Recursive Common Information for Group-Characterizable Random Variables

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

Abstract

Common information (CI) is useful in entropy-based lower bounds for secret sharing. We study CI for group-characterizable (GC) random variables. Building on the sufficient condition of Kaboli–Khazaei–Parviz, we prove an exact pair criterion: two coset random variables X_H and X_K have common information if and only if the subgroups H and K permute, that is, $HK = KH$. Consequently, a GC tuple is 1-CI exactly when every pair of subgroups in the meet closure of its labels permutes, whereas it is recursively CI exactly when every pair in the generated subgroup sublattice permutes. This also gives a finite algorithm for deciding recursive CI, and we exhibit a GC tuple over $S_3 \times S_3$ that is 1-CI but not 2-CI. Since normal subgroups satisfy the recursive criterion, homomorphic random variables are recursively CI. For the twelve-participant disjoint Fano–non-Fano access structure, the Shannon lower-bound method with all separate 1-CI extensions still gives maximum and average optima equal to one. Two depth-two recursive CI extensions instead give the lower bounds 43/41 and 54089/51756 for the maximum and average information ratios of perfect homomorphic schemes. The same bounds hold for Abelian schemes; the exact mixed-linear and linear values are already known.

Keywords: common information; group-characterizable random variables; homomorphic secret sharing; subgroup lattice; Fano and non-Fano matroids.

1 Introduction

Let G be a finite group, let U be uniformly distributed on G, and for a subgroup $H \leq G$ let $X_H = UH$ denote the left coset containing U. The random variables obtained in this way are called group-characterizable (GC), and their joint entropies are logarithms of subgroup indices [1, 2]. GC random variables play a central role in the study of entropy regions and include the algebraic random variables arising from linear, Abelian, and homomorphic secret-sharing schemes.

Common information provides another algebraic constraint on entropy vectors. In the secret-sharing setting it leads to linear-programming lower bounds that can be stronger than those obtained from the Shannon inequalities alone [3–5]. Kaboli, Khazaei, and Parviz proved that a GC tuple has the CI property whenever the intersection subgroups associated with every two subcollections permute; as a consequence, homomorphic random variables have the CI property [6, Prop. 6.2 and Cor. 6.3]. Their result is the starting point of the present paper.

We distinguish between 1-CI and recursive CI. In 1-CI, common information is required for every pair of subcollections of the original tuple. In recursive CI, after adjoining a common-information variable, the same requirement may be imposed again on the

enlarged tuple, so later CI pairs may involve previously adjoined auxiliaries. This is the random-variable analogue of the k-CI and modular-extension hierarchies considered for polymatroids and matroids [5, 7].

We first complement the sufficient condition of Kaboli–Khazaei–Parviz by proving its converse for a pair: X_H and X_K have common information exactly when the subgroups H and K permute, that is, when $HK = KH$. This yields two finite algebraic characterizations. A tuple is 1-CI exactly when every pair in the meet closure of the original subgroup labels permutes; it is recursively CI exactly when every pair in the smallest subgroup sublattice containing those labels permutes. Since G is finite, the latter criterion gives an algorithm: generate this sublattice by intersections and joins and test every pair for permutability. The distinction is strict: we exhibit a four-variable GC tuple over $S_3 \times S_3$ that is 1-CI but not 2-CI.

The recursive criterion is automatic for normal subgroups and hence for homomorphic random variables. We use it with the CI lower-bound method of Farràs, Kaced, Martín Molleví, and Padró [3] for the disjoint union $F+N$ of the six-participant Fano and non-Fano matroid ports. For a class $\mathcal{C}$ of perfect schemes, let $\rho^{\mathcal{C}}_{\max}$ and $\rho^{\mathcal{C}}_{\mathrm{avg}}$ denote, respectively, the infimum of the maximum and average share entropies normalized by the secret entropy. Jafari and Khazaei determined these quantities for $F + N$ in the mixed-linear class as $7/6$ and $41/36$, respectively, and in the linear class as $4/3$ and $41/36$ [8, 9]. We show that imposing every 1-CI constraint separately does not improve the Shannon bound, whereas two recursive CI extensions give

$$\rho^{\mathrm{hom}}_{\max}(F + N) \geq \frac{43}{41}, \qquad \rho^{\mathrm{hom}}_{\mathrm{avg}}(F + N) \geq \frac{54089}{51756}. \tag{1}$$

The same bounds hold for Abelian schemes.

The paper is organized as follows. Section 2 develops the subgroup-theoretic criteria for 1-CI and recursive CI. Section 3 separates the two notions by an explicit construction over $S_3 \times S_3$. Section 4 applies recursive CI to secret sharing and derives the bounds in (1) for the Fano–non-Fano structure. Section 5 concludes with several open problems.

2 Recursive Common Information in GC Systems

For finite-valued random variables Y and W, we write $Y \equiv W$ if

$$H(Y|W) = H(W|Y) = 0.$$

Thus Y and W contain exactly the same information, possibly with different labels for their outcomes. Throughout the paper, random variables are identified under this equivalence.

A random variable Z is a *common information* of Y and W if

$$H(Z|Y) = H(Z|W) = 0, \qquad H(Z) = I(Y; W). \tag{2}$$

Every tuple is 0-CI. For $k \geq 1$, a tuple is k-CI if, for every pair of subcollections, one can adjoin a common information so that the enlarged tuple is $(k-1)$-CI. A tuple is *recursively CI* if it is k-CI for every k.

Let U be uniformly distributed on G. For every subgroup $H \leq G$, write

$$X_H := UH.$$

Given $G_1, \ldots, G_n \leq G$, set

$$X_i := X_{G_i} := UG_i, \qquad i \in [n].$$

For $A \subseteq [n]$, write

$$X_A = (X_i : i \in A), \qquad G_A = \bigcap_{i \in A} G_i,$$

where $G_\varnothing = G$. The joint map $u \mapsto (uG_i : i \in A)$ takes the same value at $u, v \in G$ exactly when $uG_A = vG_A$. Thus its level sets are the left cosets of G_A, and hence

$$X_A \equiv X_{G_A}, \qquad H(X_A) = \log |G : G_A|. \tag{3}$$

More generally, $(X_{H_1}, \ldots, X_{H_m}) \equiv X_{H_1 \cap \cdots \cap H_m}$ for arbitrary subgroups $H_1, \ldots, H_m \leq G$.

Let $\mathrm{Sub}(G)$ denote the lattice of subgroups of G, ordered by inclusion. Its meet and join are

$$H \wedge K = H \cap K, \qquad H \vee K = \langle H, K \rangle.$$

We say that two subgroups $H, K \leq G$ *permute* if $HK = KH$. In that case HK is a subgroup and equals $H \vee K$.

For arbitrary finite random variables, the maximal common function is determined by the connected components of their bipartite support graph [10]. In the present coset setting this function is $X_{H \vee K}$: alternating H- and K-moves from g reach exactly the coset $g\langle H, K \rangle$, so the connected components are the left cosets of $H \vee K$.

Theorem 1 (Pair criterion)**.** *Let $H, K \leq G$. The following conditions are equivalent:*

(i) X_H *and* X_K *have common information;*

(ii) $HK = KH$*;*

(iii) HK *is a subgroup of* G*;*

(iv) $HK = H \vee K$*.*

If these conditions hold, X_{HK} *is a common information of* X_H *and* X_K*.*

Proof. The equivalence of (ii)–(iv) is standard. The implication (ii)⇒(i) is the two-variable case of [6, Prop. 6.2]; we include the short argument for completeness and prove the converse. Using (3),

$$I(X_H; X_K) = \log \frac{|G|\,|H \cap K|}{|H|\,|K|} = \log \frac{|G|}{|HK|},$$

where $|HK| = |H||K|/|H \cap K|$ even when HK is not a subgroup. The maximal-common-function observation gives

$$H(X_{H \vee K}) = \log \frac{|G|}{|H \vee K|} \leq I(X_H; X_K).$$

If a common information Z exists, then it is a function of $X_{H \vee K}$ and

$$I(X_H; X_K) = H(Z) \leq H(X_{H \vee K}) \leq I(X_H; X_K),$$

so $|HK| = |H \vee K|$ and $HK = H \vee K$. Conversely, if $HK = KH$, then $HK = H \vee K$ is a subgroup and X_{HK} is a function of both variables with entropy $I(X_H; X_K)$. □

For the subgroup tuple $(G; G_1, \ldots, G_n)$, let

$$\mathcal{M} = \{G_A : A \subseteq [n]\}.$$

Thus $\mathcal{M}$ is the meet closure of $G_1, \ldots, G_n$ inside $\mathrm{Sub}(G)$. We also let $\mathcal{L}$ be the smallest sublattice of $\mathrm{Sub}(G)$ containing $G_1, \ldots, G_n$; equivalently, $\mathcal{L}$ is obtained by repeatedly taking intersections and subgroup joins. In particular, $\mathcal{M} \subseteq \mathcal{L}$.

Theorem 2 (1-CI and recursive criteria)**.** *Let $(X_1, \ldots, X_n)$ be induced by $(G; G_1, \ldots, G_n)$. Then:*

1. *the tuple is 1-CI if and only if $HK = KH$ for all $H, K \in \mathcal{M}$;*
2. *the tuple is recursively CI if and only if $HK = KH$ for all $H, K \in \mathcal{L}$.*

Proof. For 1-CI, Equation (3) identifies the two joint observations X_A and X_B with subgroup labels $G_A, G_B \in \mathcal{M}$. The claim is therefore exactly Theorem 1. The forward implication is the converse missing from the sufficient criterion of [6, Prop. 6.2].

For recursion, first assume every pair in $\mathcal{L}$ permutes. Induct on k: every requested pair has intersection labels $H, K \in \mathcal{L}$, Theorem 1 supplies $X_{H \vee K}$, and the new label remains in $\mathcal{L}$. Hence the enlarged tuple is $(k-1)$-CI.

Conversely, take $H, K \in \mathcal{L}$. By definition of $\mathcal{L}$, each of H and K can be obtained from $G_1, \ldots, G_n$ by a finite expression using only intersections and subgroup joins. Choose such expressions and evaluate their join operations in an order in which every input has already been constructed. A meet is represented by taking a joint variable, by (3); a join is represented by adjoining a CI, which can be identified with the corresponding coset variable by Theorem 1. If the initial recursion depth exceeds the total number of join nodes, the resulting extension is still 1-CI and contains X_H and X_K. Hence these two variables have common information, and Theorem 1 gives $HK = KH$. □

Corollary 3 (Homomorphic RVs)**.** *Every GC tuple induced by normal subgroups is recursively CI. In particular, every homomorphic RV tuple is recursively CI.*

Proof. Meets and joins of normal subgroups are normal, hence every pair in $\mathcal{L}$ permutes. Apply Theorem 2 and the normal-subgroup representation of homomorphic RVs [6, Thm. 5.2]. □

Consequently, any prescribed finite sequence of CI adjunctions can be carried out for a homomorphic tuple, provided each new CI uses variables already present. Theorem 2 also gives an algorithm for deciding recursive CI of a finite GC tuple: generate $\mathcal{L}$ by intersections and joins and test every pair in $\mathcal{L}$ for permutability.

3 1-CI Need Not Imply Recursive CI

Let $G = S_3^{(1)} \times S_3^{(2)}$, where the two factors act on the disjoint blocks $\{1,2,3\}$ and $\{4,5,6\}$. Choose

$$\begin{aligned} a &= (1\ 2\ 3), \quad x = (2\ 3) \in S_3^{(1)}, \\ b &= (4\ 5\ 6), \quad y = (5\ 6) \in S_3^{(2)}. \end{aligned}$$

Thus (x, y) and (a, b) are elements of the direct product G. Define

$$\begin{aligned} G_1 &= \langle (x, y) \rangle, \qquad G_2 = \langle (a, b) \rangle, \\ G_3 &= \mathbf{1} \times S_3^{(2)}, \qquad G_4 = S_3^{(1)} \times \mathbf{1}. \end{aligned} \tag{4}$$

Theorem 4. *The four-variable GC tuple induced by* (4) *is 1-CI but is not 2-CI.*

Proof. All nontrivial pairwise intersections among G_1, G_2, G_3, G_4 are trivial, so

$$\mathcal{M} = \{\mathbf{1}, G, G_1, G_2, G_3, G_4\}.$$

Every pair in this set permutes: G_1G_2 is a diagonal copy of S_3, $G_1G_3 = \langle x\rangle \times S_3$, $G_1G_4 = S_3 \times \langle y\rangle$, $G_2G_3 = \langle a\rangle \times S_3$, $G_2G_4 = S_3 \times \langle b\rangle$, and $G_3G_4 = G$. Theorem 2 gives 1-CI.

Now take (X_1, X_4). Theorem 1 forces its common information to have subgroup

$$C = G_1G_4 = S_3 \times \langle y\rangle, \qquad |C| = 12.$$

In the extension, the joint variable of X_C and X_{G_3} has subgroup

$$Y = C \cap G_3 = \mathbf{1} \times \langle y\rangle, \qquad |Y| = 2.$$

But Y and $G_2 = \langle (a, b)\rangle$ do not permute: $|YG_2| = 6$ while $|\langle Y, G_2\rangle| = 18$. Thus

$$I(X_Y; X_2) = \log 6 > \log 2 = H(X_{Y\vee G_2}),$$

so this pair has no common information. By the maximal-common-function observation, the first CI is necessarily X_C. Hence no alternative choice of the first auxiliary avoids the failure. □

4 Application to the Fano–Non-Fano Structure

Let $\Gamma \subseteq 2^{[n]}$ be an access structure. A perfect scheme $(S, X_1, \ldots, X_n)$ realizes Γ if

$$H(S|X_A) = 0 \quad (A \in \Gamma), \qquad I(S; X_B) = 0 \quad (B \notin \Gamma). \tag{5}$$

For a scheme with $H(S) > 0$, define the normalized entropy function

$$h(A) := \frac{H(A)}{H(S)}$$

for every collection A of secret, share, and auxiliary random variables. Thus $h(S) = 1$. The contribution of participant i is

$$\rho_i := \frac{H(X_i)}{H(S)} = h(X_i),$$

and the maximum and average information ratios of a scheme are $\max_i \rho_i$ and $n^{-1}\sum_i \rho_i$. Their infima over all schemes realizing Γ are denoted $\rho_{\max}(\Gamma)$ and $\rho_{\text{avg}}(\Gamma)$. When the infimum is restricted to a class $\mathcal{C}$, we write $\rho^{\mathcal{C}}_{\max}(\Gamma)$ and $\rho^{\mathcal{C}}_{\text{avg}}(\Gamma)$.

We use the CI lower-bound method of Farràs, Kaced, Martín Molleví, and Padró [3]. One minimizes the desired information-ratio objective over normalized polymatroids satisfying the perfect-secret-sharing equalities, the Shannon inequalities, and suitable CI extension identities. If A and B are collections of variables, adjoining a new variable z as a CI of A and B means imposing

$$\begin{aligned} h(zA) &= h(A), & h(zB) &= h(B), \\ h(z) &= h(A) + h(B) - h(AB). \end{aligned} \tag{6}$$

A *separate* 1-*CI relaxation* uses an independent extension for each pair (A, B) of collections of original variables. In a recursive extension, a later pair may also contain CI variables adjoined earlier. We shall also use, for $A \subseteq B$ and any auxiliary collection Z, the Shannon consequence

$$0 \le h(ZB) - h(ZA) \le h(B) - h(A). \tag{7}$$

Let F be the Fano port with minimal qualified sets

$$14, 25, 36, 123, 156, 246, 345,$$

and let N be the non-Fano port obtained by adding 456. Their disjoint union $F + N$ has twelve participants and is qualified whenever either block is qualified. The exact mixed-linear and pure-linear values are [8, 9]

	$\rho_{\max}$	ρ_{avg}
mixed-linear	7/6	41/36
pure linear	4/3	41/36.

(8)

The mixed-linear maximum ratio has infimum 7/6, but no mixed-linear scheme attains this value.

For a polymatroid h on a ground set E, define

$$\mathrm{cl}_h(A) := \{e \in E : h(Ae) = h(A)\}.$$

A set P is a *flat* if $\mathrm{cl}_h(P) = P$.

Lemma 5 (Flat-pair reduction)**.** *Let $P = \mathrm{cl}_h(A)$ and $Q = \mathrm{cl}_h(B)$. Then the CI identities for (A, B) are equivalent to those for (P, Q). Moreover:*

1. *if $P \subseteq Q$ or $Q \subseteq P$, a common information is already present in the base polymatroid;*
2. *if*
$$h(P) + h(Q) = h(PQ) + h(P \cap Q),$$
then $P \cap Q$ is a common information of P and Q.

Consequently, a new CI auxiliary is needed only for incomparable flat pairs P, Q for which the submodular inequality is strict.

Proof. Since $h(A) = h(P)$, submodularity implies $h(zA) = h(zP)$ in every extension; the same holds for B and Q. Hence the CI identities depend only on the two closures. If $P \subseteq Q$, then $h(P) = I(P; Q)$, so P itself serves as a common information; the case $Q \subseteq P$ is symmetric. If equality holds in the displayed submodular inequality, then $I(P; Q) = h(P \cap Q)$, and $P \cap Q$ is a function of both P and Q. □

Let $\mathcal{P}_{\text{sep}}(F + N)$ denote the set of normalized polymatroids satisfying the perfect-access equalities (5) and all elemental Shannon inequalities, and such that every pair of collections of the original variables admits a separate Shannon extension satisfying (6).

Theorem 6 (Complete separate 1-CI)**.** *For $F + N$,*

$$\inf_{h \in \mathcal{P}_{\text{sep}}} \max_{1 \le i \le 12} h(X_i) = 1, \qquad \inf_{h \in \mathcal{P}_{\text{sep}}} \frac{1}{12} \sum_{i=1}^{12} h(X_i) = 1. \tag{9}$$

Proof. The lower bound $h(X_i) \ge 1$ follows from (5): choose a minimal qualified set containing i and delete i. For the reverse inequality, let h_0 be the rank function of the matroid obtained by taking the parallel connection of the Fano and non-Fano matroids at their common dealer element S. This matroid has rank five, realizes $F + N$, and every singleton has rank one; hence

$$h_0(S) = h_0(X_1) = \cdots = h_0(X_{12}) = 1.$$

The matroid has 168 flats. Lemma 5 removes the comparable pairs and the pairs for which equality holds in the submodular inequality. Independent automorphisms of the Fano and non-Fano blocks identify the remaining pairs into 58 symmetry classes. For one representative of each class, Supplementary Material gives an explicit Shannon extension satisfying (6); applying the same block symmetry gives an extension for every pair in that class. Therefore $h_0 \in \mathcal{P}_{\text{sep}}$, and both objectives in (9) are at most one. Together with the preceding lower bound, this proves the theorem. □

For the recursive bounds, write $z = \mathrm{CI}(A; B)$ as shorthand for adjoining a variable z that satisfies (6) for the pair (A, B). We use the following two depth-two recursive extensions:

$$\begin{aligned} z_1 &= \mathrm{CI}(X_{\{1,7\}}; X_{\{4,10\}}), \\ w_1 &= \mathrm{CI}((z_1, X_2, X_8); (z_1, X_3, X_9)), \end{aligned} \tag{10}$$

and

$$\begin{aligned} z_2 &= \mathrm{CI}(X_{\{2,3,4,7\}}; X_{\{1,10\}}), \\ w_2 &= \mathrm{CI}((z_2, X_2, X_8); (z_2, X_5, X_{11})). \end{aligned} \tag{11}$$

We impose the two recursive extensions simultaneously. By Corollary 3, every homomorphic scheme admits all four CI variables in (10)–(11).

The access structure and both objectives are invariant under independent automorphisms of the Fano and non-Fano blocks. Averaging a polymatroid over these automorphisms preserves the average objective and cannot increase the maximum objective, so it suffices to consider invariant polymatroids. Let $\mathcal{P}_{\text{rec}}$ be the normalized Shannon polyhedron obtained by imposing the perfect-access constraints, the CI identities in (10)–(11), and the inequalities (7) for the corresponding inclusions. By Corollary 3, every perfect homomorphic scheme yields a feasible point of $\mathcal{P}_{\text{rec}}$. Therefore minimizing either objective over $\mathcal{P}_{\text{rec}}$ can only decrease the value attainable by homomorphic schemes, and its optimum is a lower bound on the corresponding homomorphic information ratio.

Theorem 7 (Homomorphic bounds)**.** *For perfect homomorphic secret sharing on $F + N$,*

$$\rho^{\text{hom}}_{\max}(F + N) \geq \frac{43}{41}, \qquad \rho^{\text{hom}}_{\text{avg}}(F + N) \geq \frac{54089}{51756}. \tag{12}$$

The same inequalities hold for perfect Abelian schemes.

Proof. Exact rational optimization over $\mathcal{P}_{\text{rec}}$ gives

$$\min_{h \in \mathcal{P}_{\text{rec}}} \max_i h(X_i) = \frac{43}{41}, \qquad \min_{h \in \mathcal{P}_{\text{rec}}} \frac{1}{12} \sum_i h(X_i) = \frac{54089}{51756}.$$

The preceding relaxation argument therefore gives the two homomorphic lower bounds. Abelian schemes are a subclass of homomorphic schemes. □

Kaboli–Khazaei–Parviz further prove that, for GC schemes whose secret subgroup is normal, almost-perfect or statistical realization is eventually perfect [6, Prop. 6.6 and Cor. 6.7]. Therefore the bounds in (12) also apply under those security notions.

The role of recursion is visible already in (10): the second CI, which defines w_1, uses the previously adjoined variable z_1 on both sides. Such a constraint is absent from the separate 1-CI relaxation, whose exact optimum is given by Theorem 6.

5 Conclusion

We have completed the subgroup condition of Kaboli–Khazaei–Parviz to an exact pair criterion and characterized 1-CI and recursive CI for GC random variables: the former is controlled by the meet closure, the latter by the generated subgroup sublattice. Normal-subgroup systems, and hence homomorphic random variables, therefore admit arbitrary finite recursive CI extensions. For $F + N$, complete separate 1-CI still has optimum one, whereas two depth-two recursive extensions yield the strict homomorphic bounds (12).

Natural questions are whether every finite CI depth occurs, whether there exists a homomorphic or Abelian scheme for $F + N$ whose maximum or average information ratio is strictly smaller than the corresponding mixed-linear optimum, and how useful recursive CI extensions can be selected effectively from finite-group data.

Supplementary Information

The Supplementary Material is archived at Zenodo, doi:10.5281/zenodo.21864500. It contains the explicit Shannon extensions for the 58 symmetry classes used in Theorem 6 and exact rational primal–dual certificates for the two linear programs used in Theorem 7.

Statements and Declarations

Competing interests. The author declares no competing interests.

Data availability. The exact rational certificates used for the finite computations are available in the Supplementary Material archived at Zenodo, doi:10.5281/zenodo.21864500. No additional research dataset is required.

Use of generative AI. Generative-AI tools were used for language editing and computational assistance. The author independently checked the mathematical statements and exact certificates and takes full responsibility for the content.

References

[1] 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.2002.1013138. URL `https://doi.org/10.1109/TIT.2002.1013138`.

[2] Terence H. Chan. Group characterizable entropy functions. In *2007 IEEE International Symposium on Information Theory*, pages 506–510, 2007. doi: 10.1109/ISIT.2007.4557077. URL `https://doi.org/10.1109/ISIT.2007.4557077`.

[3] 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. doi: 10.1109/TIT.2020.3005706. URL `https://doi.org/10.1109/TIT.2020.3005706`. Preliminary version in EUROCRYPT 2018, LNCS 10820, 597–621.

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

[5] Michael Bamiloshin, Oriol Farràs, and Carles Padró. A note on extension properties and representations of matroids. *Discrete Applied Mathematics*, 376:270–280, 2025. doi: 10.1016/j.dam.2025.06.028. URL https://doi.org/10.1016/j.dam.2025.06.028.

[6] 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. URL https://doi.org/10.1016/j.tcs.2021.08.032.

[7] Kristóf Bérczi, Boglárka Gehér, András Imolay, László Lovász, Carles Padró, and Tamás Schwarcz. Interaction between skew-representability, tensor products, extension properties, and rank inequalities. In *Proceedings of the 2026 Annual ACM–SIAM Symposium on Discrete Algorithms (SODA)*, pages 328–354. Society for Industrial and Applied Mathematics, 2026. doi: 10.1137/1.9781611978971.15. URL https://doi.org/10.1137/1.9781611978971.15.

[8] 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. URL https://doi.org/10.1007/s00145-021-09410-2.

[9] 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. URL https://doi.org/10.1109/TIT.2023.3265093.

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