# General versus Linear Secret Sharing under Statistical Security on Five Participants

Shahram Khazaei
Department of Mathematical Sciences, Sharif University of Technology, Tehran, Iran
shahram.khazaei@sharif.ir

**Abstract**

How few participants are needed before general secret-sharing schemes can outperform linear ones under a fixed security notion? Under statistical security, we show that the answer is five participants; under perfect security, the corresponding threshold remains unknown. It is known that the 157 connected access structures on five participants split into 140 Shannon-exact cases and seventeen exceptional cases. For the former, linear schemes attain the Shannon polymatroid region; for each of the latter, the exact linear contribution region is the all-pairs one-common-information region and is strictly smaller than the Shannon region. We investigate the statistical contribution regions of these seventeen exceptional structures. For fifteen of them, we construct a partial scheme whose contribution vector lies outside the exact linear region; Jafari–Khazaei's partial-to-statistical transfer then gives a statistically secure family with the same asymptotic vector. One dual pair remains open. For $\Gamma_{30}$, we further show that the maximum information ratio under statistical security lies in $[14/9, 1.6502)$, improving both previously established bounds; moreover, $1.6502 < 5/3$, where $5/3$ is the optimum for linear schemes.

**Keywords:** secret sharing, statistical security, linear secret sharing, contribution region, information ratio, common information

## 1 Introduction

Under perfect security, general secret-sharing schemes are already known to outperform linear ones. For the twelve-participant union of the Fano and non-Fano matroid ports, perfect schemes attain maximum information ratios arbitrarily close to 1 [1], below the optimum $4/3$ for linear schemes [2]. The Fano and non-Fano matroids are representable over finite fields of characteristic two and of odd characteristic, respectively [3]. Since every perfect scheme is statistically secure and, within the linear class, statistical and perfect security have the same contribution region (Proposition 2.3), this example also gives a general-versus-linear separation under statistical security. The smallest number of participants admitting such a separation under statistical security was previously unknown. We prove that five participants are necessary and sufficient. The corresponding general-versus-linear threshold under perfect security remains between five and twelve.

A secret-sharing scheme (SSS) distributes a secret among participants so that prescribed subsets can recover it, while unqualified subsets obtain no information in the perfect setting

or asymptotically negligible information in the statistical setting [4, 5, 6]. Efficiency is often compressed to a maximum or average information ratio. We retain instead the complete vector of normalized share entropies, called the contribution vector (or information-ratio vector), because a scalar optimum can conceal participant tradeoffs.

For an access structure $\Gamma$, let $\Sigma_{\mathrm{lin}}(\Gamma)$ and $\Sigma_{\mathrm{stat}}(\Gamma)$ denote the contribution regions of linear and general schemes under statistical security, respectively. By Proposition 2.3, the linear contribution region is the same under perfect, partial, and statistical security. Let $K(\Gamma)$ be the Shannon polymatroid outer region, and let $K^{\text{one-CI}}(\Gamma)$ be the refinement obtained by imposing a separate common-information extension for every incomparable pair of subsets. These objects are defined in Section 2. We always have

$$\Sigma_{\mathrm{lin}}(\Gamma) \subseteq \Sigma_{\mathrm{stat}}(\Gamma) \subseteq K(\Gamma),$$
$$\Sigma_{\mathrm{lin}}(\Gamma) \subseteq K^{\text{one-CI}}(\Gamma) \subseteq K(\Gamma).$$

We call a strict inclusion

$$\Sigma_{\mathrm{lin}}(\Gamma) \subsetneq \Sigma_{\mathrm{stat}}(\Gamma)$$

a *regional separation under statistical security*. Such a separation compares general and linear schemes under the same security notion and need not improve an optimized scalar information ratio.

We study these regions for all connected access structures on five participants. Up to isomorphism, there are 180 full-support access structures on five participants, of which 157 are connected. Every disconnected access structure is a disjunctive union of connected components, and its contribution region can be recovered from those of the smaller components. Thus the connected structures are the genuinely nontrivial cases to be studied.

Bahariyan's Persian-language master's thesis first established the split into 140 Shannon-exact structures, with $K(\Gamma) = \Sigma_{\mathrm{lin}}(\Gamma)$, and seventeen exceptional structures, with $K^{\text{one-CI}}(\Gamma) = \Sigma_{\mathrm{lin}}(\Gamma) \subsetneq K(\Gamma)$ [7]. We present the classification in English and establish statistical separations for fifteen of the seventeen exceptional structures.

### 1.1 Related work and the five-participant threshold

The entropy method for lower-bounding share sizes was introduced by Capocelli, De Santis, Gargano and Vaccaro [8]; the polymatroidal linear program used here is a systematic form of that method [9, 10]. Farràs et al. strengthened this framework by common-information and Ahlswede–Körner extensions [10]. The underlying notions originate in the common information of Gács and Körner [11] and the source-coding converse of Ahlswede and Körner [12]; the common-information method for matroid ports was developed further in [13]. Jackson and Martin organized the five-participant case and numbered the 180 full-support isomorphism classes [14]. We use their numbering throughout. Thus $\Gamma_i$ denotes the Jackson–Martin class of index $i$; the minimal qualified sets of every connected class are listed in Appendix A.2. Jackson and Martin [14] determined the optimal information ratios for most five-participant access structures. Subsequent improvements to the lower and upper bounds [15, 16] left eight cases unresolved. Farràs et al. [10] settled those remaining cases for linear schemes, thereby completing the determination of the optimal linear information ratio for every five-participant access structure. Bahariyan [7] extended this classification to full contribution regions. In particular, he identified the seventeen

exceptional classes satisfying

$$\Sigma_{\mathrm{lin}}(\Gamma_i) = K^{\text{one-CI}}(\Gamma_i) \subsetneq K(\Gamma_i)$$

and introduced a recursive realization method based on $(\lambda, \omega)$-decompositions [17]. We recall the method briefly in Section 3; the access structures and the extreme points of their linear contribution regions are listed in Appendix A.2.

Several other families of small access structures have been studied in detail. These include graph access structures [18, 19], structures with three or four minimal qualified sets [20, 21], structures with intersection number one [22], and ports of non-representable matroids, including the Vámos matroid [23, 24, 25].

The main new contribution of this paper is the analysis under statistical security of the seventeen exceptional structures: for fifteen of them, we establish regional separations between general and linear schemes, and for $\Gamma_{30}$ we improve the two-sided bounds on the maximum information ratio. For completeness, we also present the linear classification and the recursive realization method, with the five-participant access structures and the extreme points of their linear contribution regions listed in Appendix A.2. Since all access structures on at most four participants are Shannon-exact [26, 27, 10], with the nonideal cases recorded in Appendix A.1, our separations show that five is the sharp participant threshold for a general-versus-linear separation under statistical security. They do not settle the corresponding general-versus-linear threshold under perfect security, which remains open.

### 1.2 Main results and significance

The seventeen exceptional structures form nine duality classes. We name a non-self-dual class by its member having the smaller Jackson–Martin index and write a star for its dual. Thus the nine classes are

$$\{\Gamma_{28}, \Gamma_{28}^*\},\ \{\Gamma_{30}, \Gamma_{30}^*\},\ \{\Gamma_{40}, \Gamma_{40}^*\},\ \{\Gamma_{53}, \Gamma_{53}^*\},\ \{\Gamma_{73}, \Gamma_{73}^*\},$$
$$\{\Gamma_{75}, \Gamma_{75}^*\},\ \{\Gamma_{76}, \Gamma_{76}^*\},\ \{\Gamma_{82}, \Gamma_{82}^*\},\ \{\Gamma_{88}\},$$

where ${\Gamma_{88}}^* \cong \Gamma_{88}$ (self-dual up to participant relabelling), and

$$\Gamma_{28}^* = \Gamma_{167}, \quad \Gamma_{30}^* = \Gamma_{153}, \quad \Gamma_{40}^* = \Gamma_{150}, \quad \Gamma_{53}^* = \Gamma_{152},$$
$$\Gamma_{73}^* = \Gamma_{151}, \quad \Gamma_{75}^* = \Gamma_{114}, \quad \Gamma_{76}^* = \Gamma_{140}, \quad \Gamma_{82}^* = \Gamma_{107}.$$

Let $\mathcal{E}$ denote this set of seventeen structures:

$$\begin{aligned}\mathcal{E} = \{&\Gamma_{28}, \Gamma_{28}^*, \Gamma_{30}, \Gamma_{30}^*, \Gamma_{40}, \Gamma_{40}^*,\\ &\Gamma_{53}, \Gamma_{53}^*, \Gamma_{73}, \Gamma_{73}^*, \Gamma_{75}, \Gamma_{75}^*,\\ &\Gamma_{76}, \Gamma_{76}^*, \Gamma_{82}, \Gamma_{82}^*, \Gamma_{88}\}.\end{aligned}$$

**Theorem 1.1** (Exact linear classification [7])**.** *Among the* 157 *connected access structures on five participants, exactly* 140 *satisfy*

$$K(\Gamma) = \Sigma_{\mathrm{lin}}(\Gamma).$$

*For every* $\Gamma \in \mathcal{E}$*, the Shannon region is not tight, but the all-pairs one-common-information region is exact:*

$$\Sigma_{\mathrm{lin}}(\Gamma) = K^{\text{one-CI}}(\Gamma) \subsetneq K(\Gamma).$$

Bahariyan [7] obtained the polyhedral part through the common-information framework of Farràs et al. [10] and realized the reported extreme points by a recursion based on weighted $(\lambda, \omega)$-decompositions. The procedure starts from nine labelled seed contribution vectors and closes under the decomposition, duality, and participant relabelling; see Section 3 and the appendices.

**Theorem 1.2** (Separations under statistical security)**.** *For every*

$$\Gamma \in \mathcal{E} \setminus \{\Gamma_{73}, \Gamma_{73}^*\},$$

*there exists a contribution vector* $c \in \Sigma_{\mathrm{stat}}(\Gamma)$ *that violates a facet-defining inequality of* $\Sigma_{\mathrm{lin}}(\Gamma)$*. Consequently,*

$$\Sigma_{\mathrm{lin}}(\Gamma) \subsetneq \Sigma_{\mathrm{stat}}(\Gamma).$$

Theorem 1.2 is restated and proved as Theorem 5.1.

Combining Theorem 1.2 with Shannon exactness for access structures on at most four participants gives the sharp threshold.

**Corollary 1.3** (Sharp participant threshold)**.**

$$\min\{n : \exists\, \Gamma \text{ on } n \text{ participants with } \Sigma_{\mathrm{lin}}(\Gamma) \subsetneq \Sigma_{\mathrm{stat}}(\Gamma)\} = 5.$$

Indeed, for access structures on at most four participants, $K(\Gamma) = \Sigma_{\mathrm{lin}}(\Gamma)$ [26, 27, 10], and hence $\Sigma_{\mathrm{lin}}(\Gamma) = \Sigma_{\mathrm{stat}}(\Gamma)$ from $\Sigma_{\mathrm{lin}}(\Gamma) \subseteq \Sigma_{\mathrm{stat}}(\Gamma) \subseteq K(\Gamma)$; the five-participant separation follows from Theorem 1.2.

Equivalently, eight of the nine exceptional duality classes are separated; the remaining class is the open dual pair $\{\Gamma_{73}, \Gamma_{73}^*\}$. The selected facets and certified construction values are given in Section 5.

**Linear classification and separation under statistical security.** Two questions should be distinguished. The first is the linear classification problem

$$K^{\text{one-CI}}(\Gamma) \stackrel{?}{=} \Sigma_{\mathrm{lin}}(\Gamma),$$

which was settled for the seventeen exceptional structures in [7]. The second is whether, under statistical security, the contribution region of general schemes is confined to the one-CI region:

$$\Sigma_{\mathrm{stat}}(\Gamma) \stackrel{?}{\subseteq} K^{\text{one-CI}}(\Gamma).$$

Because $K^{\text{one-CI}}(\Gamma) = \Sigma_{\mathrm{lin}}(\Gamma)$ for these structures, this is precisely the new general-versus-linear separation problem under statistical security. Our fifteen constructions show that the containment fails for fifteen of the seventeen exceptional structures; it remains open for $\Gamma_{73}$ and $\Gamma_{73}^*$.

**Improved information ratio.** A regional witness $c \in \Sigma_{\mathrm{stat}}(\Gamma) \setminus \Sigma_{\mathrm{lin}}(\Gamma)$ may reduce some share sizes while increasing others and therefore need not improve the best established bounds on the standard maximum or average information ratio. Indeed, except for $\Gamma_{30}$, none of the regional witnesses constructed here improves the previously established scalar

bounds; this does not determine the optimal maximum or average information ratios for those access structures. For $\Gamma_{30}$, however, we show that the maximum information ratio under statistical security lies in $[14/9, 1.6502)$, improving both previously established bounds. Farràs et al. [10] determined the optimum $5/3$ for linear schemes and established the lower bound $3/2$ for general schemes under statistical security. Our upper bound satisfies $1.6502 < 5/3$, while, by strengthening their Ahlswede–Körner method, we improve the lower bound from $3/2$ to $14/9$. See Section 6 for further details.

**The unresolved pair.** The two unresolved cases form the dual pair $(\Gamma_{73}, \Gamma_{73}^*)$. For both structures, the unique CI-sensitive facet is $c_1+c_2+c_3 \geq 5$, but neither a statistical violation nor an almost-entropic proof of this facet is known. Using the copy lemma [28, 29, 30], applied directly to the linear program as in [31], we derive the weaker converse bounds

$$c_1 + c_2 + c_3 \geq \frac{75}{17} \quad \text{for } \Gamma_{73}, \qquad c_1 + c_2 + c_3 \geq \frac{22}{5} \quad \text{for } \Gamma_{73}^*.$$

The corresponding copy sequences are specified in Section 7.

**Method.** For each exceptional structure, we choose a CI-sensitive facet of its exact linear region and seek a $\delta$-decomposition [32] whose gap-normalized contribution vector violates that facet. The components (subschemes) of the found decompositions are perfect linear schemes, group-characterizable non-perfect schemes, and explicit non-perfect rational joint probability distributions. The nonlinear schemes were found by computational searches and then recorded in exact rational form; their access functions and contribution vectors are recorded in Section 4 and Section B. The $\delta$-decomposition theorem of [32] (see Theorem 2.7) then transfers each strict violation to statistical security.

### 1.3 Organization

Section 2 gives the definitions and the two decomposition tools. Section 3 presents the formulation, selected settings, and recursive realization method for the linear classification. Section 4 introduces the components, and Section 5 presents the separating construction. The maximum-ratio result for $\Gamma_{30}$ is given in Section 6, while the two open cases and further questions are discussed in Section 7. The appendices list the relevant access structures and the extreme points of their linear contribution regions, together with the construction of the linear library.

## 2 Preliminaries

### 2.1 Secret-sharing schemes, security, and contribution vectors

Let $P = [n] = \{1, \ldots, n\}$ and let 0 denote the dealer. An access structure is a nonempty monotone family $\Gamma \subseteq 2^P$ with $\varnothing \notin \Gamma$. Its members are *qualified* and its nonmembers are *forbidden*. It has *full support* if every participant belongs to a minimal qualified set. It is *connected* if it is not a disjunctive union on any nontrivial partition of $P$. We specify $\Gamma$ by its minimal qualified sets. For example, $\Gamma = 123 + 45$ denotes the upward closure generated by the minimal qualified sets $\{1, 2, 3\}$ and $\{4, 5\}$.

A *secret-sharing scheme* (SSS) is any tuple

$$\Pi = (X_0, X_1, \ldots, X_n)$$

of jointly distributed finite-valued random variables with nonconstant secret $X_0$ and participant shares $X_1, \ldots, X_n$. Its contribution vector is

$$c = (c_1, \ldots, c_n), \qquad c_i = \frac{H(X_i)}{H(X_0)}.$$

The term SSS does not by itself impose any security notion. We use three notions in this paper: perfect security and statistical security, which are defined next, and partial security, which is recalled in Section 2.3.

For $A \subseteq P$, write $X_A = (X_i)_{i \in A}$. The SSS is *perfect* for $\Gamma$ if

$$H(X_0 \mid X_A) = 0 \quad (A \in \Gamma), \qquad I(X_0; X_B) = 0 \quad (B \notin \Gamma).$$

A linear perfect SSS is one in which the secret and shares are linear images of a uniform random vector over a finite-dimensional vector space over a finite field.

We use the worst-case statistical-security convention of Jafari–Khazaei [32, Sec. III-A]. A family $\{\Pi^{(m)}\}_{m \geq 1}$ statistically realizes $\Gamma$ if $\log |\operatorname{supp}(X_0^{(m)})| = O(m^d)$ for some constant $d > 0$, and for suitable reconstruction maps $R_{A,m}$ the quantities

$$\max_s \Pr[R_{A,m}(X_A^{(m)}) \neq s \mid X_0^{(m)} = s] \quad (A \in \Gamma)$$

and

$$\max_s \mathrm{SD}\big(P_{X_B^{(m)} \mid X_0^{(m)} = s}, P_{X_B^{(m)}}\big) \quad (B \notin \Gamma)$$

are negligible in $m$, where SD denotes statistical distance between two distributions. The polynomial bound on the secret length ensures that negligibility in $m$ also gives negligibility in the secret-length parameter; it does not alter the attainable asymptotic contribution vectors [32, Remark III.1].

The *linear contribution region* $\Sigma_{\mathrm{lin}}(\Gamma)$ is the topological closure of the set of contribution vectors of linear perfect SSSs for $\Gamma$, over all finite fields. The *statistical contribution region* $\Sigma_{\mathrm{stat}}(\Gamma)$ is the topological closure of the set of coordinatewise limits of contribution vectors of statistically secure families. Padding any participant's share with independent randomness preserves security and increases only that coordinate; therefore both regions are coordinatewise upward closed.

An *access function* on $P$ is a monotone set function $\Phi : 2^P \to [0, 1]$ satisfying $\Phi(\varnothing) = 0$. It is a weighted generalization of an access structure. The access structure $\Gamma$ corresponds to the binary access function

$$\Phi_\Gamma(A) = \mathbf{1}[A \in \Gamma].$$

Every SSS $\Pi$ induces the access function

$$\Phi_\Pi(A) = \frac{I(X_0; X_A)}{H(X_0)}.$$

The normalization by the secret entropy is what places $\Phi_\Pi$ in $[0, 1]$: nonnegativity of mutual information gives $\Phi_\Pi \geq 0$, and $I(X_0; X_A) \leq H(X_0)$ gives $\Phi_\Pi \leq 1$, with $\Phi_\Pi(A) = 1$ exactly when $X_A$ determines $X_0$. If $\Pi$ is perfect for $\Gamma$, then $\Phi_\Pi = \Phi_\Gamma$.

**Duality.** The *dual* of an access structure $\Gamma$ on $P$ is

$$\Gamma^* = \{A \subseteq P : \ P \setminus A \notin \Gamma\},$$

again a monotone family, with $\Gamma^{**} = \Gamma$. For an access function the corresponding operation is $\Phi^*(A) = 1 - \Phi(P \setminus A)$, which is monotone and $[0,1]$-valued whenever $\Phi$ is, and reduces to the above on indicators. Duality is relevant here because it acts on schemes and not merely on structures: if $\Pi$ is a linear scheme for $\Gamma$, there is a linear scheme for $\Gamma^*$ in which every participant holds a share of the same size [33, 27]. Hence

$$c \in \Sigma_{\mathrm{lin}}(\Gamma) \iff c \in \Sigma_{\mathrm{lin}}(\Gamma^*),$$

so the two linear regions coincide. Jafari and Khazaei [2] extended this to Abelian schemes, where the same conclusion holds. Section 3 uses duality as a construction closure on exactly this basis: a linear component for $\Gamma$ yields one for $\Gamma^*$ with the same contribution vector, up to the canonical relabelling that puts $\Gamma^*$ in the numbering of Appendix A.

### 2.2 Polymatroidal and extension outer regions

Each outer region below is obtained by imposing linear entropy constraints and projecting to the contribution coordinates. Adding valid extension constraints can only shrink the projected region. The Shannon region $K(\Gamma)$ is the projection of all normalized polymatroids satisfying the access equalities of $\Gamma$. This is the polymatroidal linear-programming relaxation developed for secret sharing by Csirmaz [9].

For $U \subseteq \{0, 1, \ldots, n\}$ write $X_U = (X_i)_{i \in U}$ and normalize

$$h(U) = \frac{H(X_U)}{H(X_0)}.$$

Then $h \geq 0$, $h(\varnothing) = 0$, $h(\{0\}) = 1$, and $h$ is monotone and submodular; thus it is a normalized polymatroid. Let $K(\Gamma)$ be the topological closure of the projection to $c_i = h(\{i\})$ of all such polymatroids satisfying

$$\begin{aligned} h(A \cup \{0\}) &= h(A) && (A \in \Gamma), \\ h(B \cup \{0\}) &= h(B) + 1 && (B \notin \Gamma). \end{aligned}$$

**Common-information extensions.** We use the common-information extension framework of Farràs et al. [10]. Let $\mathcal{B}(\Gamma)$ be the set of normalized polymatroids on the base variables $X_0, X_1, \ldots, X_n$ that satisfy the access equalities above, and let $\mathcal{I}_n$ be the set of unordered pairs $\{A, B\}$ of incomparable nonempty subsets of $\{0, 1, \ldots, n\}$.

For $\{A, B\} \in \mathcal{I}_n$, let $\mathcal{B}^{\mathrm{CI}(A,B)}(\Gamma)$ be the projection onto the base entropy coordinates of the polymatroids on $X_0, X_1, \ldots, X_n, Z_{A,B}$ that satisfy the access equalities for $\Gamma$ and

$$\begin{aligned} H(Z_{A,B} \mid X_A) = H(Z_{A,B} \mid X_B) = 0, \\ H(Z_{A,B}) = I(X_A; X_B). \end{aligned} \tag{1}$$

Thus $h \in \mathcal{B}^{\mathrm{CI}(A,B)}(\Gamma)$ precisely when the base polymatroid $h$ admits a common-information extension for the pair $\{A, B\}$.

We define the all-pairs one-common-information region in the base entropy space by

$$\mathcal{B}^{\text{one-CI}}(\Gamma) = \bigcap_{\{A,B\}\in\mathcal{I}_n} \mathcal{B}^{\text{CI}(A,B)}(\Gamma). \tag{2}$$

We denote the topological closure of the projection of $\mathcal{B}^{\text{one-CI}}(\Gamma)$ to the contribution coordinates $\big(h(\{1\}),\dots,h(\{n\})\big)$ by

$$K^{\text{one-CI}}(\Gamma) = \overline{\big\{\big(h(\{1\}),\dots,h(\{n\})\big) : h \in \mathcal{B}^{\text{one-CI}}(\Gamma)\big\}}. \tag{3}$$

Private padding shows that this closed projection, like $K(\Gamma)$, is coordinatewise upward closed.

The intersection in (2) is taken before projection to the contribution coordinates. Consequently, the same base polymatroid must admit a common-information extension for every incomparable pair. The extensions are nevertheless separate: each pair may use its own auxiliary variable $Z_{A,B}$, and no joint entropy involving auxiliary variables belonging to two different pairs is imposed. This is the meaning of $K^{\text{one-CI}}(\Gamma)$ in this paper.

For $n = 5$, the set $\mathcal{I}_n$ contains 1351 incomparable nonempty pairs, so the all-pairs construction uses 1351 separate one-CI extensions.

**Proposition 2.1** (Common-information containment)**.** *For every access structure* $\Gamma$*,*

$$\Sigma_{\text{lin}}(\Gamma) \subseteq K^{\text{one-CI}}(\Gamma).$$

This is the common-information property for linear random variables used in the framework of Farràs et al. [10]. More generally, group-characterizable random variables with commuting subgroups, and hence homomorphic schemes, satisfy the same property [34, Proposition 6.2 and Corollary 6.3].

### 2.3 Partial secret sharing

The SSS $\Pi$ *partially realizes* $\Gamma$ if its access function satisfies

$$D = \min_{A\in\Gamma} \Phi_\Pi(A) - \max_{B\notin\Gamma} \Phi_\Pi(B) > 0.$$

Its partial contribution vector is denoted by $c = (c_1,\dots,c_n)$, where

$$c_i = \frac{H(X_i)/H(X_0)}{D}.$$

A perfect scheme has $D = 1$ and recovers the earlier definition $c_i = H(X_i)/H(X_0)$. Thus the same notation $c$ is used for ordinary and partial contribution vectors; the normalizing denominator, stated in each context, distinguishes them.

Writing

$$L = \min_{A\in\Gamma} \Phi_\Pi(A), \qquad W = \max_{B\notin\Gamma} \Phi_\Pi(B),$$

we have $D = L - W$, and $c_i$ is the normalized share entropy of participant $i$ divided by that gap. We name $L$ and $W$ for each construction that appears later in the paper, for ease of reference.

Partial realization is useful because it transfers to statistical security. The following is [32, Theorem VI.1], specialized to the situation used here.

**Theorem 2.2** (Jafari–Khazaei partial-to-statistical transfer [32, Thm. VI.1])**.** *A partial SSS for* $\Gamma$ *with partial contribution vector* $c = (c_1, \ldots, c_n)$ *yields a statistically secure family for* $\Gamma$ *whose contribution vectors converge coordinatewise to* $c$*.*

**Proof idea.** The proof interprets the partial scheme as a wiretap broadcast channel whose legitimate receivers are the qualified coalitions and whose eavesdroppers are the forbidden coalitions. The gap $D$ is an achievable secrecy rate; coding near that rate divides every normalized share entropy by $D$ and gives a single statistically secure family converging to the whole vector $c$. We use only the consequence $c \in \Sigma_{\mathrm{stat}}(\Gamma)$.

**Proposition 2.3** (Security collapse for linear schemes [32])**.** *Within the linear class, statistical, partial, and perfect security have the same contribution region.*

**Proof idea.** The collapse of statistical to perfect security for linear schemes is standard [35]: restrict the secret space to the intersection of the kernels of the leakage maps of the finitely many forbidden coalitions. Statistical security makes the relative codimension vanish asymptotically, while qualified coalitions continue to reconstruct. The partial-security statement follows by applying [32, Proposition V.4 and Section III] to linear schemes.

### 2.4 $(\lambda, \omega)$-decompositions

The first decomposition tool works entirely inside the linear world: linear subschemes in, a linear scheme out. We state its most general form through the access-function formulation of Jafari and Khazaei [32, Definition VIII.1 and Theorem VIII.2]. It builds on Stinson's original $\lambda$-decomposition [26, 36], the weighted variant of Sun and Chen [37], the $(\lambda, \omega)$ extension of van Dijk, Jackson, and Martin [17], and its weighted generalizations by Gharahi and Khazaei [38, 19].

**Definition 2.4** (Weighted $(\lambda, \omega)$-decomposition)**.** Let $\lambda, \omega, m_1, \ldots, m_N$ be nonnegative integers with $0 \le \omega < \lambda$, and let $\Phi_1, \ldots, \Phi_N$ be rational-valued access functions on $P$ such that each $m_j \Phi_j$ is integer-valued. The pairs $(m_j, \Phi_j)$ form a weighted $(\lambda, \omega)$-decomposition of $\Gamma$ if

$$\sum_j m_j \Phi_j(A) \ge \lambda \qquad (A \in \Gamma),$$

$$\sum_j m_j \Phi_j(B) \le \omega \qquad (B \notin \Gamma).$$

**Theorem 2.5** ($(\lambda, \omega)$-decomposition)**.** *Let* $(m_1, \Phi_1), \ldots, (m_N, \Phi_N)$ *be a weighted* $(\lambda, \omega)$*-decomposition of* $\Gamma$*. If every* $\Phi_j$ *has a linear SSS with contribution vector* $c^{(j)}$*, all of the same field characteristic, then* $\Gamma$ *has a linear scheme with contribution vector*

$$\frac{1}{\lambda - \omega} \sum_j m_j c^{(j)}.$$

This linear-in/linear-out construction is used for the exact linear regions; the $\delta$-decomposition below allows arbitrary components but has a statistical conclusion.

### 2.5 $\delta$-decompositions

The second decomposition tool permits arbitrary nonnegative real weights and arbitrary SSS components, which need not be linear or perfect. Its conclusion is statistical rather than linear.

**Definition 2.6** ($\delta$-decomposition)**.** Let $\Gamma$ be an access structure on $P$. Let $\Phi_1, \dots, \Phi_N$ be access functions on $P$, and let $h_1, \dots, h_N$ be nonnegative real numbers. Define

$$\Psi = \sum_{j=1}^{N} h_j \Phi_j$$

and put

$$L = \min_{A \in \Gamma} \Psi(A), \qquad W = \max_{B \notin \Gamma} \Psi(B).$$

The pairs

$$(h_1, \Phi_1), \dots, (h_N, \Phi_N)$$

form a $\delta$-decomposition of $\Gamma$ if

$$\delta := L - W > 0.$$

The aggregate $\Psi$ is nonnegative, monotone, and vanishes at $\varnothing$, but it need not take values in $[0, 1]$ and therefore need not itself be an access function.

The following theorem is due to Jafari and Khazaei [32].

**Theorem 2.7** ($\delta$-decomposition theorem)**.** *Let*

$$(h_1, \Phi_1), \dots, (h_N, \Phi_N)$$

*be a $\delta$-decomposition of $\Gamma$. Suppose that, for every $j \in [N]$, the access function $\Phi_j$ is realized by an SSS $\Pi_j$ with contribution vector*

$$c^{(j)} = (c_1^{(j)}, \dots, c_n^{(j)}).$$

*Then*

$$c = \frac{1}{\delta} \sum_{j=1}^{N} h_j c^{(j)}$$

*belongs to $\Sigma_{\mathrm{stat}}(\Gamma)$.*

## 3 Bahariyan's linear classification

Following the common-information framework of Farràs et al. [10], Bahariyan [7] determined the exact linear contribution regions of all connected five-participant access structures. The polyhedral step computes either the Shannon region $K(\Gamma)$ or a selected one-CI refinement, while the realization step constructs every reported extreme point recursively by $(\lambda, \omega)$-decomposition, duality, and participant relabelling.

Appendix A lists the 157 connected five-participant access structures and the extreme points of their linear contribution regions. Bahariyan's recursion uses nine seed contribution vectors: the trivial one-participant seed, which is realizable over finite fields of every

characteristic, and eight further seeds listed in Appendix C, where their characteristic-universal realizability is proved. Since the recursive operations preserve this property, with the decomposition step supplied by Theorem 2.5, we obtain the following proposition. This is a statement about the particular library constructed here; characteristic independence fails for monotone span programs in general [39].

**Proposition 3.1** (Characteristic-universal five-participant library)**.** *For every prime $p$, each extreme contribution vector used in the classification of access structures on at most five participants is realizable over a finite extension of* $\mathrm{GF}(p)$*. Consequently, their linear contribution regions are independent of the field characteristic.*

## 4 Component catalogue

Every construction in Sections 5 and 6 is a nonnegative weighted sum of components from this section. For each component we specify the object from which its access function and contribution vector follow: a perfect linear scheme, a group-coset system, or a rational probability mass function.

### 4.1 Perfect linear components

A perfect linear component $L_j$ is specified by its labelled minimal qualified sets and contribution vector. Its access function is

$$\Phi_{L_j}(A) = \mathbf{1}\big[A \text{ contains one of the listed sets}\big]. \tag{4}$$

The labels $L_1, \dots, L_{53}$ are local to this paper. For an ideal component, the contribution vector is determined by the active participants and is omitted; nonideal vectors are displayed explicitly. The printed antichains are the actual labelled access structures used in the $\delta$-decompositions, not merely isomorphism-class representatives. Their linear realizations follow from the classification in Appendix A and the recursion in Appendix C. All 53 component types occur in the $\delta$-decompositions for the regional separations of Section 5 or in the improved maximum-ratio construction of Section 6.

Table 1: Labelled ideal perfect-linear components $L_1, \dots, L_{36}$. Each active participant has contribution one and each dummy participant contribution zero.

| component/class | minimal qualified sets | component/class | minimal qualified sets |
|---|---|---|---|
| $L_1$ | $1$ | $L_2$ | $1 + 345$ |
| $L_3$ | $2$ | $L_4$ | $3$ |
| $L_5$ | $4$ | $L_6$ | $1 + 5$ |
| $L_7$ | $2 + 3$ | $L_8$ | $2 + 4$ |
| $L_9$ | $3 + 4$ | $L_{10}$ | $12$ |
| $L_{11}$ | $2 + 13 + 145 + 345$ | $L_{12}$ | $25$ |
| $L_{13}$ | $23 + 14 + 25$ | $L_{14}$ | $34$ |
| $L_{15}$ | $13 + 14 + 34 + 25$ | $L_{16}$ | $1 + 24$ |
| $L_{17}$ | $24 + 35$ | $L_{18}$ | $13$ |
| $L_{19}$ | $23 + 25$ | $L_{20}$ | $13 + 15 + 35$ |
| $L_{21}$ | $134$ | $L_{22}$ | $14 + 15 + 45$ |
| $L_{23}$ | $23 + 24 + 34$ | $L_{24}$ | $23 + 124 + 134$ |
| $L_{25}$ | $235$ | $L_{26}$ | $2 + 45$ |
| $L_{27}$ | $34 + 35$ | $L_{28}$ | $23 + 4 + 25$ |
| $L_{29}$ | $12 + 13 + 24 + 34$ | $L_{30}$ | $1 + 45$ |
| $L_{31} \cong \Gamma_{144}$ | $123 + 124 + 234 + 125 + 245$ | $L_{32} \cong \Gamma_{98}$ | $13 + 234 + 15 + 245$ |
| $L_{33} \cong \Gamma_{102}$ | $13 + 24 + 235 + 145 + 345$ | $L_{34} \cong \Gamma_{115}$ | $12 + 134 + 234 + 135 + 245 + 345$ |
| $L_{35} \cong \Gamma_{29}$ | $12+13+23+14+24+15+35+45$ | $L_{36} \cong \Gamma_{172}$ | $124 + 135 + 2345$ |

Table 2: Labelled nonideal perfect-linear components $L_{37}, \ldots, L_{53}$ and their contribution vectors.

| component/class | minimal qualified sets | contribution vector |
|---|---|---|
| $L_{37}$ | $1 + 23 + 24 + 345$ | $(1, 2, 1, 1, 1)$ |
| $L_{38}$ | $12 + 24 + 45$ | $(1, 1, 0, 2, 1)$ |
| $L_{39}$ | $12 + 15 + 245$ | $(1, 2, 0, 1, 2)$ |
| $L_{40} \cong \Gamma_{39}$ | $12 + 13 + 24 + 34 + 35 + 45$ | $(1, 2, 3, 1, 2)$ |
| $L_{41} \cong \Gamma_{71}$ | $14 + 24 + 15 + 35$ | $(1, 1, 1, 2, 2)$ |
| $L_{42} \cong \Gamma_{53}$ | $13 + 23 + 14 + 24 + 15 + 345$ | $(1, 2, 2, 2, 2)$ |
| $L_{43} \cong \Gamma_{116}$ | $123 + 24 + 134 + 125 + 135$ | $(2, 1, 1, 1, 1)$ |
| $L_{44} \cong \Gamma_{57}$ | $12 + 13 + 14 + 234 + 235 + 245$ | $(1, 2, 2, 2, 1)$ |
| $L_{45} \cong \Gamma_{80}$ | $12 + 14 + 234 + 35 + 245$ | $(1, 2, 1, 2, 1)$ |
| $L_{46} \cong \Gamma_{126}$ | $12 + 134 + 235$ | $(2, 1, 2, 1, 1)$ |
| $L_{47} \cong \Gamma_{148}$ | $123 + 124 + 134 + 125 + 235 + 245 + 345$ | $(1, 1, 2, 2, 1)$ |
| $L_{48} \cong \Gamma_{112}$ | $12 + 134 + 234 + 135 + 145$ | $(1, 2, 2, 2, 1)$ |
| $L_{49} \cong \Gamma_{71}$ | $12 + 13 + 24 + 35$ | $(2, 1, 1, 1, 1)$ |
| $L_{50} \cong \Gamma_{151}$ | $123 + 124 + 234 + 135 + 235 + 145$ | $(1, 2, 2, 2, 1)$ |
| $L_{51} \cong \Gamma_{56}$ | $12 + 23 + 134 + 25 + 135$ | $(2, 1, 2, 1, 2)$ |
| $L_{52} \cong \Gamma_{52}$ | $12 + 13 + 24 + 25 + 145$ | $(1, 2, 1, 1, 1)$ |
| $L_{53} \cong \Gamma_{81}$ | $12 + 13 + 234 + 235 + 145$ | $(1, 2, 2, 1, 1)$ |

*Label convention.* Component labels index labelled realizations, not isomorphism classes. Thus $L_{41}$ and $L_{49}$ are both isomorphic to $\Gamma_{71}$ but have different labelled antichains and contribution vectors.

### 4.2 Group-characterizable components

Let $G$ be a finite group with dealer subgroup $G_0$ and participant subgroups $G_1, \ldots, G_5$. Choose $g \in G$ uniformly and define $(X_0, X_1, \ldots, X_5) = (gG_0, gG_1, \ldots, gG_5)$; this coset random vector is the associated group-characterizable SSS [40, 41]. Put $G_A = \bigcap_{i \in A} G_i$, with $G_\varnothing = G$. Then

$$\Phi_{N_j}(A) = \frac{\log\left(\dfrac{|G|\,|G_0 \cap G_A|}{|G_0|\,|G_A|}\right)}{\log(|G|/|G_0|)}, \qquad c_i = \frac{\log(|G|/|G_i|)}{\log(|G|/|G_0|)}. \tag{5}$$

The main groups and all subgroup generators and orders are given in Tables 3 to 5; these data determine the access function and contribution vector of each group-characterizable scheme. Appendix B.1 gives the contribution vectors and simpler index profiles from which the access functions can be computed.

Let $\mathrm{S}_m$ denote the symmetric group on $\{1, \ldots, m\}$, where $m = 5$ or 6 as indicated in the tables; permutations are composed from right to left. Each table gives the main group $G$, the dealer subgroup $G_0$, and the five participant subgroups by explicit generators.

Table 3: Group systems $N_1$, $N_2$, $N_3$.

| used for subgroup | $N_1$ $\Gamma^*_{82}$ generators | order | $N_2$ $\Gamma_{82}, \Gamma_{88}$ generators | order | $N_3$ $\Gamma_{30}$ maximum ratio generators | order |
|---|---|---|---|---|---|---|
| $G$ | $S_5$ | 120 | $S_5$ | 120 | $S_6$ | 720 |
| $G_0$ | $\langle(1\,2\,3\,5\,4), (2\,3\,4\,5)\rangle$ | 20 | $\langle(1\,2\,3\,5\,4), (2\,3\,4\,5)\rangle$ | 20 | $\langle(1\,4)(5\,6), (1\,5)(4\,6)\rangle$ | 4 |
| $G_1$ | $\langle(1\,2)(3\,4\,5), (2\,3)\rangle$ | 120 | $\langle(1\,2)(3\,4\,5), (2\,3)\rangle$ | 120 | $\langle(1\,2)(3\,5\,6), (2\,3)\rangle$ | 120 |
| $G_2$ | $\langle(2\,3\,4\,5), (3\,5)\rangle$ | 8 | $\langle(2\,3\,4\,5), (3\,5)\rangle$ | 8 | $\langle(4\,5\,6), (1\,4)(5\,6)\rangle$ | 12 |
| $G_3$ | $\langle(1\,2\,3\,4), (2\,4)\rangle$ | 8 | $\langle(1\,2\,3), (2\,3)(4\,5)\rangle$ | 6 | $\langle(1\,2\,3\,6\,4\,5), (3\,4\,6\,5)\rangle$ | 120 |
| $G_4$ | $\langle(1\,4\,5), (2\,3)(4\,5)\rangle$ | 6 | $\langle(1\,2\,5\,4), (2\,4)\rangle$ | 8 | $\langle(1\,2\,3\,5\,4\,6), (3\,4\,5\,6)\rangle$ | 120 |
| $G_5$ | $\langle(1\,2\,3\,4\,5), (3\,4\,5)\rangle$ | 60 | $\langle(1\,2\,3\,4\,5), (3\,4\,5)\rangle$ | 60 | $\langle(1\,2\,5\,3\,6\,4), (2\,3\,4)\rangle$ | 18 |

Table 4: Group systems $N_4$, $N_5$.

| used for subgroup | $N_4$ $\Gamma_{53}$ generators | order | $N_5$ $\Gamma_{30}$ regional generators | order |
|---|---|---|---|---|
| $G$ | $S_6$ | 720 | $S_6$ | 720 |
| $G_0$ | $\langle(2\,5), (1\,3)(4\,6), (1\,4)(3\,6)\rangle$ | 8 | $\langle(1\,4)(5\,6), (1\,5)(4\,6)\rangle$ | 4 |
| $G_1$ | $\langle(2\,3\,4\,5\,6), (1\,2)(5\,6)\rangle$ | 360 | $\langle(1\,2)(3\,5\,6), (2\,3)\rangle$ | 120 |
| $G_2$ | $\langle(2\,5\,6)(3\,4), (1\,3)(5\,6)\rangle$ | 36 | $\langle(4\,5\,6), (1\,4)(5\,6)\rangle$ | 12 |
| $G_3$ | $\langle(1\,3)(4\,5\,6), (3\,4)\rangle$ | 120 | $\langle(1\,2\,3\,6\,4\,5), (3\,4\,6\,5)\rangle$ | 120 |
| $G_4$ | $\langle(2\,6)(3\,4\,5), (1\,3)\rangle$ | 48 | $\langle(1\,2\,3\,5\,4\,6), (3\,4\,5\,6)\rangle$ | 120 |
| $G_5$ | $\langle(2\,3)(4\,5\,6), (1\,2)(3\,4)\rangle$ | 720 | $\langle(1\,2\,5\,4\,6\,3), (3\,4)(5\,6)\rangle$ | 36 |

Table 5: Group system $N_6$.

| used for subgroup | $\Gamma_{30}$ maximum ratio generators | order |
|---|---|---|
| $G$ | $S_6$ | 720 |
| $G_0$ | $\langle(1\,4)(5\,6), (1\,5)(4\,6)\rangle$ | 4 |
| $G_1$ | $\langle(1\,2)(3\,5\,6), (2\,3)\rangle$ | 120 |
| $G_2$ | $\langle(4\,5\,6), (1\,4)(5\,6)\rangle$ | 12 |
| $G_3$ | $\langle(1\,2\,3\,6\,4\,5), (3\,4\,6\,5)\rangle$ | 120 |
| $G_4$ | $\langle(1\,2\,3\,5\,4\,6), (3\,4\,5\,6)\rangle$ | 120 |
| $G_5$ | $\langle(1\,4\,2\,5\,3\,6), (2\,3)(5\,6)\rangle$ | 36 |

### 4.3 Explicit finite probability mass functions

For a finite joint PMF on $(X_0, X_1, \ldots, X_5)$, marginalization gives

$$\Phi_{D_j}(A) = \frac{I(X_0; X_A)}{H(X_0)} = \frac{H(X_0) + H(X_A) - H(X_0, X_A)}{H(X_0)}, \qquad c_i = \frac{H(X_i)}{H(X_0)}. \tag{6}$$

The laws $D_1, \ldots, D_9$ are listed in Table 6; $D_{10}$ is obtained from $D_9$ by swapping participants 2 and 3, and participants 4 and 5. Writing $\eta_j = H_{D_j}(X_0)$, their secret entropies are

$$\begin{aligned} &\eta_1 = \eta_2 = \eta_6 = 1, && \eta_3 = 1.577890091\ldots, && \eta_4 = 1.490764802\ldots, \\ &\eta_5 = 2.111132932\ldots, && \eta_7 = 0.365923651\ldots, && \eta_8 = 0.141440543\ldots, \\ &\eta_9 = \eta_{10} = 1.671246146\ldots. \end{aligned}$$

The corresponding 32 values of $\eta_j \Phi_{D_j}(A) = I_{D_j}(X_0; X_A)$ are given in Appendix B.2.

Table 6: Exact rational laws $D_1, \ldots, D_9$. For each support point, its probability is the displayed integer mass times the stated normalization factor.

probability mass functions

$D_1$; used for $\Gamma^*_{53}, \Gamma^*_{30}$; normalization 1/12.

| support point $(X_0, \ldots, X_5)$ | mass |
|---|---|
| $(0,1,0,1,1,0)$ | 2 |
| $(0,0,0,0,0,0)$ | 2 |
| $(0,0,0,0,1,1)$ | 1 |
| $(0,0,0,1,0,1)$ | 1 |
| $(1,0,0,1,1,1)$ | 2 |
| $(1,1,0,0,0,1)$ | 2 |
| $(1,1,0,1,0,0)$ | 1 |
| $(1,1,0,0,1,0)$ | 1 |

$D_2$; used for $\Gamma_{75}$; normalization 1/200.

| support point $(X_0, \ldots, X_5)$ | mass |
|---|---|
| $(0,1,1,1,1,0)$ | 75 |
| $(0,1,1,0,1,1)$ | 25 |
| $(1,1,0,0,1,1)$ | 80 |
| $(1,1,2,0,1,1)$ | 12 |
| $(1,1,1,0,0,0)$ | 8 |

$D_3$; used for $\Gamma_{28}$; normalization 1/10000.

| support point $(X_0, \ldots, X_5)$ | mass |
|---|---|
| $(0,0,0,0,0,0)$ | 295 |
| $(1,0,0,1,1,0)$ | 1344 |
| $(2,0,1,1,0,0)$ | 279 |
| $(1,0,1,0,0,0)$ | 1164 |
| $(1,0,0,1,0,1)$ | 1296 |
| $(0,0,0,0,0,1)$ | 2830 |
| $(2,0,1,1,1,0)$ | 2792 |

$D_4$; used for $\Gamma_{40}$; normalization 1/10000.

| support point $(X_0, \ldots, X_5)$ | mass |
|---|---|
| $(0,0,0,0,0,0)$ | 4154 |
| $(1,1,0,1,1,1)$ | 559 |
| $(2,2,0,1,1,1)$ | 560 |
| $(1,2,0,0,0,1)$ | 1901 |
| $(2,1,0,0,0,1)$ | 1890 |
| $(0,0,0,0,1,1)$ | 936 |

$D_5$; used for $\Gamma^*_{40}$; normalization 1/1000.

| support point $(X_0, \ldots, X_5)$ | mass |
|---|---|
| $(1,0,3,2,2,4)$ | 76 |
| $(2,0,3,4,0,2)$ | 224 |
| $(0,2,3,1,1,3)$ | 73 |
| $(0,4,3,1,0,2)$ | 83 |
| $(2,4,3,4,2,4)$ | 26 |
| $(3,2,3,3,2,4)$ | 105 |
| $(4,0,3,0,1,3)$ | 54 |
| $(2,4,3,3,2,3)$ | 11 |
| $(4,4,3,1,1,2)$ | 14 |
| $(0,4,3,0,1,2)$ | 16 |
| $(3,4,3,2,2,3)$ | 8 |
| $(4,2,3,1,0,2)$ | 307 |
| $(4,0,3,4,2,3)$ | 3 |

$D_6$; used for $\Gamma^*_{76}$; normalization 1/1000.

| support point $(X_0, \ldots, X_5)$ | mass |
|---|---|
| $(0,1,0,1,1,0)$ | 100 |
| $(1,1,0,1,0,1)$ | 100 |
| $(0,0,0,0,0,0)$ | 218 |
| $(1,0,0,0,1,1)$ | 218 |
| $(0,0,0,1,0,1)$ | 145 |
| $(1,1,0,0,1,0)$ | 37 |
| $(0,1,0,0,0,1)$ | 37 |
| $(1,0,0,1,1,0)$ | 145 |

Table 6 (continued)

probability mass functions

$D_7$; used for $\Gamma_{76}$; normalization 1/100.

| support point $(X_0, \ldots, X_5)$ | mass |
|---|---|
| $(0,0,0,0,0,0)$ | 56 |
| $(0,0,0,0,1,1)$ | 37 |
| $(1,1,0,0,1,1)$ | 6 |
| $(1,0,0,1,1,0)$ | 1 |

$D_8$; used for $\Gamma^*_{75}$; normalization 1/100.

| support point $(X_0, \ldots, X_5)$ | mass |
|---|---|
| $(0,0,0,0,0,0)$ | 84 |
| $(0,0,0,1,0,1)$ | 12 |
| $(0,1,0,0,0,1)$ | 2 |
| $(1,1,0,1,0,1)$ | 1 |
| $(1,1,0,0,1,0)$ | 1 |

$D_9$; used for $\Gamma^*_{28}$; normalization 1/10000.

| support point $(X_0, \ldots, X_5)$ | mass |
|---|---|
| $(1,3,0,1,3,2)$ | 295 |
| $(2,3,0,2,3,2)$ | 2003 |
| $(3,3,0,4,1,1)$ | 1458 |
| $(1,3,0,1,0,1)$ | 238 |
| $(3,3,0,4,3,2)$ | 1859 |
| $(3,3,3,1,0,1)$ | 254 |
| $(2,3,3,4,1,1)$ | 1535 |
| $(1,3,0,1,3,1)$ | 19 |
| $(3,3,0,1,3,1)$ | 164 |
| $(2,3,0,4,3,1)$ | 838 |
| $(0,3,3,2,3,1)$ | 1337 |

## 5 Fifteen regional separations

Each $\delta$-decomposition forms $\Psi = \sum_j h_j \Phi_j$, evaluates it on all 32 coalitions, and sets $L = \min_{A \in \Gamma} \Psi(A)$, $W = \max_{B \notin \Gamma} \Psi(B)$, and $\delta = L - W$. The aggregate contribution is divided by $\delta$ as in Theorem 2.7. The component data are exact, and all logarithms and entropies are evaluated in bits using outward-directed interval arithmetic. Each displayed strict margin exceeds its rounding interval. Summary tables display six decimal places; individual $\delta$-decompositions display additional digits to expose the rounding margin. The definition allows $\delta > 1$ because $\Psi$ need not be $[0,1]$-valued.

The CI-sensitive facets of all seventeen exceptional structures are listed in Table 14. For each of the fifteen separated structures, Table 7 selects one such facet and gives a certified upper bound on its left-hand side at our statistical construction.

Table 7: Selected facet-defining inequalities of the exact linear contribution regions and certified upper bounds on their left-hand sides at the statistical constructions. The displayed bounds are outward-rounded to six decimal places.

| structure | selected facet of $\Sigma_{\mathrm{lin}}(\Gamma)$ | certified LHS upper bound | construction |
|---|---|---|---|
| $\Gamma_{28}$ | $4c_1 + c_2 + c_3 \geq 9$ | $< 8.976995$ | Section 5.1 |
| $\Gamma^*_{28}$ | $4c_1 + c_2 + c_3 \geq 9$ | $< 8.943379$ | Section 5.2 |
| $\Gamma_{30}$ | $c_1 + c_2 + c_3 \geq 5$ | $< 4.942727$ | Section 5.3 |
| $\Gamma^*_{30}$ | $c_1 + c_2 + c_4 \geq 5$ | $< 4.915103$ | Tables 8 and 9 |
| $\Gamma_{40}$ | $c_1 + 3c_2 + c_3 \geq 8$ | $< 7.990980$ | Tables 8 and 9 |
| $\Gamma^*_{40}$ | $c_1 + 2c_2 + c_5 \geq 6$ | $< 5.997642$ | Tables 8 and 9 |
| $\Gamma_{53}$ | $c_1 + c_3 + c_5 \geq 5$ | $< 4.984154$ | Tables 8 and 9 |
| $\Gamma^*_{53}$ | $c_1 + c_2 + c_4 \geq 5$ | $< 4.886689$ | Tables 8 and 9 |
| $\Gamma_{75}$ | $2c_1 + c_4 \geq 4$ | $< 3.952201$ | Tables 8 and 9 |
| $\Gamma^*_{75}$ | $2c_2 + c_4 \geq 4$ | $< 3.971466$ | Tables 8 and 9 |
| $\Gamma_{76}$ | $c_1 + 2c_2 + c_3 \geq 6$ | $< 5.978827$ | Tables 8 and 9 |
| $\Gamma^*_{76}$ | $c_1 + 2c_2 + c_4 \geq 6$ | $< 5.996898$ | Tables 8 and 9 |
| $\Gamma_{82}$ | $2c_1 + c_5 \geq 4$ | $< 3.869110$ | Tables 8 and 9 |
| $\Gamma^*_{82}$ | $2c_1 + c_5 \geq 4$ | $< 3.839732$ | Tables 8 and 9 |
| $\Gamma_{88}$ | $2c_1 + c_5 \geq 4$ | $< 3.738287$ | Tables 8 and 9 |

**Theorem 5.1** (Regional separations under statistical security)**.** *For every*

$$\begin{aligned}\Gamma \in \{&\Gamma_{28}, \Gamma^*_{28}, \Gamma_{30}, \Gamma^*_{30}, \Gamma_{40}, \Gamma^*_{40},\\ &\Gamma_{53}, \Gamma^*_{53}, \Gamma_{75}, \Gamma^*_{75}, \Gamma_{76}, \Gamma^*_{76},\\ &\Gamma_{82}, \Gamma^*_{82}, \Gamma_{88}\},\end{aligned}$$

*we have* $\Sigma_{\mathrm{stat}}(\Gamma) \not\subseteq \Sigma_{\mathrm{lin}}(\Gamma)$.

*Proof.* For each target $\Gamma$, Table 7 gives a facet-defining inequality

$$\ell_\Gamma(c) \geq b_\Gamma$$

of the exact linear contribution region and a contribution vector $c_\Gamma$ satisfying $\ell_\Gamma(c_\Gamma) < b_\Gamma$. The corresponding subsection or Tables 8 and 9 gives a $\delta$-decomposition producing $c_\Gamma$. By Theorem 2.7, $c_\Gamma \in \Sigma_{\mathrm{stat}}(\Gamma)$, while the strict facet violation gives $c_\Gamma \notin \Sigma_{\mathrm{lin}}(\Gamma)$. Hence $\Sigma_{\mathrm{lin}}(\Gamma) \subsetneq \Sigma_{\mathrm{stat}}(\Gamma)$. By Proposition 2.3, this is a separation between general and linear schemes under statistical security. □

### 5.1 $\Gamma_{28}$: six linear components and a seven-point joint PMF

Let $\Gamma_{28} = 12 + 13 + 23 + 14 + 24 + 15 + 35$, with facet $4c_1 + c_2 + c_3 \geq 9$. The reduced $\delta$-decomposition is

$$\begin{aligned}20{,}000\Psi_{28} = {}& 19{,}156\Phi_{L_1} + 76\Phi_{L_4} + 3{,}648\Phi_{L_{17}}\\ &+ 3{,}171\Phi_{L_{35}} + 56\Phi_{L_{39}} + 4{,}166\Phi_{L_{41}}\\ &+ 26{,}002\eta_3\Phi_{D_3}.\end{aligned} \tag{7}$$

The qualified minimizer is `35`, while the forbidden maximizer is `1`. Outward-directed interval evaluation gives

$$\delta > 0.9999818434$$

and

$$c = \big(1.3274741\ldots, 1.8329433\ldots, 1.8341553\ldots,\\ 2.0323426\ldots, 2.0344840\ldots\big).$$

Moreover, $4c_1 + c_2 + c_3 < 8.9769949880 < 9$. Thus the certified separation margin exceeds 0.023.

### 5.2 $\Gamma^*_{28}$: eight linear components and two eleven-point joint PMFs

Let $\Gamma^*_{28} = 123 + 124 + 135 + 2345$, whose exact linear region has the facet $4c_1 + c_2 + c_3 \geq 9$. This facet is the dual, after the canonical relabelling, of the corresponding $\Gamma_{28}$ facet. With $D_{10}$ the relabelled copy of $D_9$ defined in Section 4.3, take

$$\begin{aligned} 50{,}000\Psi^*_{28} = {} & 30{,}156\Phi_{L_1} + 8{,}459\Phi_{L_2} + 5{,}275\Phi_{L_3} \\ & + 5{,}275\Phi_{L_4} + 8{,}459\Phi_{L_9} + 6{,}922\Phi_{L_{30}} \\ & + 13{,}836\Phi_{L_{36}} + 8{,}459\Phi_{L_{39}} + 23{,}438\eta_9\Phi_{D_9} \\ & + 23{,}438\eta_{10}\Phi_{D_{10}}. \end{aligned} \tag{8}$$

The qualified minimizers are `124` and `135`, while the forbidden maximizers are `134` and `125`. Outward-directed interval evaluation gives

$$\delta > 0.9999946748$$

and

$$c = \big(1.3566472\ldots, 1.7583946\ldots, 1.7583946\ldots,\\ 1.9149795\ldots, 1.9149795\ldots\big).$$

Moreover, $4c_1 + c_2 + c_3 < 8.9433781972 < 9$, a certified margin exceeding 0.056.

### 5.3 $\Gamma_{30}$: six linear components and one group system

Let $\Gamma_{30} = 12 + 13 + 23 + 14 + 24 + 15 + 345$, with facet $c_1 + c_2 + c_3 \geq 5$. The reduced seven-term $\delta$-decomposition is

$$\begin{aligned} 30{,}000\Psi_{30} = {} & 23{,}457\Phi_{L_1} + 11{,}365\Phi_{L_2} + 12{,}226\Phi_{L_9} \\ & + 861\Phi_{L_{20}} + 861\Phi_{L_{22}} + 7{,}404\Phi_{L_{23}} \\ & + 49{,}020\Phi_{N_5}. \end{aligned}$$

The qualified minimizer is `23`, while the forbidden maximizer is `35`. Outward-directed interval evaluation of the single group profile gives

$$\delta > 0.9999931645$$

and

$$c = \big(1.7819351\ldots, 1.5351245\ldots, 1.6256674\ldots,\\ 1.6256674\ldots, 1.3788708\ldots\big).$$

Moreover, $c_1 + c_2 + c_3 < 4.9427269502 < 5$, a certified margin exceeding 0.057.

### 5.4 The remaining twelve separations

For the remaining twelve access structures, the integer $\delta$-decompositions are given in Table 8, and their outward-directed verification is reported in Table 9.

Table 8: Integer $\delta$-decompositions for the twelve tabulated regional separations. Each row defines $\Psi_\Gamma$ by $10^4 s_\Gamma \Psi_\Gamma = \sum_j m_j \Phi_j$.

| target | $s_\Gamma$ | integer numerator $\sum_j m_j \Phi_j$ |
|---|---|---|
| $\Gamma_{30}^*$ | 3 | $30{,}000\Phi_{L_1} + 23{,}113\Phi_{L_3} + 8{,}113\Phi_{L_4} + 3{,}113\Phi_{L_7} + 6{,}887\Phi_{L_{12}} + 8{,}113\Phi_{L_{14}} + 8{,}113\Phi_{L_{22}} + 3{,}774\Phi_{L_{23}} + 11{,}226\Phi_{L_{28}} + 15{,}000\eta_1\Phi_{D_1}$ |
| $\Gamma_{40}$ | 2 | $2{,}579\Phi_{L_2} + 8{,}182\Phi_{L_3} + 9{,}178\Phi_{L_4} + 1{,}171\Phi_{L_6} + 7{,}199\Phi_{L_8} + 4{,}620\Phi_{L_{11}} + 6{,}600\Phi_{L_{13}} + 628\Phi_{L_{15}} + 2{,}414\Phi_{L_{19}} + 14{,}661\eta_4\Phi_{D_4}$ |
| $\Gamma_{40}^*$ | 5 | $12{,}734\Phi_{L_1} + 7{,}264\Phi_{L_3} + 133\Phi_{L_4} + 11{,}966\Phi_{L_{12}} + 3{,}781\Phi_{L_{20}} + 2{,}211\Phi_{L_{21}} + 15{,}732\Phi_{L_{24}} + 15{,}107\Phi_{L_{46}} + 16{,}114\Phi_{L_{47}} + 14{,}479\eta_5\Phi_{D_5}$ |
| $\Gamma_{53}$ | 1 | $1{,}560\Phi_{L_4} + 7{,}274\Phi_{L_6} + 2{,}274\Phi_{L_7} + 3{,}572\Phi_{L_{12}} + 1{,}720\Phi_{L_{15}} + 1{,}560\Phi_{L_{16}} + 5{,}000\Phi_{L_{45}} + 11{,}166\Phi_{N_4}$ |
| $\Gamma_{53}^*$ | 2 | $1{,}092\Phi_{L_4} + 8{,}908\Phi_{L_7} + 13{,}864\Phi_{L_{10}} + 3{,}864\Phi_{L_{14}} + 2{,}772\Phi_{L_{20}} + 3{,}864\Phi_{L_{22}} + 10{,}000\Phi_{L_{28}} + 13{,}362\eta_1\Phi_{D_1}$ |
| $\Gamma_{75}$ | 2 | $8{,}638\Phi_{L_1} + 256\Phi_{L_7} + 4{,}700\Phi_{L_9} + 5{,}810\Phi_{L_{16}} + 5{,}810\Phi_{L_{25}} + 5{,}858\Phi_{L_{40}} + 5{,}810\Phi_{L_{52}} + 19{,}142\eta_2\Phi_{D_2}$ |
| $\Gamma_{75}^*$ | 2 | $8{,}882\Phi_{L_3} + 400\Phi_{L_6} + 1{,}004\Phi_{L_{19}} + 4{,}348\Phi_{L_{34}} + 1{,}422\Phi_{L_{43}} + 9{,}092\Phi_{L_{51}} + 186{,}520\eta_8\Phi_{D_8}$ |
| $\Gamma_{76}$ | 2 | $4{,}542\Phi_{L_3} + 142\Phi_{L_4} + 260\Phi_{L_{20}} + 6{,}742\Phi_{L_{26}} + 3{,}844\Phi_{L_{27}} + 4{,}104\Phi_{L_{29}} + 8{,}717\Phi_{L_{33}} + 1{,}348\Phi_{L_{38}} + 3{,}844\Phi_{L_{49}} + 43{,}970\eta_7\Phi_{D_7}$ |
| $\Gamma_{76}^*$ | 2 | $3{,}267\Phi_{L_1} + 2{,}451\Phi_{L_3} + 7{,}154\Phi_{L_{18}} + 5{,}668\Phi_{L_{19}} + 965\Phi_{L_{22}} + 554\Phi_{L_{27}} + 7{,}112\Phi_{L_{31}} + 4{,}703\Phi_{L_{34}} + 5{,}734\Phi_{L_{43}} + 8{,}044\eta_6\Phi_{D_6}$ |
| $\Gamma_{82}$ | 2 | $3{,}691\Phi_{L_7} + 3{,}691\Phi_{L_{32}} + 10{,}000\Phi_{L_{44}} + 10{,}000\Phi_{L_{53}} + 16{,}309\Phi_{N_2}$ |
| $\Gamma_{82}^*$ | 2 | $4{,}526\Phi_{L_1} + 4{,}526\Phi_{L_8} + 7{,}738\Phi_{L_{48}} + 4{,}526\Phi_{L_{50}} + 7{,}738\Phi_{L_{53}} + 20{,}000\Phi_{N_1}$ |
| $\Gamma_{88}$ | 2 | $20{,}000\Phi_{L_1} + 7{,}382\Phi_{L_7} + 7{,}382\Phi_{L_{32}} + 32{,}618\Phi_{N_2}$ |

Table 9: Outward-directed verification of the twelve tabulated $\delta$-decompositions. The value $\delta$ may exceed 1 because $\Psi$ need not be $[0,1]$-valued.

| target | $A_{\min}$ | $B_{\max}$ | $\delta$ |
|---|---|---|---|
| $\Gamma_{30}^*$ | 123 | 234 | $> 0.9999927081$ |
| $\Gamma_{40}$ | 23 | 24 | $> 0.9999712188$ |
| $\Gamma_{40}^*$ | 235 | 145 | $> 0.9999849704$ |
| $\Gamma_{53}$ | 25 | 1 | $> 0.9999720856$ |
| $\Gamma_{53}^*$ | 134 | 34 | $> 0.9998999999$ |
| $\Gamma_{75}$ | 24 | 15 | $> 1.0000498409$ |
| $\Gamma_{75}^*$ | 12 | 24 | $> 0.9999777143$ |
| $\Gamma_{76}$ | 12 | 23 | $> 0.9999639454$ |
| $\Gamma_{76}^*$ | 125 | 24 | $> 0.9999457005$ |
| $\Gamma_{82}$ | 12 | 2 | $= 1$ |
| $\Gamma_{82}^*$ | 235 | 13 | $> 1.0000056144$ |
| $\Gamma_{88}$ | 12 | 15 | $> 0.9999817566$ |

Here $A_{\min}$ is a qualified minimizer and $B_{\max}$ a forbidden maximizer. The selected facets and their construction bounds are reported in Table 7. For $\Gamma_{82}$ the gap is exactly $\delta = 1$.

## 6 Two-sided maximum-ratio bounds for $\Gamma_{30}$

The separations of Section 5 are regional and need not improve a standard scalar optimum. For $\Gamma_{30}$ we obtain both a non-Shannon lower bound and a statistical construction, giving a two-sided interval for the maximum information ratio. For an access structure $\Gamma$ on five participants, define

$$\sigma_{\mathrm{stat}}^{\max}(\Gamma) := \inf_{c \in \Sigma_{\mathrm{stat}}(\Gamma)} \max_{1 \le i \le 5} c_i,$$
$$\sigma_{\mathrm{lin}}^{\max}(\Gamma) := \inf_{c \in \Sigma_{\mathrm{lin}}(\Gamma)} \max_{1 \le i \le 5} c_i,$$

and

$$\sigma_{\mathrm{stat}}^{\mathrm{av}}(\Gamma) := \inf_{c \in \Sigma_{\mathrm{stat}}(\Gamma)} \frac{1}{5} \sum_{i=1}^{5} c_i,$$
$$\sigma_{\mathrm{lin}}^{\mathrm{av}}(\Gamma) := \inf_{c \in \Sigma_{\mathrm{lin}}(\Gamma)} \frac{1}{5} \sum_{i=1}^{5} c_i.$$

Thus $\sigma_{\mathrm{stat}}^{\max}$ and $\sigma_{\mathrm{stat}}^{\mathrm{av}}$ optimize over general schemes under statistical security, whereas $\sigma_{\mathrm{lin}}^{\max}$ and $\sigma_{\mathrm{lin}}^{\mathrm{av}}$ optimize over linear schemes under the same security notion. By Proposition 2.3, the latter two quantities are unchanged if perfect or partial security is used within the linear class. These infima are attained: after fixing any feasible vector, minimization may be restricted to a compact coordinate box because the contribution regions are closed and coordinatewise upward closed.

**Theorem 6.1** (Certified 14/9 lower bound)**.** *For* $\Gamma_{30} = 12 + 13 + 23 + 14 + 24 + 15 + 345$*,*

$$\sigma_{\mathrm{stat}}^{\max}(\Gamma_{30}) \geq \frac{14}{9}.$$

*Proof.* Normalize $H(X_0) = 1$. Following the Ahlswede–Körner extension framework [12] as used by Farràs et al. [10], for nonempty base subsets $A, B$ and a base subset $C$, let $W$ be an auxiliary variable satisfying

$$\begin{aligned} H(W \mid X_{A\cup B}) &= 0, \\ H(X_A \mid W) &= H(X_A \mid X_C), \\ H(X_B \mid W) &= H(X_B \mid X_C), \\ H(X_{A\cup B} \mid W) &= H(X_{A\cup B} \mid X_C). \end{aligned}$$

Use the record $(A, B, C) = (\{3\}, \{4\}, \{5\})$ and minimize

$$2H(X_1) + 3H(X_2) + 3H(X_3) + H(X_4)$$

over the extended Shannon cone and the access equalities of $\Gamma_{30}$. The reported exact optimum is 14, whereas the Shannon program without the AK extension has optimum 13.5. Hence

$$2H(X_1) + 3H(X_2) + 3H(X_3) + H(X_4) \geq 14H(X_0).$$

Since the coefficients of the share entropies sum to 9, the inequality gives $\max_i H(X_i)/H(X_0) \geq 14/9$. Direct minimization of $\max_i c_i$ over the same AK relaxation also gives 14/9, so the coefficient-sum step is lossless. □

**Theorem 6.2** (Statistical upper bound)**.**

$$\sigma_{\mathrm{stat}}^{\max}(\Gamma_{30}) < 1.6502 < \frac{5}{3} = \sigma_{\mathrm{lin}}^{\max}(\Gamma_{30}).$$

*Proof.* Consider the following ten-component $\delta$-decomposition. Clearing the common denominator $10^{10}$ gives the integer-scaled form

$$\begin{aligned} 10^{10}\Psi_{30}^{\max} = {} & 6{,}749{,}199{,}924\Phi_{L_1} + 3{,}003{,}200{,}305\Phi_{L_2} \\ & + 514{,}483{,}339\Phi_{L_4} + 514{,}483{,}339\Phi_{L_5} \\ & + 3{,}003{,}200{,}305\Phi_{L_9} + 1{,}615{,}758{,}140\Phi_{L_{23}} \\ & + 266{,}883{,}567\Phi_{L_{37}} + 1{,}615{,}758{,}140\Phi_{L_{42}} \\ & + 1{,}854{,}981{,}115\Phi_{N_3} + 12{,}249{,}493{,}991\Phi_{N_6}. \end{aligned}$$

All components are as in Section 4. The qualified minimizers are the coalitions 23, 24, 235, and 245, and the forbidden maximizers are 35 and 45. Outward-directed interval evaluation of the group-index logarithms gives the rigorous enclosures

$$0.99999999993345 < \delta < 0.99999999993346,$$

$$1.65016001534 < \max_i c_i < 1.65016001535 < 1.6502 < \frac{5}{3}.$$

The individual coordinates are

$$\begin{aligned} c = \big(&1.65016001534\ldots,\ 1.65016001523\ldots,\\ &1.65016001534\ldots,\ 1.65016001534\ldots,\\ &1.48858420130\ldots\big). \end{aligned}$$

By Theorem 2.7, this contribution vector belongs to $\Sigma_{\mathrm{stat}}(\Gamma_{30})$, whence the stated bound on $\sigma^{\max}_{\mathrm{stat}}$. The linear value $5/3$ is established in [10]. □

## 7 Open cases and further questions

**Status of the open dual pair.** The unresolved pair is

$$\begin{aligned} \Gamma_{73} &= 12 + 13 + 24 + 35 + 145,\\ \Gamma^*_{73} &= 123 + 124 + 134 + 125 + 235 + 345. \end{aligned}$$

For both structures, the exact linear region has the unique CI-sensitive facet $c_1 + c_2 + c_3 \geq 5$ [7]. We use the following copy convention. A new block that copies $Y$ over $Z$ has the same joint entropy profile with $Z$ as $Y$ and is conditionally independent of all previously introduced variables outside $Z$, given $Z$.

For $\Gamma_{73}$, introduce five successive auxiliaries: $U_1$ copies $X_{02}$ over $X_{14}$; $V_1$ copies $X_{03}$ over $X_{15}$; $U_2$ copies $U_1$ over $X_{15}$; $V_2$ copies $V_1$ over $X_{14}$; and $V_3$ copies $V_2$ over $X_{15}$. Optimizing the Shannon program with these copy equalities gives

$$17\big(H(X_1) + H(X_2) + H(X_3)\big) \geq 75H(X_0),$$

hence $c_1 + c_2 + c_3 \geq 75/17$. The successive exact optima found along this route are

$$\frac{13}{3},\quad \frac{57}{13},\quad \frac{22}{5},\quad \frac{75}{17}.$$

For $\Gamma^*_{73}$, let $A = (A_4, A_5)$ copy $(X_4, X_5)$ over $X_{0123}$; let $B = (B_0, B_1)$ copy $(X_0, X_1)$ over $(X_{234}, A_4)$; and let $C = (C_0, C_2)$ copy $(X_0, X_2)$ over $(X_{135}, A_5)$, with the $B$ and $C$ copy conditions imposed simultaneously. The resulting program gives

$$5\big(H(X_1) + H(X_2) + H(X_3)\big) \geq 22H(X_0),$$

hence $c_1 + c_2 + c_3 \geq 22/5$.

The remaining gaps to the linear value 5 are $10/17$ and $3/5$. Extensive searches have not produced a partial scheme violating the facet. The increasing copy bounds above suggest that more elaborate copy systems might approach 5 for either structure, although the present finite sequences do not imply convergence and natural continuations can plateau. A construction below 5 would separate the corresponding regions, while an almost-entropic proof of 5 would establish equality.

**Dual separation.** Information inequalities are not closed under polymatroid duality [42]. Csirmaz constructed an almost-perfect ideal scheme on 174 participants whose complexity is strictly smaller than that of its dual [43]. Almost-perfect and statistical security have

the same asymptotic contribution region [32], so this is also a statistical duality separation. The smallest access structure satisfying $\Sigma_{\mathrm{stat}}(\Gamma) \neq \Sigma_{\mathrm{stat}}(\Gamma^*)$ remains unknown and may already occur among the eight non-self-dual exceptional classes studied here. Our searches have not yet produced a partial-scheme witness for such a separation among these classes. This should be viewed only as a limitation of the construction families tested here, not as evidence that no such witness exists. A dual separation among these small exceptional classes remains quite plausible and may require a different construction paradigm.

**Algebraic separations.** By Proposition 3.1, all linear realizations used on at most five participants are characteristic-universal, and hence the resulting linear regions are characteristic-independent. Allowing direct sums over different characteristics therefore does not enlarge them. Homomorphic and Abelian schemes satisfy the common-information property [34, Proposition 6.2 and Corollary 6.3], while $K^{\text{one-CI}}(\Gamma) = \Sigma_{\mathrm{lin}}(\Gamma)$ for every exceptional structure. As already observed for the homomorphic class in [34, Section 6.2], it follows that no access structure on at most five participants separates linear, mixed-characteristic linear, homomorphic, or Abelian schemes. Six participants are the next natural range.

**Scalar status.** Table 10 collects the best established maximum and average statistical information ratios. A regional separation need not move either optimized scalar ratio.

Table 10: Status and best established statistical maximum and average information ratios for the seventeen exceptional structures. A singleton is an exact value; a bracketed entry is the current interval. Linear schemes give the stated upper bounds, while the entropy inequalities in the cited sources give the lower bounds. A regional separation need not change either optimized scalar ratio, so exact singleton entries are compatible with the status "separated."

| class | minimal qualified sets | status | $\sigma^{\max}_{\mathrm{stat}}$ | $\sigma^{\mathrm{av}}_{\mathrm{stat}}$ | references |
|---|---|---|---|---|---|
| $\Gamma_{28}$ | $12+13+23+14+24+15+35$ | separated | 3/2 | 7/5 | [10, 14] |
| $\Gamma^*_{28}$ | $123+124+135+2345$ | separated | 3/2 | 7/5 | [10, 14] |
| $\Gamma_{30}$ | $12+13+23+14+24+15+345$ | separated | [14/9, 1.6502) | 7/5 | Theorems 6.1 and 6.2; [10] |
| $\Gamma^*_{30}$ | $123+124+134+125+2345$ | separated | [3/2, 5/3] | 7/5 | [10] |
| $\Gamma_{40}$ | $12+13+23+14+25+345$ | separated | [14/9, 5/3] | 7/5 | [10] |
| $\Gamma^*_{40}$ | $123+124+134+125+235$ | separated | [3/2, 5/3] | 7/5 | [10] |
| $\Gamma_{53}$ | $12+13+14+234+25+35$ | separated | [14/9, 5/3] | 3/2 | [10] |
| $\Gamma^*_{53}$ | $123+124+134+125+345$ | separated | [3/2, 5/3] | 3/2 | [10] |
| $\Gamma_{73}$ | $12+13+24+35+145$ | open | [14/9, 5/3] | [53/35, 23/15] | [10] |
| $\Gamma^*_{73}$ | $123+124+134+125+235+345$ | open | [3/2, 5/3] | [3/2, 23/15] | [10] |
| $\Gamma_{75}$ | $12+13+24+235+145$ | separated | 3/2 | 7/5 | [10, 14] |
| $\Gamma^*_{75}$ | $12+134+234+135+245$ | separated | 3/2 | 7/5 | [10, 14] |
| $\Gamma_{76}$ | $12+13+24+235+145+345$ | separated | 3/2 | 7/5 | [10, 14] |
| $\Gamma^*_{76}$ | $123+124+134+234+125+135+245$ | separated | 3/2 | 7/5 | [10, 14] |
| $\Gamma_{82}$ | $12+13+234+235+145+245$ | separated | 3/2 | 13/10 | [10, 14] |
| $\Gamma^*_{82}$ | $12+134+234+135+235+145$ | separated | 3/2 | 13/10 | [10, 14] |
| $\Gamma_{88}$ | $12+13+234+145+245$ | separated | 3/2 | 7/5 | [10, 14] |

The two open-pair sum bounds do not improve the scalar intervals in Table 10; the sharpened $\Gamma_{30}$ interval follows from Theorems 6.1 and 6.2.

## 8 Conclusion

Five is the sharp participant threshold for a general-versus-linear regional separation under statistical security: among the 157 connected five-participant structures, 140 are Shannon-exact, seventeen have exact linear region $K^{\text{one-CI}}(\Gamma)$, and partial schemes yield such separations for fifteen of those seventeen structures. For $\Gamma_{30}$, we obtained $\sigma^{\max}_{\text{stat}}(\Gamma_{30}) \in [14/9, 1.6502)$, while the optimum for linear schemes is $5/3$.

The pair $\Gamma_{73}, \Gamma^*_{73}$ remains open, with copy-lemma bounds $75/17$ and $22/5$ toward the common linear facet value 5. As a working conjecture, we suspect that suitable sequences of valid copy extensions may converge to the facet value 5 for both structures; this is not implied by the finite sequences currently known.

We have also examined whether the statistical contribution region can differ from that of the dual access structure among the non-self-dual exceptional classes. The construction families tested here have not produced such a partial-scheme witness, but this negative outcome should not be interpreted as evidence against its existence. A duality separation on a small number of participants remains quite plausible and may require constructions different from those used for the regional separations in this paper.

The analogous general-versus-linear participant threshold under perfect security is also open: this paper gives a lower bound of five, while the known perfect example has twelve participants. These questions, together with the absence of algebraic-class separations on at most five participants, point naturally to the six-participant case.

## Supplementary Information

A self-contained verification package for the computer-assisted results is archived at Zenodo: `doi:10.5281/zenodo.21871834`. From the finite data used in the paper, the package reconstructs the group and finite-PMF components, checks the fifteen $\delta$-decompositions on all 32 coalitions, verifies the selected one-common-information inequalities used in the separations, checks the $\Gamma_{30}$ maximum-ratio construction and its exact Ahlswede–Körner lower-bound certificate, and verifies the copy-lemma bounds for $\Gamma_{73}$ and $\Gamma_{151}$. Rational identities are checked exactly; logarithmic and entropy calculations use outward-directed interval arithmetic.

## Statements and Declarations

**Competing interests.** The author declares no competing interests.

**Data availability.** The exact rational certificates, finite component data, and verification code used for the computer-assisted results are available in the supplementary verification package archived at Zenodo, `doi:10.5281/zenodo.21871834`. No additional research dataset is required.

**Use of generative AI.** The author used OpenAI ChatGPT and Anthropic Claude as generative-AI assistants. In Sections 4–7 and Appendices A–C, these tools were used for computational exploration, including searching for and checking $\delta$-decompositions, group- and PMF-based constructions, lower-bound computations, and related exact data.

They were also used in preparing LaTeX and auxiliary verification code. In Sections 1–8 and the appendices, the tools were used to assist with drafting, rewriting, and editorial revision of portions of the exposition. All mathematical claims, computational results, constructions, citations, and final text were independently reviewed by the author, who takes full responsibility for the content of the paper.

# A Connected access structures on at most five participants

For completeness, this appendix records, following Bahariyan [7], the nonideal connected four-participant and connected full-support five-participant access structures, together with the extreme points of their linear contribution regions.

For each listed access structure $\Gamma$, let $V_\Gamma$ denote the set of extreme contribution vectors displayed in the corresponding table. Then

$$\Sigma_{\mathrm{lin}}(\Gamma) = \mathrm{conv}(V_\Gamma) + \mathbb{R}^n_{\geq 0},$$

where $n$ is the number of participants and $\mathrm{conv}(V_\Gamma)$ denotes the convex hull of $V_\Gamma$.

## A.1 Connected structures on at most four participants

Every connected access structure on at most three participants is ideal. Up to participant relabelling, the four nonideal connected four-participant structures and the extreme-point descriptions of their linear contribution regions are given in Table 11. Together with the ideal cases, this records the Shannon-exact classification on at most four participants [26, 27, 10].

Table 11: The nonideal connected four-participant classes, up to participant relabelling, and the extreme points of their linear contribution regions. The middle two rows are dual; the first and last rows are self-dual up to relabelling.

| minimal qualified sets | duality status | $V_\Gamma$ |
|---|---|---|
| $12 + 13 + 24$ | self-dual | $(1,2,1,1),\ (2,1,1,1)$ |
| $12 + 13 + 23 + 14$ | dual of next row | $(1,2,2,1),\ (2,1,1,1)$ |
| $12 + 13 + 234$ | dual of previous row | $(1,2,2,1),\ (2,1,1,1)$ |
| $12 + 13 + 14 + 234$ | self-dual | $(1,2,2,2),\ (2,1,1,1)$ |

## A.2 Five-participant catalogue

The 157 connected full-support five-participant structures are represented by 95 rows: 62 connected dual pairs, 10 self-dual structures, and 23 connected structures whose dual is disconnected. Thus

$$2 \cdot 62 + 10 + 23 = 157.$$

The catalogue follows the Jackson–Martin numbering [14].

**The ideal classes.** Among the 157 connected structures, 42 are ideal. They are represented by the 33 rows of Table 12: nine connected dual pairs, five self-dual structures, and nineteen connected structures whose dual is disconnected. The final column records the connected dual partner, says "self-dual", or says "disconnected".

Table 12: Ideal connected five-participant structures, one row per connected dual pair, self-dual class, or connected class with disconnected dual.

| class | minimal qualified sets | dual |
|---|---|---|
| $\Gamma_{23}$ | $12+13+23+14+24+34+15+25+35$ | $\Gamma_{175}$ |
| $\Gamma_{24}$ | $12+13+23+14+24+34+15+25+35+45$ | $\Gamma_{179}$ |
| $\Gamma_{26}$ | $12+13+23+14+24+15+25$ | $\Gamma_{132}$ |
| $\Gamma_{29}$ | $12+13+23+14+24+15+35+45$ | $\Gamma_{172}$ |
| $\Gamma_{46}$ | $12+13+23+145+245$ | $\Gamma_{106}$ |
| $\Gamma_{47}$ | $12+13+23+145+245+345$ | $\Gamma_{135}$ |
| $\Gamma_{59}$ | $12+13+14+15$ | disconnected |
| $\Gamma_{63}$ | $12+13+14+25+35+45$ | disconnected |
| $\Gamma_{93}$ | $12+13+145$ | disconnected |
| $\Gamma_{95}$ | $12+13+145+245+345$ | self-dual |
| $\Gamma_{98}$ | $12+13+245+345$ | disconnected |
| $\Gamma_{102}$ | $12+34+135+235+145$ | $\Gamma_{115}$ |
| $\Gamma_{103}$ | $12+34+135+235+145+245$ | $\Gamma_{141}$ |
| $\Gamma_{104}$ | $12+34+135+245$ | self-dual |
| $\Gamma_{108}$ | $12+134+234+135+235+145+245$ | self-dual |
| $\Gamma_{109}$ | $12+134+234+135+235+145+245+345$ | $\Gamma_{137}$ |
| $\Gamma_{110}$ | $12+134+234+135+235+145+345$ | self-dual |
| $\Gamma_{118}$ | $12+134+135$ | disconnected |
| $\Gamma_{119}$ | $12+134+135+145$ | disconnected |
| $\Gamma_{131}$ | $12+1345$ | disconnected |
| $\Gamma_{138}$ | $123+124+134+234+125+135+235+145+245+345$ | self-dual |
| $\Gamma_{144}$ | $123+124+134+125+135$ | disconnected |
| $\Gamma_{145}$ | $123+124+134+125+135+145$ | disconnected |
| $\Gamma_{156}$ | $123+124+134+235+245+345$ | disconnected |
| $\Gamma_{158}$ | $123+124+125$ | disconnected |
| $\Gamma_{163}$ | $123+124+135+145$ | disconnected |
| $\Gamma_{171}$ | $123+145$ | disconnected |
| $\Gamma_{173}$ | $123+1245$ | disconnected |
| $\Gamma_{174}$ | $123+1245+1345$ | disconnected |
| $\Gamma_{176}$ | $1234+1235$ | disconnected |
| $\Gamma_{177}$ | $1234+1235+1245$ | disconnected |
| $\Gamma_{178}$ | $1234+1235+1245+1345$ | disconnected |
| $\Gamma_{180}$ | $12345$ | disconnected |

The ideal structures are omitted from Table 13, which records the 98 nonideal Shannon-exact connected structures in 53 rows: 45 connected dual pairs, four self-dual structures, and four connected structures whose dual is disconnected. The "dual" column uses the same convention as Table 12.

Table 13: The nonideal Shannon-exact connected five-participant access structures, one row per connected dual pair, self-dual class, or connected class with disconnected dual, together with the extreme points of their linear contribution regions.

| class | dual | minimal qualified sets | extreme points of $\Sigma_{\text{lin}}$ |
|---|---|---|---|
| $\Gamma_{21}$ | $\Gamma_{157}$ | $12+13+23+14+24+34+15$ | $(1,2,2,2,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{22}$ | $\Gamma_{170}$ | $12+13+23+14+24+34+15+25$ | $(1,1,2,2,1)$, $(2,2,1,1,1)$ |
| $\Gamma_{25}$ | $\Gamma_{129}$ | $12+13+23+14+24+15$ | $(1,2,2,2,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{27}$ | $\Gamma_{161}$ | $12+13+23+14+24+15+25+345$ | $(1,1,2,2,2)$, $(2,2,1,1,1)$ |
| $\Gamma_{31}$ | $\Gamma_{154}$ | $12+13+23+14+24+35$ | $(1,1,2,1,1)$, $(2,2,1,1,1)$ |
| $\Gamma_{32}$ | $\Gamma_{168}$ | $12+13+23+14+24+35+45$ | $(1,1,2,2,1)$, $(2,2,1,1,1)$ |
| $\Gamma_{33}$ | $\Gamma_{133}$ | $12+13+23+14+24+345$ | $(1,1,2,2,1)$, $(2,2,1,1,1)$ |
| $\Gamma_{34}$ | $\Gamma_{99}$ | $12+13+23+14+15$ | $(1,2,2,1,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{35}$ | $\Gamma_{164}$ | $12+13+23+14+15+45$ | $(1,2,2,2,2)$, $(2,1,1,1,1)$ |
| $\Gamma_{36}$ | $\Gamma_{125}$ | $12+13+23+14+15+245$ | $(1,2,2,2,2)$, $(2,1,1,1,1)$ |
| $\Gamma_{37}$ | $\Gamma_{149}$ | $12+13+23+14+15+245+345$ | $(1,2,2,2,2)$, $(2,1,1,1,1)$ |

continued on next page

Table 13 (continued)

| class | dual | minimal qualified sets | extreme points of $\Sigma_{\text{lin}}$ |
|---|---|---|---|
| $\Gamma_{38}$ | $\Gamma_{126}$ | $12+13+23+14+25$ | $(1,2,2,1,1)$, $(3/2,3/2,3/2,1,1)$, $(2,1,2,1,1)$, $(2,2,1,1,1)$ |
| $\Gamma_{39}$ | $\Gamma_{165}$ | $12+13+23+14+25+45$ | $(1,2,2,2,2)$, $(1,3,2,2,1)$, $(3/2,3/2,3/2,3/2,3/2)$, $(3/2,2,3/2,3/2,1)$, $(2,1,2,2,2)$, $(2,3/2,3/2,1,3/2)$, $(2,2,1,1,1)$, $(3,1,2,1,2)$ |
| $\Gamma_{41}$ | $\Gamma_{155}$ | $12+13+23+14+45$ | $(1,2,2,2,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{42}$ | $\Gamma_{105}$ | $12+13+23+14+245$ | $(1,2,2,2,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{43}$ | $\Gamma_{134}$ | $12+13+23+14+245+345$ | $(1,2,2,2,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{45}$ | $\Gamma_{79}$ | $12+13+23+145$ | $(1,2,2,1,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{48}$ | $\Gamma_{68}$ | $12+13+14+234+15$ | $(1,2,2,2,1)$, $(2,1,2,2,1)$, $(2,2,1,2,1)$, $(2,2,2,1,1)$, $(3,1,1,1,1)$ |
| $\Gamma_{49}$ | $\Gamma_{96}$ | $12+13+14+234+15+235$ | $(1,2,2,2,2)$, $(2,1,1,1,1)$ |
| $\Gamma_{50}$ | $\Gamma_{121}$ | $12+13+14+234+15+235+245$ | $(1,2,2,2,2)$, $(2,1,1,1,1)$ |
| $\Gamma_{51}$ | $\Gamma_{146}$ | $12+13+14+234+15+235+245+345$ | $(1,2,2,2,2)$, $(2,1,1,1,1)$ |
| $\Gamma_{52}$ | $\Gamma_{122}$ | $12+13+14+234+25$ | $(1,2,2,2,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{54}$ | $\Gamma_{159}$ | $12+13+14+234+25+35+45$ | $(1,2,2,2,1)$, $(2,1,1,1,2)$ |
| $\Gamma_{55}$ | $\Gamma_{147}$ | $12+13+14+234+25+345$ | $(1,2,2,2,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{56}$ | $\Gamma_{87}$ | $12+13+14+234+235$ | $(1,2,2,2,1)$, $(2,1,2,1,1)$, $(2,2,1,1,1)$, $(3,1,1,2,1)$ |
| $\Gamma_{57}$ | $\Gamma_{112}$ | $12+13+14+234+235+245$ | $(1,2,2,2,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{58}$ | $\Gamma_{139}$ | $12+13+14+234+235+245+345$ | $(1,2,2,2,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{60}$ | self-dual | $12+13+14+15+2345$ | $(1,2,2,2,2)$, $(2,1,2,2,2)$, $(2,2,1,2,2)$, $(2,2,2,1,2)$, $(2,2,2,2,1)$, $(3,1,1,1,1)$ |
| $\Gamma_{61}$ | $\Gamma_{97}$ | $12+13+14+25$ | $(1,2,1,1,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{62}$ | $\Gamma_{128}$ | $12+13+14+25+35$ | $(1,2,2,1,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{64}$ | $\Gamma_{124}$ | $12+13+14+25+345$ | $(1,2,2,2,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{65}$ | self-dual | $12+13+14+235$ | $(1,2,2,1,1)$, $(2,1,2,1,1)$, $(2,2,1,1,1)$, $(3,1,1,1,1)$ |
| $\Gamma_{66}$ | $\Gamma_{94}$ | $12+13+14+235+245$ | $(1,2,2,2,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{67}$ | $\Gamma_{120}$ | $12+13+14+235+245+345$ | $(1,2,2,2,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{69}$ | $\Gamma_{117}$ | $12+13+24+34+235$ | $(1,2,2,1,1)$, $(2,1,1,2,1)$ |
| $\Gamma_{70}$ | $\Gamma_{142}$ | $12+13+24+34+235+145$ | $(1,2,2,2,1)$, $(1,3,3,1,2)$, $(3/2,3/2,3/2,3/2,1)$, $(2,1,2,2,1)$, $(2,2,1,2,1)$, $(2,2,2,1,1)$, $(3,1,1,3,2)$ |
| $\Gamma_{71}$ | $\Gamma_{127}$ | $12+13+24+35$ | $(1,2,2,1,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{72}$ | $\Gamma_{166}$ | $12+13+24+35+45$ | $(1,2,2,1,2)$, $(1,2,2,2,1)$, $(3/2,3/2,3/2,3/2,3/2)$, $(2,1,1,2,2)$, $(2,1,2,2,1)$, $(2,2,1,1,2)$ |
| $\Gamma_{74}$ | $\Gamma_{90}$ | $12+13+24+235$ | $(1,2,2,1,1)$, $(2,1,2,1,1)$, $(2,2,1,1,1)$ |
| $\Gamma_{77}$ | $\Gamma_{116}$ | $12+13+24+235+345$ | $(1,2,2,1,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{78}$ | $\Gamma_{100}$ | $12+13+24+345$ | $(1,2,1,1,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{80}$ | $\Gamma_{148}$ | $12+13+234+235+45$ | $(1,2,2,1,1)$, $(3/2,3/2,3/2,1,1)$, $(2,1,1,2,2)$, $(2,1,2,1,1)$, $(2,2,1,1,1)$ |
| $\Gamma_{81}$ | self-dual | $12+13+234+235+145$ | $(1,2,2,1,1)$, $(2,1,2,1,1)$, $(2,2,1,1,1)$, $(3,1,1,2,2)$ |
| $\Gamma_{83}$ | $\Gamma_{136}$ | $12+13+234+235+145+245+345$ | $(1,2,2,1,1)$, $(3/2,3/2,3/2,1,1)$, $(2,1,1,2,2)$, $(2,1,2,1,1)$, $(2,2,1,1,1)$ |
| $\Gamma_{84}$ | self-dual | $12+13+234+235+245$ | $(1,2,2,1,1)$, $(2,1,2,1,1)$, $(2,2,1,1,1)$ |
| $\Gamma_{85}$ | $\Gamma_{111}$ | $12+13+234+235+245+345$ | $(1,2,2,1,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{86}$ | $\Gamma_{123}$ | $12+13+234+45$ | $(1,2,2,1,1)$, $(3/2,3/2,3/2,1,1)$, $(2,1,1,2,1)$, $(2,1,2,1,1)$, $(2,2,1,1,1)$ |
| $\Gamma_{89}$ | $\Gamma_{113}$ | $12+13+234+145+245+345$ | $(1,2,2,1,1)$, $(3/2,3/2,3/2,1,1)$, $(2,1,1,2,1)$, $(2,1,2,1,1)$, $(2,2,1,1,1)$ |
| $\Gamma_{91}$ | $\Gamma_{101}$ | $12+13+234+245+345$ | $(1,2,2,1,1)$, $(2,1,1,1,1)$ |
| $\Gamma_{143}$ | disconnected | $123+124+134+125$ | $(1,1,2,2,1)$, $(1,2,1,1,1)$ |
| $\Gamma_{160}$ | disconnected | $123+124+125+1345$ | $(1,1,2,2,2)$, $(1,2,1,1,1)$ |
| $\Gamma_{162}$ | disconnected | $123+124+135$ | $(1,1,2,1,1)$, $(1,2,1,1,1)$ |
| $\Gamma_{169}$ | disconnected | $123+124+1345$ | $(1,1,2,2,1)$, $(1,2,1,1,1)$ |

**The exceptional structures.** The remaining seventeen structures form the nine rows of Table 14. The first column gives a representative and the second its connected dual partner; $\Gamma_{88}$ is self-dual up to participant relabelling. The minimal qualified sets, CI-sensitive facets, and extreme vectors in each row refer to the representative. The corresponding data for a non-self-dual partner are obtained by the canonical participant relabelling that puts the

dual in Jackson–Martin form.

Table 14: The nine exceptional duality classes, with the CI-sensitive facets and extreme points of the representative's exact linear contribution region.

| class | dual | minimal qualified sets | CI-sensitive facets | extreme points of $\Sigma_{\mathrm{lin}}$ |
|---|---|---|---|---|
| $\Gamma_{28}$ | $\Gamma_{167}$ | $12+13+23+14+24+15+35$ | $4c_1+c_2+c_3\geq 9$ | $(1,2,3,2,2)$, $(1,3,2,2,2)$, $(3/2,3/2,3/2,3/2,3/2)$, $(2,1,2,1,1)$, $(2,2,1,1,1)$ |
| $\Gamma_{30}$ | $\Gamma_{153}$ | $12+13+23+14+24+15+345$ | $c_1+c_2+c_4\geq 5$; $c_1+c_2+c_3\geq 5$; $3c_1+c_2+c_4\geq 8$; $3c_1+c_2+c_3\geq 8$ | $(1,2,3,3,2)$, $(1,3,2,2,2)$, $(3/2,3/2,2,2,3/2)$, $(3/2,2,3/2,3/2,3/2)$, $(2,1,2,2,1)$, $(2,2,1,1,1)$ |
| $\Gamma_{40}$ | $\Gamma_{150}$ | $12+13+23+14+25+345$ | $c_1+c_2+c_3\geq 5$; $c_1+2c_2+c_4\geq 6$; $2c_1+c_2+c_5\geq 6$; $c_1+3c_2+c_3\geq 8$; $3c_1+c_2+c_3\geq 8$ | $(1,2,3,2,2)$, $(1,3,2,2,1)$, $(3/2,3/2,2,3/2,3/2)$, $(3/2,2,3/2,3/2,1)$, $(2,1,3,2,2)$, $(2,3/2,3/2,1,3/2)$, $(2,2,1,1,1)$, $(3,1,2,1,2)$ |
| $\Gamma_{53}$ | $\Gamma_{152}$ | $12+13+14+234+25+35$ | $c_1+c_3+c_5\geq 5$; $c_1+c_2+c_5\geq 5$; $2c_1+c_2+c_3+c_4\geq 8$; $2c_1+c_2+2c_3\geq 8$; $2c_1+2c_2+c_3\geq 8$ | $(1,2,2,2,2)$, $(1,3,3,2,1)$, $(2,1,2,1,2)$, $(2,4/3,4/3,4/3,5/3)$, $(2,3/2,3/2,1,3/2)$, $(2,2,1,1,2)$, $(2,2,2,1,1)$, $(3,1,1,2,2)$ |
| $\Gamma_{73}$ | $\Gamma_{151}$ | $12{+}13{+}24{+}35{+}145$ | $c_1+c_2+c_3\geq 5$ | $(1,2,2,1,2)$, $(1,2,2,2,1)$, $(5/3,5/3,5/3,4/3,4/3)$, $(2,1,2,2,1)$, $(2,2,1,1,2)$, $(2,2,2,1,1)$, $(3,1,1,2,2)$ |
| $\Gamma_{75}$ | $\Gamma_{114}$ | $12+13+24+235+145$ | $2c_2+c_3\geq 4$; $2c_1+c_4\geq 4$; $c_1+2c_2+c_3\geq 6$; $2c_1+c_2+c_4\geq 6$ | $(1,2,2,2,1)$, $(3/2,3/2,3/2,3/2,1)$, $(3/2,2,3/2,1,3/2)$, $(2,1,2,2,1)$, $(2,3/2,1,3/2,3/2)$, $(2,2,1,1,1)$ |
| $\Gamma_{76}$ | $\Gamma_{140}$ | $12+13+24+235+145+345$ | $c_1+2c_2+c_3\geq 6$; $2c_1+c_2+c_4\geq 6$ | $(1,2,2,2,1)$, $(1,3,2,1,2)$, $(3/2,3/2,3/2,3/2,1)$, $(3/2,2,3/2,1,3/2)$, $(2,1,2,2,1)$, $(2,3/2,1,3/2,3/2)$, $(2,2,1,1,1)$, $(3,1,1,2,2)$ |
| $\Gamma_{82}$ | $\Gamma_{107}$ | $12+13+234+235+145+245$ | $2c_1+c_5\geq 4$; $2c_1+c_4\geq 4$ | $(1,2,2,2,2)$, $(3/2,3/2,3/2,1,1)$, $(2,1,1,2,2)$, $(2,1,2,1,1)$, $(2,2,1,1,1)$ |
| $\Gamma_{88}$ | self-dual | $12+13+234+145+245$ | $2c_1+c_5\geq 4$ | $(1,2,2,2,2)$, $(3/2,3/2,3/2,3/2,1)$, $(2,1,1,2,1)$, $(2,1,2,1,1)$, $(2,2,1,1,1)$ |

# B Technical profiles of nonlinear components

To verify the $\delta$-decompositions in Section 5 and the $\delta$-decomposition in Theorem 6.2, one needs the complete access functions and contribution vectors of the group-characterizable and PMF-based components. This appendix records those profiles in a form suitable for direct checking.

## B.1 Derived parameters of the group components

For a group component $N_j$, define

$$r_{N_j}(A)=\frac{|G_A|}{|G_0\cap G_A|}.$$

Then

$$\Phi_{N_j}(A) = \frac{\log\bigl(r_{N_j}(\varnothing)/r_{N_j}(A)\bigr)}{\log r_{N_j}(\varnothing)}, \qquad c_i = \frac{\log(|G|/|G_i|)}{\log r_{N_j}(\varnothing)}.$$

Thus the following ratios, together with the contribution-vector table below, give the complete profiles needed in the decompositions. Encode a coalition $A \subseteq \{1,\dots,5\}$ by

$$m(A) = \sum_{i\in A} 2^{i-1}.$$

The entry in row $N_j$ and column $m(A)$ is $r_{N_j}(A)$. For example, $A = \{1,3,5\}$ has $m(A) = 1+4+16 = 21$, and the entry in row $N_2$, column 21, gives $r_{N_2}(\{1,3,5\}) = 3$.

Table 15: The values $r_{N_j}(A)$, indexed by $m(A) = 0,\dots,31$. The columns are split into two blocks for readability.

| component / $m(A)$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $N_1$ | 6 | 6 | 2 | 2 | 4 | 4 | 2 | 2 | 3 | 3 | 2 | 2 | 2 | 2 | 1 | 1 |
| $N_2$ | 6 | 6 | 2 | 2 | 3 | 3 | 2 | 2 | 4 | 4 | 2 | 2 | 2 | 2 | 1 | 1 |
| $N_3$ | 180 | 120 | 3 | 3 | 60 | 20 | 1 | 1 | 60 | 20 | 1 | 1 | 24 | 4 | 1 | 1 |
| $N_4$ | 90 | 90 | 18 | 18 | 30 | 15 | 12 | 6 | 48 | 24 | 12 | 6 | 24 | 12 | 6 | 3 |
| $N_5$ | 180 | 120 | 3 | 3 | 60 | 20 | 1 | 1 | 60 | 20 | 1 | 1 | 24 | 4 | 1 | 1 |
| $N_6$ | 180 | 120 | 3 | 3 | 60 | 20 | 1 | 1 | 60 | 20 | 1 | 1 | 24 | 4 | 1 | 1 |

| component / $m(A)$ | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $N_1$ | 6 | 6 | 2 | 2 | 2 | 2 | 1 | 1 | 3 | 3 | 2 | 2 | 2 | 2 | 1 | 1 |
| $N_2$ | 6 | 6 | 2 | 2 | 3 | 3 | 2 | 2 | 2 | 2 | 1 | 1 | 2 | 2 | 1 | 1 |
| $N_3$ | 18 | 3 | 3 | 3 | 6 | 1 | 1 | 1 | 6 | 1 | 1 | 1 | 2 | 1 | 1 | 1 |
| $N_4$ | 90 | 90 | 18 | 18 | 30 | 15 | 12 | 6 | 48 | 24 | 12 | 6 | 24 | 12 | 6 | 3 |
| $N_5$ | 36 | 6 | 3 | 3 | 12 | 2 | 1 | 1 | 12 | 2 | 1 | 1 | 4 | 1 | 1 | 1 |
| $N_6$ | 36 | 6 | 3 | 1 | 12 | 2 | 1 | 1 | 12 | 2 | 1 | 1 | 4 | 2 | 1 | 1 |

Table 16: Contribution vectors of the group-characterizable components. Each logarithm base is the corresponding $r_{N_j}(\varnothing)$ value in column 0 of Table 15.

| component | contribution vector |
|---|---|
| $N_1$ | $(0, \log_6 15, \log_6 15, \log_6 20, \log_6 2)$ |
| $N_2$ | $(0, \log_6 15, \log_6 20, \log_6 15, \log_6 2)$ |
| $N_3$ | $(\log_{180} 6, \log_{180} 60, \log_{180} 6, \log_{180} 6, \log_{180} 40)$ |
| $N_4$ | $(\log_{90} 2, \log_{90} 20, \log_{90} 6, \log_{90} 15, 0)$ |
| $N_5$ | $(\log_{180} 6, \log_{180} 60, \log_{180} 6, \log_{180} 6, \log_{180} 20)$ |
| $N_6$ | $(\log_{180} 6, \log_{180} 60, \log_{180} 6, \log_{180} 6, \log_{180} 20)$ |

Although $N_5$ and $N_6$ have the same contribution vector, their access profiles are different; for example, they differ in Table 15 at $m(A) = 19$ and $m(A) = 29$.

### B.2 Access profiles of the finite laws

For $D_j$, let $\eta_j = H_{D_j}(X_0)$. Then

$$\Phi_{D_j}(A) = \frac{I_{D_j}(X_0; X_A)}{\eta_j}, \qquad \eta_j \Phi_{D_j}(A) = I_{D_j}(X_0; X_A).$$

The columns use the same coalition index $m(A) = \sum_{i \in A} 2^{i-1}$ as in Section B.1. Displayed decimals are rounded to five places, with trailing zeros suppressed; theorem checks use outward-directed intervals evaluated from the exact rational PMFs.

Table 17: Unnormalized finite-law access values $\eta_j \Phi_{D_j}(A) = I_{D_j}(X_0; X_A)$ in bits. The two blocks use $m(A) = 0, \ldots, 15$ and $m(A) = 16, \ldots, 31$, respectively.

| law | $\eta_j$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $D_1$ | 1 | 0 | 0.0817 | 0 | 0.0817 | 0 | 0.54085 | 0 | 0.54085 | 0 | 0.54085 | 0 | 0.54085 | 0 | 1 | 0 | 1 |
| $D_2$ | 1 | 0 | 0 | 0.79429 | 0.79429 | 0.5488 | 0.5488 | 0.86816 | 0.86816 | 0.0412 | 0.0412 | 1 | 1 | 0.56216 | 0.56216 | 1 | 1 |
| $D_3$ | 1.57789 | 0 | 0 | 0.64506 | 0.64506 | 0.64738 | 0.64738 | 1.57789 | 1.57789 | 0.48701 | 0.48701 | 1.08982 | 1.08982 | 0.73377 | 0.73377 | 1.57789 | 1.57789 |
| $D_4$ | 1.49076 | 0 | 1.11057 | 0 | 1.11057 | 0.12542 | 1.49076 | 0.12542 | 1.49076 | 0.00214 | 1.49076 | 0.00214 | 1.49076 | 0.20646 | 1.49076 | 0.20646 | 1.49076 |
| $D_5$ | 2.11113 | 0 | 0.7786 | 0 | 0.7786 | 1.5078 | 1.76212 | 1.5078 | 1.76212 | 0.73153 | 2.03244 | 0.73153 | 2.03244 | 1.6057 | 2.11113 | 1.6057 | 2.11113 |
| $D_6$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.27807 | 0.76941 | 0.27807 | 0.76941 | 0.52199 | 1 | 0.52199 | 1 |
| $D_7$ | 0.36592 | 0 | 0.28603 | 0 | 0.28603 | 0.03938 | 0.36592 | 0.03938 | 0.36592 | 0.08779 | 0.29921 | 0.08779 | 0.29921 | 0.11522 | 0.36592 | 0.11522 | 0.36592 |
| $D_8$ | 0.14144 | 0 | 0.10144 | 0 | 0.10144 | 0.01181 | 0.11389 | 0.01181 | 0.11389 | 0.06079 | 0.11389 | 0.06079 | 0.11389 | 0.09058 | 0.14144 | 0.09058 | 0.14144 |
| $D_9$ | 1.67125 | 0 | 0 | 0.35323 | 0.35323 | 0.69358 | 0.69358 | 1.3143 | 1.3143 | 0.19857 | 0.19857 | 1.02395 | 1.02395 | 0.71311 | 0.71311 | 1.38579 | 1.38579 |
| $D_{10}$ | 1.67125 | 0 | 0 | 0.69358 | 0.69358 | 0.35323 | 0.35323 | 1.3143 | 1.3143 | 0.11555 | 0.11555 | 1.23936 | 1.23936 | 0.36816 | 0.36816 | 1.41327 | 1.41327 |

| law | $\eta_j$ | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $D_1$ | 1 | 0.0817 | 0.33333 | 0.0817 | 0.33333 | 0.0817 | 0.54085 | 0.0817 | 0.54085 | 0.0817 | 0.54085 | 0.0817 | 0.54085 | 1 | 1 | 1 | 1 |
| $D_2$ | 1 | 0.37232 | 0.37232 | 0.81017 | 0.81017 | 0.56216 | 0.56216 | 1 | 1 | 0.56216 | 0.56216 | 1 | 1 | 0.56216 | 0.56216 | 1 | 1 |
| $D_3$ | 1.57789 | 0.48486 | 0.48486 | 0.7367 | 0.7367 | 1.08048 | 1.08048 | 1.57789 | 1.57789 | 0.61476 | 0.61476 | 1.10521 | 1.10521 | 1.09568 | 1.09568 | 1.57789 | 1.57789 |
| $D_4$ | 1.49076 | 0.6288 | 1.11057 | 0.6288 | 1.11057 | 0.6604 | 1.49076 | 0.6604 | 1.49076 | 0.79544 | 1.49076 | 0.79544 | 1.49076 | 0.99977 | 1.49076 | 0.99977 | 1.49076 |
| $D_5$ | 2.11113 | 0.66019 | 2.0314 | 0.66019 | 2.0314 | 1.81513 | 2.05337 | 1.81513 | 2.05337 | 0.762 | 2.06257 | 0.762 | 2.06257 | 1.81987 | 2.11113 | 1.81987 | 2.11113 |
| $D_6$ | 1 | 0.05405 | 0.06474 | 0.05405 | 0.06474 | 0.2173 | 1 | 0.2173 | 1 | 0.4709 | 0.76941 | 0.4709 | 0.76941 | 0.52199 | 1 | 0.52199 | 1 |
| $D_7$ | 0.36592 | 0.0426 | 0.29329 | 0.0426 | 0.29329 | 0.11522 | 0.36592 | 0.11522 | 0.36592 | 0.11522 | 0.36592 | 0.11522 | 0.36592 | 0.11522 | 0.36592 | 0.11522 | 0.36592 |
| $D_8$ | 0.14144 | 0.01 | 0.11389 | 0.01 | 0.11389 | 0.01214 | 0.14144 | 0.01214 | 0.14144 | 0.08844 | 0.11389 | 0.08844 | 0.11389 | 0.09058 | 0.14144 | 0.09058 | 0.14144 |
| $D_9$ | 1.67125 | 0.11555 | 0.11555 | 0.36816 | 0.36816 | 1.23936 | 1.23936 | 1.41327 | 1.41327 | 0.4727 | 0.4727 | 1.05376 | 1.05376 | 1.31412 | 1.31412 | 1.66244 | 1.66244 |
| $D_{10}$ | 1.67125 | 0.19857 | 0.19857 | 0.71311 | 0.71311 | 1.02395 | 1.02395 | 1.38579 | 1.38579 | 0.4727 | 0.4727 | 1.31412 | 1.31412 | 1.05376 | 1.05376 | 1.66244 | 1.66244 |

# C Construction of the linear library

This appendix gives Bahariyan's recursive procedure, recalled in Section 3, for constructing the linear library. A library record is a labelled pair $(\Gamma, c)$, where $\Gamma$ is realized by a perfect linear scheme and $c$ is its contribution vector. Two records are identified only when both the labelled access structures and the contribution vectors coincide.

## C.1 Base cases on at most four participants

The recursion starts from the unique nontrivial one-participant access structure and its ideal scheme. Appendix A.1 records the remaining base cases: every connected access structure on at most three participants is ideal, and the four nonideal connected four-participant structures have the listed exact linear contribution regions. These records extend the base library for the five-participant recursion.

## C.2 Recursive step

Assume that the extreme contribution vectors of the connected access structures on fewer than $n$ participants have been reported and realized. To construct records on $[n]$:

1. choose a nonempty active set and partition it into blocks;
2. place on every block a smaller connected access structure together with a linear scheme realizing one of its extreme contribution vectors;
3. form the disjunctive union using a common secret, and add dummy participants outside the active set;
4. insert all participant relabellings and the linear schemes obtained by duality;
5. deduplicate the resulting labelled pairs.

Here a participant orbit is the set of all labelled records obtained by simultaneous permutation of the access structure and the coordinates of its contribution vector. For $n = 2, 3, 4$, every access structure is Shannon type, and this recursion realizes all extreme contribution vectors of $K(\Gamma)$. At $n = 5$, the Shannon and one-CI regions are computed first, and the same decomposition system is then applied to the resulting finite lists of extreme vectors. The two direct-seed stages described below occur only at this five-participant stage.

The records are then closed under weighted $(\lambda, \omega)$-decomposition. For a target extreme vector $t$ of an access structure $\Gamma$, the feasibility system is

$$\begin{aligned}
\sum_j \alpha_j \Phi_{\Gamma_j}(Q) &\geq \omega + 1 && (Q \in \Gamma),\\
\sum_j \alpha_j \Phi_{\Gamma_j}(F) &\leq \omega && (F \notin \Gamma),\\
\sum_j \alpha_j c_i^{(j)} &\leq t_i && (1 \leq i \leq 5),\\
\alpha_j &\geq 0.
\end{aligned}$$

A rational solution is converted into a finite linear scheme by clearing denominators and applying Theorem 2.5. All schemes used in one decomposition are realized in a common characteristic; extension fields may be used without changing the contribution vectors. Every newly realized extreme vector is inserted together with its orbit and dual, and the process is repeated until no new record is obtained.

### C.3 Direct seeds

Here a pair $(\Gamma, c)$ is called *characteristic-universal* if, for every prime characteristic $p$, some finite extension of $\mathrm{GF}(p)$ supports a perfect linear scheme realizing the same labelled access structure $\Gamma$ and the same contribution vector $c$. The extension degree may depend on $p$. Thus "universal" refers only to field characteristic; it does not claim that one fixed matrix works over every finite field. This property lets all components of a finite decomposition be embedded in one common extension field.

Universality matters here because the recursive decompositions may combine many components, all of which must be placed over one field characteristic before Theorem 2.5 is applied. The smaller-structure recursion supplies almost every needed record. The only additional inputs are five all-one records and three non-ideal extreme-vector records; the longer construction below exists solely to certify these eight inputs uniformly in the characteristic.

**Proposition C.1** (Characteristic-universal direct seeds)**.** *The eight pairs in Table 18 are characteristic-universal perfect linear schemes. Participant relabelling and linear duality applied to them supply every direct record missing from the recursive library.*

Table 18: Eight direct characteristic-universal seeds. Here $M$ and $M'$ denote the parametrized rank-three families below, while $U_{52}, U_{75}, U_{81}$ denote the integer multi-row representations in (9). The other members of each isomorphism–duality class are obtained by closure.

| role | structure | minimal qualified sets | vector | representation |
|---|---|---|---|---|
| all-one | $\Gamma_{102}$ | $12+34+135+235+145$ | $\mathbf{1}$ | $M$ |
| all-one | $\Gamma_{103}$ | $12+34+135+235+145+245$ | $\mathbf{1}$ | $M$ |
| all-one | $\Gamma_{104}$ | $12+34+135+245$ | $\mathbf{1}$ | $M$ |
| all-one | $\Gamma_{109}$ | $12+134+234+135+235+145+245+345$ | $\mathbf{1}$ | $M'$ |
| all-one | $\Gamma_{110}$ | $12+134+234+135+235+145+345$ | $\mathbf{1}$ | $M'$ |
| residual | $\Gamma_{52}$ | $12+13+14+234+25$ | $(2,1,1,1,1)$ | $U_{52}$ |
| residual | $\Gamma_{75}$ | $12+13+24+235+145$ | $(2,1,2,2,1)$ | $U_{75}$ |
| residual | $\Gamma_{81}$ | $12+13+234+235+145$ | $(1,2,2,1,1)$ | $U_{81}$ |

*Proof. All-one representatives.* Columns are ordered as dealer, participants $1,\dots,5$. Consider

$$M(x_1,x_2,y_3,y_4,z)=\begin{pmatrix}1 & x_1 & x_2 & y_3 & y_4 & z\\ 0 & 1 & 1 & 0 & 0 & 1\\ 0 & 0 & 0 & 1 & 1 & 1\end{pmatrix}.$$

Assume $x_1 \neq x_2$ and $y_3 \neq y_4$. Then 12 and 34 are minimal qualified, and the qualification of $i\,j\,5$, for $i \in \{1,2\}$ and $j \in \{3,4\}$, is decided by the nonvanishing of

$$a_{ij} = z - x_i - y_j.$$

Thus $\Gamma_{102}$ is obtained by $a_{24} = 0$ with the other three $a_{ij} \neq 0$; $\Gamma_{103}$ by all four $a_{ij} \neq 0$; and $\Gamma_{104}$ by $a_{14} = a_{23} = 0$ and $a_{13}, a_{24} \neq 0$. These choices exist in every characteristic. For $\Gamma_{102}$, take $z = x_2 + y_4$ and choose nonzero $u = x_2 - x_1$ and $v = y_4 - y_3$ with $u + v \neq 0$; over characteristic two one may use GF(4). For $\Gamma_{104}$, the choice

$$(x_1, y_3, x_2, y_4, z) = (0, 0, 1, 1, 1)$$

works in every characteristic. For $\Gamma_{103}$, take a sufficiently large finite extension and choose $z$ outside the four values $\{x_i + y_j\}$.

For the other two ideal seeds use

$$M'(s_1, \ldots, s_5; t) = \begin{pmatrix} 1 & s_1 & s_2 & s_3 & s_4 & s_5 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & t \end{pmatrix}.$$

Besides $s_1 \neq s_2$, the seven decisive determinants are

$$\begin{aligned} d_{134} &= -s_1 - s_3 + s_4, \quad & d_{234} &= -s_2 - s_3 + s_4, \\ d_{135} &= -s_1 - ts_3 + s_5, \quad & d_{235} &= -s_2 - ts_3 + s_5, \\ d_{145} &= (t-1)s_1 - ts_4 + s_5, \quad & d_{245} &= (t-1)s_2 - ts_4 + s_5, \\ & & d_{345} &= (t-1)s_3 + s_4 - s_5. \end{aligned}$$

Taking all seven determinants nonzero gives $\Gamma_{109}$. Taking $d_{245} = 0$ and the other six nonzero gives $\Gamma_{110}$. For the latter, impose

$$s_5 = ts_4 - (t-1)s_2.$$

After this substitution every condition to be avoided remains a nonzero polynomial over every prime field. In both cases, a sufficiently large finite extension contains a point outside the finite union of their zero sets. Hence the five displayed ideal schemes exist over some extension of every field characteristic.

*Residual-vector representatives.* Let the dealer target be $e_1 = (1, 0, \ldots, 0)$, and let $V_i$ be the row space assigned to participant $i$. The following integer row systems define the three schemes:

$$\begin{array}{lll} U_{52}: & V_1 = \langle (-1,1,0), (0,1,1) \rangle, & V_2 = \langle (0,0,1) \rangle, \quad V_3 = \langle (1,1,1) \rangle, \\ & V_4 = \langle (0,1,0) \rangle, & V_5 = \langle (1,0,1) \rangle; \\ U_{75}: & V_1 = \langle (0,0,1,0), (0,1,0,1) \rangle, & V_2 = \langle (1,1,1,1) \rangle, \\ & V_3 = \langle (-1,1,0,1), (1,0,1,1) \rangle, & V_4 = \langle (1,0,1,1), (0,1,1,1) \rangle, \\ & V_5 = \langle (0,0,0,1) \rangle; & \\ U_{81}: & V_1 = \langle (0,1,1,0) \rangle, & V_2 = \langle (0,1,1,-1), (1,0,0,1) \rangle, \\ & V_3 = \langle (1,1,1,0), (1,0,1,1) \rangle, & V_4 = \langle (1,0,1,0) \rangle, \quad V_5 = \langle (0,1,0,0) \rangle. \end{array} \tag{9}$$

The share dimensions are respectively $(2,1,1,1,1)$, $(2,1,2,2,1)$, and $(1,2,2,1,1)$.

The determinant analysis above proves the assertion for the five ideal seeds. For each of the three integer row systems and every coalition $A \subseteq [5]$, let $R_A$ be the matrix of its share rows and let $\widetilde{R}_A = [e_1; R_A]$. Direct integer elimination gives only 1's as the nonzero

Smith invariant factors of both $R_A$ and $\widetilde{R}_A$. Therefore both ranks are unchanged after reduction modulo any prime. The condition

$$e_1 \in \operatorname{rowspan}(R_A) \quad \Longleftrightarrow \quad \operatorname{rank} R_A = \operatorname{rank} \widetilde{R}_A$$

is consequently independent of the characteristic. Reducing modulo two gives, respectively, the minimal qualified sets printed for $\Gamma_{52}, \Gamma_{75}, \Gamma_{81}$, so the same access relations hold in every characteristic. This also proves the displayed share dimensions in every characteristic. All $3 \times 32 \times 2$ rank and Smith-invariant conditions are verified by direct computation. □

The recursive completion uses exactly eight direct seeds: five all-one seeds and three residual-vector seeds. The five all-one representatives cover the duality classes

$$\{\Gamma_{102}, \Gamma_{115}\}, \quad \{\Gamma_{103}, \Gamma_{141}\}, \quad \{\Gamma_{104}\}, \quad \{\Gamma_{109}, \Gamma_{137}\}, \quad \{\Gamma_{110}\},$$

while the three residual representatives cover

$$\{\Gamma_{52}, \Gamma_{122}\}, \qquad \{\Gamma_{75}, \Gamma_{75}^{*}\}, \qquad \{\Gamma_{81}\}.$$

The structures $\Gamma_{104}, \Gamma_{110}, \Gamma_{81}$ are self-dual up to relabelling. These same counts—five all-one seeds, three residual seeds, eight total—are used throughout Section 3 and this appendix. After orbit and dual closure, the linear library contains 20,124 labelled records. The exact subset audit shows that all three residual duality classes are needed to generate the seven residual labelled endpoints.

### C.4 Realization of the extreme points

For each connected five-participant access structure, we first compute the relevant outer polyhedron: $K(\Gamma)$ in the Shannon-exact cases and $K^{\text{one-CI}}(\Gamma)$ in the exceptional cases. The decomposition system above is then solved for every extreme point of this polyhedron. The access structures and the extreme points of their linear contribution regions are listed in Appendix A. The recursive program produces a rational weighted decomposition realizing every listed vector. In particular, all 111 vertices of the one-CI regions of the seventeen exceptional structures are realized linearly.

## References

[1] Amos Beimel and Noam Livne. On matroids and nonideal secret sharing. *IEEE Transactions on Information Theory*, 54(6):2626–2643, 2008. doi:10.1109/TIT.2008.921708.

[2] Amir Jafari and Shahram Khazaei. On abelian and homomorphic secret sharing schemes. *Journal of Cryptology*, 34(4):43, 2021. doi:10.1007/s00145-021-09410-2.

[3] František Matúš. Matroid representations by partitions. *Discrete Mathematics*, 203(1–3):169–194, 1999. doi:10.1016/S0012-365X(99)00004-7.

[4] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979. doi:10.1145/359168.359176.

[5] George R. Blakley. Safeguarding cryptographic keys. In *AFIPS Conference Proceedings*, volume 48, pages 313–317, 1979. doi:10.1109/MARK.1979.8817296.

[6] Amos Beimel. Secret-sharing schemes: A survey. In Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology*, volume 6639 of *Lecture Notes in Computer Science*, pages 11–46. Springer, 2011. doi:10.1007/978-3-642-20901-7_2.

[7] Sorush Bahariyan. Determining the linear contribution-vector regions of small access structures. Master's thesis, Sharif University of Technology, Tehran, Iran, 2019. In Persian.

[8] Renato M. Capocelli, Alfredo De Santis, Luisa Gargano, and Ugo Vaccaro. On the size of shares for secret sharing schemes. *Journal of Cryptology*, 6(3):157–167, 1993. doi:10.1007/BF00198463.

[9] László Csirmaz. The size of a share must be large. *Journal of Cryptology*, 10(4):223–231, 1997. doi:10.1007/s001459900029.

[10] Oriol Farràs, Tarik Kaced, Sebastià Martín Molleví, and Carles Padró. Improving the linear programming technique in the search for lower bounds in secret sharing. *IEEE Transactions on Information Theory*, 66(11):7088–7100, 2020. Preliminary version in EUROCRYPT 2018. doi:10.1109/TIT.2020.3005706.

[11] Peter Gács and János Körner. Common information is far less than mutual information. *Problems of Control and Information Theory*, 2(2):149–162, 1973.

[12] Rudolf Ahlswede and János Körner. Source coding with side information and a converse for degraded broadcast channels. *IEEE Transactions on Information Theory*, 21(6):629–637, 1975. doi:10.1109/TIT.1975.1055469.

[13] Michael Bamiloshin, Aner Ben-Efraim, Oriol Farràs, and Carles Padró. Common information, matroid representation, and secret sharing for matroid ports. *Designs, Codes and Cryptography*, 89(1):143–166, 2021. doi:10.1007/s10623-020-00811-1.

[14] Wen-Ai Jackson and Keith M. Martin. Perfect secret sharing schemes on five participants. *Designs, Codes and Cryptography*, 9(3):267–286, 1996. doi:10.1007/BF00129769.

[15] Carles Padró, Leonor Vázquez, and An Yang. Finding lower bounds on the complexity of secret sharing schemes by linear programming. *Discrete Applied Mathematics*, 161:1072–1084, 2013.

[16] Motahhareh Gharahi and M. H. Dehkordi. Average complexities of access structures on five participants. *Advances in Mathematics of Communications*, 7:311–317, 2013.

[17] Marten van Dijk, Wen-Ai Jackson, and Keith M. Martin. A general decomposition construction for incomplete secret sharing schemes. *Designs, Codes and Cryptography*, 15(3):301–321, 1998. doi:10.1023/A:1008381427667.

[18] Carlo Blundo, Alfredo De Santis, Douglas R. Stinson, and Ugo Vaccaro. Graph decompositions and secret sharing schemes. *Journal of Cryptology*, 8(1):39–64, 1995. doi:10.1007/BF00204801.

[19] Motahhareh Gharahi and Shahram Khazaei. Optimal linear secret sharing schemes for graph access structures on six participants. *Theoretical Computer Science*, 771:1–8, 2019. doi:10.1016/j.tcs.2018.11.007.

[20] Jaume Martí-Farré and Carles Padró. Secret sharing schemes with three or four minimal qualified subsets. *Designs, Codes and Cryptography*, 34(1):17–34, 2005. doi:10.1007/s10623-003-4192-1.

[21] Jaume Martí-Farré, Carles Padró, and Leonor Vázquez. Optimal complexity of secret sharing schemes with four minimal qualified subsets. *Designs, Codes and Cryptography*, 61(2):167–186, 2011. doi:10.1007/s10623-010-9446-0.

[22] Jaume Martí-Farré and Carles Padró. Secret sharing schemes on access structures with intersection number equal to one. *Discrete Applied Mathematics*, 154(3):552–563, 2006. doi:10.1016/j.dam.2005.09.003.

[23] Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes. *Journal of Cryptology*, 4(2):123–134, 1991. doi:10.1007/BF00196772.

[24] Amos Beimel, Noam Livne, and Carles Padró. Matroids can be far from ideal secret sharing. In *Theory of Cryptography, TCC 2008*, volume 4948 of *Lecture Notes in Computer Science*, pages 194–212. Springer, 2008. doi:10.1007/978-3-540-78524-8_12.

[25] Jessica Ruth Metcalf-Burton. Improved upper bounds for the information rates of the secret sharing schemes induced by the Vámos matroid. *Discrete Mathematics*, 311(8–9):651–662, 2011. doi:10.1016/j.disc.2011.01.003.

[26] Douglas R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, 2(4):357–390, 1992. doi:10.1007/BF00125203.

[27] Wen-Ai Jackson and Keith M. Martin. Geometric secret sharing schemes and their duals. *Designs, Codes and Cryptography*, 4(1):83–95, 1994. doi:10.1007/BF01388562.

[28] Zhen Zhang and Raymond W. Yeung. On characterization of entropy function via information inequalities. *IEEE Transactions on Information Theory*, 44(4):1440–1452, 1998. doi:10.1109/18.681320.

[29] František Matúš. Infinitely many information inequalities. In *2007 IEEE International Symposium on Information Theory*, pages 2101–2105, 2007. doi:10.1109/ISIT.2007.4557201.

[30] Randall Dougherty, Christopher Freiling, and Kenneth Zeger. Non-shannon information inequalities in four random variables. arXiv:1104.3602, 2011.

[31] Emirhan Gürpınar and Andrei E. Romashchenko. How to use undiscovered information inequalities: Direct applications of the copy lemma. In *2019 IEEE International Symposium on Information Theory*, pages 1377–1381, 2019. doi:10.1109/ISIT.2019.8849309.

[32] Amir Jafari and Shahram Khazaei. Partial secret sharing schemes. *IEEE Transactions on Information Theory*, 69(8):5364–5385, 2023. doi:10.1109/TIT.2023.3265093.

[33] Oriol Farràs, Torben Brandt Hansen, Tarik Kaced, and Carles Padró. On the information ratio of non-perfect secret sharing schemes. *Algorithmica*, 79(4):987–1013, 2017. doi:10.1007/s00453-016-0217-9.

[34] Reza Kaboli, Shahram Khazaei, and Maghsoud Parviz. On group-characterizability of homomorphic secret sharing schemes. *Theoretical Computer Science*, 891:116–130, 2021. doi:10.1016/j.tcs.2021.08.032.

[35] Amos Beimel and Yuval Ishai. On the power of nonlinear secret-sharing. *SIAM Journal on Discrete Mathematics*, 19(1):258–280, 2005. Preliminary version in CCC 2001. doi:10.1137/S0895480102412868.

[36] Douglas R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Transactions on Information Theory*, 40(1):118–125, 1994. doi:10.1109/18.272461.

[37] Hung-Min Sun and Bor-Liang Chen. Weighted decomposition construction for perfect secret sharing schemes. *Computers & Mathematics with Applications*, 43(6–7):877–887, 2002. doi:10.1016/S0898-1221(01)00328-5.

[38] Motahhareh Gharahi and Shahram Khazaei. Reduced access structures with four minimal qualified subsets on six participants. *Advances in Mathematics of Communications*, 12(1):199–214, 2018. doi:10.3934/amc.2018014.

[39] Amos Beimel and Enav Weinreb. Separating the power of monotone span programs over different fields. *SIAM Journal on Computing*, 34(5):1196–1215, 2005. doi:10.1137/S0097539704444038.

[40] Terence H. Chan and Raymond W. Yeung. On a relation between information inequalities and group theory. *IEEE Transactions on Information Theory*, 48(7):1992–1995, 2002. doi:10.1109/TIT.2002.1013134.

[41] Terence H. Chan. Group characterizable entropy functions. In *2007 IEEE International Symposium on Information Theory*, pages 506–510, 2007. doi:10.1109/ISIT.2007.4557275.

[42] Tarik Kaced. Information inequalities are not closed under polymatroid duality. *IEEE Transactions on Information Theory*, 64(6):4379–4381, 2018. doi:10.1109/TIT.2018.2823328.

[43] László Csirmaz. Secret sharing and duality. *Journal of Mathematical Cryptology*, 15(1):157–173, 2021. doi:10.1515/jmc-2019-0045.