϵ_i^{2n-1} to the end of the vectors in E_b, $b \in P_2$, and 0^{2n-1} to the end of the vectors in E_a, $a \in P_1$.

To get a secret sharing scheme on $(0, m+k), (\ell, k), (n+\ell, 0)$, perform the first extension step (as for $(0, m+1), (2, 1), (n+2, 0)$) $\ell - 1$ and the second extension step (as for $(0, m+2), (1, 2), (n+1, 0)$) $k-1$ times one after the other.

The arrangement realizes the bipartite structure $(0, m+k), (\ell, k), (n+\ell, 0)$ if the following five conditions hold:

(a) For every ℓ participants from P_1 and every k participants from P_2, the linear hull of subspaces assigned to them contains E_0.
(b) For every $n+\ell$ participants from P_1, the linear hull of subspaces assigned to them contains E_0.
(c) For every $m+k$ participants from P_2, the linear hull of subspaces assigned to them contains E_0.
(d) For every $n+\ell-1$ participants from P_1 and every $k-1$ participants from P_2, the linear hull of subspaces assigned to these participants intersect E_0 trivially.
(e) For every $\ell - 1$ participants from P_1 and every $m+k-1$ participants from P_2, the linear hull of subspaces assigned to these participants intersect E_0 trivially.

We prove that the constructed secret sharing scheme satisfies all of these conditions. First, let v and w be two vectors with the following properties: $supp(v) = supp(w)$ ($supp(v)$ denotes the support of v), the first coordinate of both vectors is 1 and the other non-zero coordinates are different generic values. Denote the index of one of the non-zero coordinates by i, $i \neq 1$. It is possible to construct a new vector v' (or in other words eliminate the i coordinate of v with w) such that the first coordinate of v' is 1, and $supp(v') = supp(v) \cup \{i\}$. The construction of v' is easy, $v' = \frac{1}{w_i - v_i}(w_i v - v_i w)$. ($v_i$ and w_i are the ith coordinates of v and w respectively, $v_i \neq w_i$).

(a),(b),(c): Every vector in E_a, $a \in P_1$ has $\ell - 1$, and every vector in E_b, $b \in P_2$ has $k-1$ extra non-zero coordinates in compare to the construction in Proposition 1. However there are $\ell - 1$ more participants from P_1 in (a) and (b), and $k-1$ more participants from P_2 in (a) and (c). The share of each of those extra participants can be used to eliminate one extra coordinate from the vectors of the others (see the method above). As the number of the extra non-zero coordinates and the extra participants are equal, therefore after eliminating all the extra coordinates, they can recover the secret as in Proposition 1.

$$E_b = \left(\begin{array}{ccccc|ccccccccc} 0 & 0 & 0 & 0 & 0 & \beta_1 & 0 & 0 & \beta_2 & 0 & 0 & \beta_3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \beta_1 & 0 & 0 & \beta_2 & 0 & 0 & \beta_3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \beta_1 & 0 & 0 & \beta_2 & 0 & 0 & \beta_3 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Fig. 18 E_b in the case of (1,1),(3,0)

(d): Suppose that there exists a non-trivial linear combination of the vectors of the participants that is equal to a vector s from E_0. We note that s has only zero coordinates, except for the first $2n-1$. The last $(k-1)(2n-1)$ coordinates of every vector from E_a, $a \in P_1$ is 0, however, if we put the last $(k-1)(2n-1)$ coordinates of all the $2n-1$ vectors of all the $k-1$ participants from P_2 in a square matrix, then the resulting matrix is non-singular because of the generic values. Therefore none of the shares of the participants from P_2 was used for the linear combination. Now consider only vectors of the first type of the participants from P_1 and put them in a matrix. Remove the first $2n-1$ columns and those columns that contain only zero elements. The remaining entries form a non-singular $n(n+\ell-1) \times n(n+\ell-1)$ matrix because of the generic values, therefore no vector of the first type is used in the linear combination. E_0 intersects the linear hull of vectors of the second type trivially and so we get a contradiction.

(e): The proof is essentially the same as for part (d), but the roles of a and b are reversed. □

Theorem 6 *There exists a linear scheme with complexity* $2 - 1/n$ *for the bipartite access structure* Γ *defined by the points* (m, k), $(m+n, 0)$, $m, k, n \in \mathbb{N}$, $m, n, k \geq 1$.

Proof The proof is very similar to Theorem 5, hence we provide only a sketch. First, we construct the shares for $(1, 1)$, $(n+1, 0)$. The subspaces assigned to participants in P_1 and the secret are the same as in the case of the bipartite structure $(0, m+1)$, $(1, 1)$, $(n+1, 0)$. The subspaces assigned to participants in E_b are slightly changed:

- First type: $y_i = (0^{2n-1}, \delta_i^{n \cdot n})$ for $i = 1, \ldots, n$.
- Second type: e_i^N for $i = 2, \ldots, n$.

The shares for (m, k), $(m+n, 0)$ are made from the shares $(1, 1)$, $(n+1, 0)$ the same way as the shares of $(0, m+k)$, (ℓ, k), $(n+\ell, 0)$ made from $(0, m+1)$, $(1, 1)$, $(n+1, 0)$ by adding ϵ_i and 0^{2n-1} to the end of the shares. □

Using the properties of duality we can compute the linear complexity and the information ratio for bipartite access structures defined by two points. It is easy to show that the dual of a bipartite access structure is also bipartite.

Theorem 7 *There exists a linear scheme with complexity* $2 - 1/n$ *for the bipartite access structure* Γ *defined by the points* $(\ell, m+k)$, $(n+\ell, k)$ *if* $n, m, \ell, k \neq 0$ *and* $n \geq m$.

Proof Let $s = P_1$ and $t = P_2$. The maximal unqualified sets in Γ are $(\ell - 1, t)$, $(n+\ell-1, m+k-1)$ and $(s, k-1)$ hence the dual of Γ is a bipartite access structure given by the points $(0, t-k+1)$, $(s-n-\ell+1, t-m-k+1)$, $(s-\ell+1, 0)$. With the notation $a = s-n-\ell+1$, $b = t-m-k+1$, the three points can be written in the more familiar form $(0, m+b)$, (a, b), $(n+a, 0)$. Theorem 5 implies that the linear complexity of $\Gamma^\perp$ is $\lambda(\Gamma^\perp) = 2 - 1/n$. Using the properties of the duality

$$\lambda(\Gamma) = \lambda(\Gamma^\perp) = 2 - 1/n$$

□

Corollary 1 *Let Γ be an access structure given by two points, $(\ell, m+k)$, $(n+\ell, k)$, $n \geq m$. If $\ell = k = 0$ then $\sigma(\Gamma) = 1$, otherwise $\sigma(\Gamma) = 2 - 1/n$.*

Proof There are three cases, depending on if both, one of, or neither of ℓ and k is 0. If $\ell = k = 0$, the access structure is ideal [27]. If exactly one of ℓ and k is 0, then the lower bound is due to Lemma 3, while the upper bound is from [18] or Theorem 6. If neither of ℓ and k is 0, then the lower bound is due to Lemma 3 once again, and the upper bound is from Theorem 7. □

4 Conclusions

In this paper, we presented two results on bipartite access structures. We computed the Shannon complexity of regular bipartite access structures. An interesting open question is to construct efficient secret sharing schemes for such structures, as the best-known share is proportional to the length of the staircase. Our second result is optimal linear secret sharing schemes for bipartite structures defined by three points $(0, y_1)$, (x_2, y_2), $(x_3, 0)$. As a consequence of duality, the construction also yields an optimal secret sharing scheme for the bipartite access structures given by two points (x_1, y_1), (x_2, y_2), $x_1, y_2 \neq 0$.

Funding Open access funding provided by Eötvös Loránd University.

References

1. Beimel A.: Secret-sharing schemes: a survey. In: Proceedings of the Third International Conference on Coding and Cryptology (IWCC'11), pp. 11–46. Springer, Berlin (2011).
2. Bellare M., Neven G.: Identity-based multi-signatures from RSA. In: Topics in Cryptology-CT-RSA. Lecture Notes in Computer Science, vol. 4377. Springer, Berlin.
3. Ben-Or M., Goldwasser S., Wigderson A.: Completeness theorems for non-cryptographic fault-tolerant distributed computations. In: Proceedings of the 20th ACM Symposium on the Theory of Computing, pp. 1–10 (1988).
4. Blakley G.R.: Safeguarding cryptographic keys. Proc. Nat. Comput. Conf. **48**, 313–317 (1979).
5. Blundo C., De Santis A., Stinson D.R., Vaccaro U.: Graph decomposition and secret sharing schemes. J. Cryptol. **8**, 39–64 (1995).
6. Bonawitz K.A., Ivanov V., Kreuter B., Marcedone A., McMahan H.B., Patel S., Ramage D., Segal A., Seth K.: Practical Secure Aggregation for Federated Learning on User-Held Data, NIPS Workshop on Private Multi-Party Machine Learning (2016).
7. Brickell E.F.: Some ideal secret sharing schemes. J. Comb. Math. Comb. Comput. **9**, 105–113 (1989).
8. Chaum D., Crépeau C., Damgåard I.: Multiparty unconditionally secure protocols. In: 20th ACM Symposium on the Theory of Computing, pp. 11–19 (1988).
9. Cramer R., Damgård I., Maurer U.: General secure multi-party computation from any linear secret-sharing scheme. In: Advances in Cryptology-EUROCRYPT, vol. 18 (2000).
10. Csirmaz L.: The size of a share must be large. J. Cryptol. **10**, 223–231 (1997).

11. Csirmaz L.: An impossibility result on graph secret sharing. Des. Codes Cryptogr. **53**, 195–209 (2009).
12. Csirmaz L.: Secret sharing on the d-dimensional cube. Des. Codes Cryptogr. **74**, 719–729 (2015).
13. Csirmaz L.: Secret sharing and duality. J. Math. Cryptol. **15**(1), 157–173 (2021).
14. Csirmaz L., Tardos G.: Optimal information rate of secret sharing schemes on trees. IEEE Trans. Inf. Theory **59**, 2527–2630 (2013).
15. Csirmaz L., Matus F., Padró C.: Bipartite secret sharing and staircases. arxiv:2103.04904.
16. Csiszár I., Körner J.: Information Theory. Coding Theorems for Discrete Memoryless Systems. Academic Press, New York (1981).
17. Farràs O., Martí-Farré J., Padró C.: Ideal multipartite secret sharing schemes. J. Cryptol. **25**(3), 434–463 (2012).
18. Farràs O., Metcalf-Burton J.R., Padró C., Vàzquez L.: On the optimization of bipartite secret sharing schemes. Des. Codes Cryptogr. **63**(2), 255–271 (2012).
19. Farràs O., Kaced T., Martin S., Padró C.: Improving the linear programming technique in the search for lower bounds in secret sharing. IEEE Trans. Inf. Theory **66**(11), 7088–7100 (2020).
20. Gharahi M., Dehkordi M.H.: Perfect secret sharing schemes for graph access structures on six participants. J. Math. Cryptol. **7**, 143–146 (2013).
21. Goyal V., Pandey O., Sahai A., Waters B.: Attribute-based encryption for fine-grained access control of encrypted data. In: 13th ACM Conference on Computer and Communications Security, pp. 89–98 (2006).
22. Gyarmati M., Ligeti P.: Smallest graph achieving the Stinston bound. IEEE Trans. Inf. Theory **66**(7), 4609–4612 (2020).
23. Gyarmati M., Ligeti P.: On the information ratio of graphs without high-degree neighbors. Discret. Appl. Math. **304**(15), 55–62 (2021).
24. Jackson W., Martin K.M.: Geometric secret sharing schemes and their duals. Des. Codes Cryptogr. **4**, 83–95 (1994).
25. Jackson W., Martin K.M.: Perfect secret sharing schemes on five participants. Des. Codes Cryptogr. **9**, 233–250 (1996).
26. Ng S.-L.: Ideal secret sharing schemes with multipartite access structures. IEEE Proc. Commun. **153**, 165–168 (2006).
27. Padró C., Sáez G.: Secret sharing schemes with bipartite access structure. IEEE Trans. Inf. Theory **46**(7), 2596–2604 (2000).
28. Rado R.: Note on independence functions. Proc. Lond. Math. Soc. 7 (1957).
29. Shamir A.: How to share a secret. Commun. ACM **22**, 612–613 (1979).
30. van Dijk M.: On the information rate of perfect secret sharing schemes. Des. Codes Cryptogr. **6**, 143–160 (1995).
31. Simmons G.J.: How to (really) share a secret. In: Advances in Cryptology-CRYPTO'88. Lecture Notes in Computer Science, vol. 403, pp. 390–448 (1990).
32. Sun H.L., Chen B.L.: Weighted decomposition construction for perfect secret sharing schemes. Comput. Math. Appl. **43**, 877–887 (2002).