Reverse Substitution in Secret Sharing:
The Critical One-Half Threshold and a Route to Superpolynomial Lower Bounds

Shahram Khazaei
Department of Mathematical Sciences, Sharif University of Technology

Abstract

The contribution vector (convec) of a secret-sharing scheme is the vector of its normalized share sizes. The average and maximum coordinates of a convec give, respectively, the average and maximum information ratios of the scheme. Obtaining superlinear lower bounds on these quantities for unrestricted perfect secret sharing has remained a challenging open problem for about four decades. In this paper, we study substitution, a natural way to build complicated access structures from simpler ones: one participant of an outer access structure is replaced by an inner access structure. Given secret-sharing schemes for the two factors, the standard forward construction composes them into a scheme for the composite access structure. We study the converse question. Given an arbitrary scheme for the composite access structure, we ask to what extent its convec admits a reverse factorization into convecs for the outer and inner factors, up to a common multiplicative loss.

Exact reversal is false: we give a counterexample whose optimal reverse factor is $8/9$, with a composite scheme that is scalar-linear over every finite field. On the positive side, we prove that a factor $1/2$ is always attainable, and that every fixed instance admits a strictly larger factor.

For a recursive family built from Csirmaz's classical access structure $\mathcal{C}_k$, whose distinguished set has size k, we identify a critical reverse factor that determines when the resulting lower bound becomes superlinear. This critical factor exceeds one half by only an amount of order $(\log k)/k$. Crossing it yields superlinear lower bounds, while any fixed positive excess above one half gives a route to superpolynomial lower bounds. Using only Shannon inequalities, the corresponding recursive factor cannot cross the critical value. Thus any improvement sufficient to pass this threshold must exploit constraints beyond the Shannon inequalities.

Keywords. secret sharing; access structures; information ratio; substitution; contribution vectors; multilinear secret sharing.

1 Introduction

A perfect secret-sharing scheme distributes a secret among a finite set of participants so that every qualified coalition can reconstruct it while every forbidden coalition learns nothing about it [1, 2]. The efficiency of a scheme is measured by the sizes of the shares relative to the size of the secret; the maximum of these normalized share sizes is called the information ratio of the scheme. For general access structures on n participants, obtaining large lower bounds on these normalized share sizes remains a central problem; the classical construction of Csirmaz gives the benchmark $\Omega(n/\log n)$ lower bound for unrestricted perfect secret sharing [5, 15]. In a 2026 preprint, Williamson proved an $\Omega(n)$ lower bound on the maximum information ratio, together with an $\Omega(n^2)$

lower bound on the total normalized share size, using only Shannon inequalities [22, Corollary 3]. These match the universal $O(n)$ and $O(n^2)$ ceilings of the Shannon-information method up to constants [5, Theorem 3.5]. Thus any superlinear lower bound on the maximum information ratio must use information beyond Shannon inequalities. Non-Shannon information inequalities, beginning with the inequality of Zhang and Yeung [7], provide one possible source of such additional information. Auxiliary-variable methods, notably the copy lemma and the Ahlswede–Körner method, give systematic ways of deriving such inequalities; their relation is studied in [10]. These tools have produced strict improvements over Shannon bounds for particular access structures [8, 12]. However, no superlinear asymptotic lower bound for unrestricted perfect secret sharing is known from these methods. There are also known limitations on what such inequalities can yield: Beimel and Orlov showed that all four- and five-variable information inequalities, together with the higher-variable inequalities known at the time, cannot yield an $\omega(n)$ lower bound on the share size [9]; further limitations for bounded-variable information inequalities were obtained in [11].

Much stronger lower bounds are known under algebraic restrictions. Monotone-span-program methods yield strong lower bounds for scalar-linear secret sharing [16, 17]. Pitassi and Robere proved exponential lower bounds for scalar-linear secret sharing of explicit access structures over arbitrary fields [19]; a counting argument gives a $2^{n/2-o(n)}$ lower bound on the scalar-linear information ratio of almost all access structures, and Nir recently proved the matching worst-case upper bound [20]. Exponential lower bounds for the multilinear information ratio of explicit access structures were recently proved in the preprint [21]. These results concern restricted algebraic classes; the question here is whether reverse substitution can yield stronger lower bounds for unrestricted perfect secret sharing.

1.1 Substitution and the forward construction

One way to seek larger lower bounds is to build access structures recursively. The operation studied here is *substitution*, introduced in the secret-sharing setting by Martin [4]. Let Γ be an outer access structure on $R \sqcup \{p\}$, and let Δ be an inner access structure on a disjoint participant set Q. We write

$$\Gamma[p \leftarrow \Delta]$$

for the access structure obtained by replacing the role of p by a copy of Δ: informally, whenever an outer coalition needs participant p, the replacing participants must contain a qualified coalition of Δ. The precise definition is given in Section 2.4.

The same notation has a numerical counterpart. If

$$x = (x_R, x_p) \qquad \text{and} \qquad y = (y_q)_{q \in Q}$$

are real vectors, we define

$$x[p \leftarrow y] = (x_R, (x_p y_q)_{q \in Q}).$$

When x and y are the contribution vectors (convecs), i.e., the vectors of normalized share sizes, of schemes for the outer and inner access structures Γ and Δ, respectively, the factor x_p has a simple meaning: the inner scheme is sharing an object whose size is the size of the outer share at p.

This formula is exactly what the standard forward construction gives when the two schemes are distribution-compatible. One first runs the outer scheme and obtains the share X_p intended for p, and then shares X_p using the inner scheme. If x and y are the corresponding convecs, and if, up to relabeling, X_p and the secret of the inner scheme are identically distributed, then the resulting composite convec is

$$c = x[p \leftarrow y]. \tag{1}$$

Thus, under this distribution-compatibility assumption, substitution provides an immediate upper-bound template: choose schemes for the two factors and compose them. Section 2.5 states the precise forward construction. This compatibility condition concerns the forward construction only; the reverse problem below starts from a composite scheme that already exists.

1.2 The reverse question

For lower bounds, we need a converse to the construction in (1). Suppose that an arbitrary scheme for

$$\Omega = \Gamma[p \leftarrow \Delta]$$

is given, with convec c. There is no reason for this scheme to have been produced by the forward construction. We ask whether one can nevertheless find an outer convec x and an inner convec y for which

$$r\, x[p \leftarrow y] \le c \tag{2}$$

coordinatewise, with a universal constant $r > 0$. Exact reverse substitution corresponds to $r = 1$.

Outer and inner schemes can each be recovered separately from the scheme for the composed access structure Ω, but not necessarily with convecs compatible with (2). Two elementary constructions make this distinction explicit.

First, group the entire inner block of the composite scheme into one share and give that tuple to a new participant playing the role of p. This produces a valid outer scheme for Γ and leaves all untouched outer shares unchanged. The problem is that the new share at p may be much larger than necessary. If the inner access structure has a participant that is qualified by itself, however, the share of that participant alone can play the role of p, so grouping the entire inner block is unnecessary. In that case the outer scheme can be recovered while using only this one inner share in the role of p; see Proposition 5.3.

Second, we use Martin's contraction construction [4]. Choose an outer coalition A that is forbidden without p but qualified after p is added. Conditioning the composite scheme on the shares of A leaves, on the inner participants, a valid scheme for Δ whose shares are no larger than the corresponding inner shares of the composite. Thus an inner scheme can also be extracted directly. See Lemma 5.1 and Proposition 5.2 for details.

The two constructions do not by themselves solve the reverse problem because their normalization factors need not match. If the outer construction needs a share of normalized size a at p, then the inner block must contain a times an inner convec in order to substitute that inner scheme back into the outer one. The elementary inner construction guarantees only one normalized copy. Schematically, if the best outer construction currently visible needs $a = 3$ while the inner extraction certifies only scale 1, recovering the two schemes separately is not enough to obtain (2) with $r = 1$. The central issue is therefore not the existence of outer and inner schemes, but whether they can be chosen with compatible scales.

A universal one-half factor. There is another simple outer construction that improves this mismatch in a different way. Split the role of p into the two cases "qualified without p" and "qualified after adding p," extract a scheme for each case from the composite, and combine them. In the resulting outer scheme, participant p has information ratio 1, while every untouched outer share is enlarged by at most a factor 2. Together with an inner convec dominated by the inner coordinates of c, this yields $r = 1/2$, proved in Section 5.

1.3 Simultaneous reversal and the critical Csirmaz factor

For a fixed composite convec c, let $\rho(c)$ denote the largest factor r for which (2) is possible.

A tempting first guess is that the reverse decomposition loses nothing:

$$\rho(c) = 1 \qquad \text{for every composite convec } c. \tag{3}$$

This exact statement is false. Section 8 gives a counterexample already in the multilinear class whose reverse-substitution factor is exactly $8/9$; the composite convec itself is, more strongly, scalar-linearly realizable over every finite field.

The universal factor $1/2$ can be applied successively when several participants are replaced. If I consists of k replaced participants, reversing them one at a time yields

$$\rho_I(c) \geq 2^{-k}, \tag{4}$$

where $\rho_I(c)$ is the largest factor achievable by reversing all substitutions at I simultaneously.

We next consider a recursive family built from Csirmaz's classical access structures [5]. For every k, Csirmaz's construction provides an access structure $\mathcal{C}_k$ with a distinguished set I_k of k participants satisfying

$$\sum_{p \in I_k} x_p \geq 2^k - 1 \qquad \text{for every convec } x \text{ of } \mathcal{C}_k. \tag{5}$$

Repeatedly substituting the preceding level into the participants of I_k gives an access structure $\Gamma_{k,\ell}$ at recursion depth ℓ. Let r_k denote the largest number such that every level of this recursion admits simultaneous reverse factor at least r_k^k. Combining this reverse factor with the distinguished-set bound in (5), the recursive lifting bound of Theorem 3.4 shows that each recursive step multiplies the contribution lower bound by $(2^k-1)r_k^k$. At the baseline value $r_k = 1/2$, this factor is $1-2^{-k} < 1$, so this lower-bound mechanism does not amplify the contribution lower bound from one level to the next. At each recursive level, the number of participants grows by a factor k, whereas the contribution lower bound grows by a factor $(2^k-1)r_k^k$. Thus, after ℓ levels, writing $N = |P(\Gamma_{k,\ell})|$, the resulting lower bound on the average information ratio grows, up to constants depending on k, like

$$\left(\frac{(2^k-1)r_k^k}{k}\right)^{\ell} \asymp N^{\log_k((2^k-1)r_k^k)-1},$$

which is superlinear in N precisely when

$$(2^k-1)r_k^k > k^2.$$

Equivalently, the critical value is

$$r_k^\star := \left(\frac{k^2}{2^k-1}\right)^{1/k} = \frac{1}{2} + \frac{\log k}{k} + O\left(\frac{(\log k)^2}{k^2}\right), \tag{6}$$

where log denotes the natural logarithm. Thus the main question is not merely whether $r_k > 1/2$; it is whether r_k is large enough to cross the critical value, which lies about $(\log k)/k$ above one half.

We conjecture that it does: for some constant $\eta > 1$ and all sufficiently large k,

$$r_k \geq \frac{1}{2} + \eta\frac{\log k}{k}. \tag{7}$$

This would already give superlinear information-ratio lower bounds. More generally, if $k(r_k - 1/2)/\log k$ is unbounded, then the exponents supplied by these recursive families are unbounded, giving a route to superpolynomial lower bounds. A fixed gap $r_k \geq 1/2 + \delta$ is a stronger sufficient condition and yields the explicit bound

$$N^{\Omega(\log N/\log\log N)}.$$

We also analyze the same recursive family after replacing entropic functions by arbitrary polymatroids satisfying only the Shannon inequalities. In this Shannon-polymatroid relaxation, if r_k^{Sh} denotes the corresponding factor that works at every recursion depth, then we prove

$$r_k^{\mathrm{Sh}} \leq r_k^{\star}.$$

Consequently, any proof that crosses (6) must use constraints beyond the Shannon inequalities. The upper bound $r_k^{\mathrm{Sh}} \leq r_k^{\star}$ is forced by Csirmaz's $O(N)$ upper bound on the information ratio in this Shannon-polymatroid relaxation. Whether this bound is attained by the recursive Csirmaz family remains open; if equality holds for any fixed k, the corresponding recursion already has average information ratio $\Omega(N)$.

1.4 What is proved

Universal half-bound and pointwise gap. Theorem 3.1 gives the universal single-participant bound

$$\rho(c) \geq \frac{1}{2}.$$

For every fixed composite convec the inequality is strict (Theorem 6.4). Corollary 6.7 strengthens this observation along the Csirmaz recursion: at every fixed k and finite depth, the k-th root of the guaranteed simultaneous factor is strictly larger than $1/2$. The unresolved issue is whether this excess above $1/2$ persists uniformly with depth and is large enough to cross the critical value (6).

Necessary properties of a near-half sequence. Section 6 introduces two quantities tailored to the single-participant problem. The *minimum outer scale* μ (Definition 6.1) is the smallest contribution required at the replaced outer participant when the untouched outer coordinates are fixed. The *inner capacity* κ (Definition 6.3) is the largest scaling of an inner convec that can fit inside the replacing block. In Section 6.4, we prove that

$$\rho(c_n) \longrightarrow \frac{1}{2} \quad \Longrightarrow \quad \mu_n \longrightarrow \infty, \qquad \frac{\kappa_n}{\mu_n} \longrightarrow 0.$$

Thus a family approaching one half must exhibit an increasingly severe mismatch between the outer scale that has to be replaced and the inner capacity available inside the composite convec.

Anchoring and inner capacity. Section 7 first shows that the infimum of the reverse factor is unchanged if one restricts to inner access structures containing a participant that is qualified by itself (called an anchor). It then characterizes the inner capacity supported by the remaining inner participants in terms of *weighted information ratios*, a weighted variant of the average information ratio. Thus, a uniform lower bound keeping this inner capacity a fixed positive fraction of the minimum outer scale would imply a uniform reverse gap above $1/2$.

The Shannon-polymatroid relaxation. In this relaxation, where entropic functions are replaced by arbitrary polymatroids satisfying only the Shannon inequalities, the universal single-participant reverse factor $1/2$ is best possible (Theorem 7.4). For the recursive Csirmaz family, the reverse

factor that can be certified at every recursion depth is bounded above by $r_k^\star$, the same value that marks the threshold for superlinear growth. Thus any proof that the reverse factor exceeds $r_k^\star$, and hence yields a superlinear lower bound for this recursion, must use constraints beyond the Shannon inequalities.

1.5 Preliminary versions and organization

Preliminary forms of the convec-set viewpoint, substitution, and the recursive lifting method appeared in the unpublished IACR Cryptology ePrint reports [23, 24]. The present paper is self-contained and supersedes those reports; no definition or result from them is assumed here.

Section 2 establishes the secret-sharing framework and the forward construction. Section 3 develops the general reverse-substitution and recursive-lifting machinery. Section 4 applies that machinery to Csirmaz access structures, identifies the critical reverse factor, and derives superlinear and superpolynomial consequences from quantitative bounds on that factor. Section 5 proves the unconditional single-participant one-half bound. Section 6 develops the minimum outer scale and inner capacity and proves pointwise strictness. Section 7 studies anchoring, weighted information ratios, and the Shannon barrier. Section 8 gives the 8/9 counterexample to exact reversal, and Section 9 records the remaining open problems.

2 Preliminaries, substitution, and the forward construction

This section recalls perfect secret sharing and convecs, defines the convec regions, and establishes their basic properties. We also show that every participant admits a unit-share realization (Lemma 2.1), and review substitution and the standard forward construction (Proposition 2.2).

2.1 Access structures and perfect secret sharing

Let P be a finite set of participants. An *access structure* on P is an upward-closed family $\Gamma \subseteq 2^P$ with $\varnothing \notin \Gamma$; Γ may be empty. We write $P(\Gamma)$ for the participant set of Γ. Members of Γ are *qualified*; the remaining subsets are *forbidden*. A participant p is *important*, or *non-dummy*, if some forbidden set becomes qualified after p is added. A participant that is not important is called *dummy*.

A *secret-sharing scheme* (SSS) on P is a tuple

$$\Pi = (S, (X_i)_{i \in P})$$

of jointly distributed discrete random variables with finite supports and $H(S) > 0$.

An SSS Π is said to be a *perfect* scheme for Γ, or to *perfectly realize* Γ, if

$$\begin{aligned} H(S \mid X_A) &= 0 && (\forall A \in \Gamma), \\ H(S \mid X_A) &= H(S) && (\forall A \notin \Gamma), \end{aligned}$$

where $X_A = (X_i)_{i \in A}$. The first condition is reconstruction and the second is perfect privacy. Throughout the paper, SSS means perfect secret sharing.

2.2 Information ratios and convec sets

The vector $x = (x_i)_{i \in P}$ is the *contribution vector* of Π, abbreviated *convec*, where

$$x_i = \frac{H(X_i)}{H(S)}$$

is the *information ratio* of participant i in Π.

The set of all convecs of perfect schemes for Γ is denoted by $\Sigma(\Gamma)$. Its Euclidean closure

$$\overline{\Sigma}(\Gamma) := \overline{\Sigma(\Gamma)} \subseteq \mathbb{R}^P_{\geq 0}$$

is called the *closed convec set* of Γ. Working with the closure avoids repeatedly distinguishing attained convecs from limiting ones.

The average and maximum information ratios of an access structure Γ on N participants can be expressed directly in terms of its closed convec set:

$$\widetilde{\sigma}(\Gamma) = \min_{x \in \overline{\Sigma}(\Gamma)} \frac{1}{N} \sum_{i \in P(\Gamma)} x_i,$$

and

$$\sigma(\Gamma) = \min_{x \in \overline{\Sigma}(\Gamma)} \max_{i \in P(\Gamma)} x_i.$$

The secret may be taken uniform without changing $\Sigma(\Gamma)$; see, for example, [6]. If $\Gamma = \varnothing$, then

$$\Sigma(\Gamma) = \mathbb{R}^P_{\geq 0}.$$

If every participant of Γ is important, then

$$\Sigma(\Gamma) \subseteq \mathbb{R}^P_{\geq 1}.$$

The closed convec set is nonempty, convex, and coordinatewise upward closed. We will use these properties repeatedly below.

2.3 Linear schemes and a lemma

Fix a finite field $\mathbb{F}$. A *multilinear secret-sharing scheme over* $\mathbb{F}$ [18] has a secret S uniformly distributed over $\mathbb{F}^d$, for some $d \geq 1$, and independent randomness R uniformly distributed over $\mathbb{F}^m$, for some $m \geq 0$. Each participant i receives a share

$$X_i = L_i(S, R) \in \mathbb{F}^{d_i},$$

where $L_i : \mathbb{F}^{d+m} \to \mathbb{F}^{d_i}$ is a surjective linear map. The information ratio of participant i is d_i/d. The case $d = 1$ is called *scalar-linear*.

For $P = R \sqcup \{p\}$, define

$$\Gamma_0 := \{A \subseteq R : A \in \Gamma\}, \qquad \Gamma_1 := \{A \subseteq R : A \cup \{p\} \in \Gamma\}. \tag{8}$$

Then $\Gamma_0 \subseteq \Gamma_1$. The family Γ_0 is an access structure, possibly empty. If $\{p\} \notin \Gamma$, then Γ_1 is also an access structure.

The next lemma shows that any prescribed participant can have information ratio one.

Lemma 2.1 (Unit information ratio for a prescribed participant)**.** *Let Γ be an access structure on $P = R \sqcup \{p\}$. Then Γ admits a perfect scheme with convec x satisfying*

$$x_p = 1.$$

More precisely, if $\{p\} \in \Gamma$, any perfect scheme for Γ_0 in (8) extends to a perfect scheme for Γ by giving p the secret itself. If $\{p\} \notin \Gamma$ and Γ_0, Γ_1 in (8) admit perfect schemes whose secrets are

uniform on the same finite alphabet, with convecs $u^{(0)}$ and $u^{(1)}$, respectively, then Γ admits a perfect scheme with convec

$$(x_R, x_p) = (u^{(0)} + u^{(1)}, 1).$$

If the component schemes are multilinear (respectively, scalar-linear) over the same finite field, then so is the resulting scheme.

Proof. Suppose first that $\{p\} \in \Gamma$. Take any perfect scheme for Γ_0 with secret S, and give p the secret itself. Coalitions containing p reconstruct S, while coalitions contained in R have exactly the reconstruction and privacy properties prescribed by Γ_0. Thus the resulting scheme realizes Γ and has $x_p = 1$.

Now suppose that $\{p\} \notin \Gamma$. Take the two schemes in the statement independently, with uniform secrets S and Y on the same finite alphabet, and equip this alphabet with an abelian-group structure. Give participant p the share

$$S - Y,$$

and give each $r \in R$ the pair

$$(X_r^{(0)}, X_r^{(1)}).$$

If $A \subseteq R$ is qualified in Γ, then $A \in \Gamma_0$ and reconstructs S from the first component. If $A \cup \{p\}$ is qualified, then $A \in \Gamma_1$, so A reconstructs Y from the second component and hence reconstructs S from Y and $S - Y$. For privacy, let first $A \subseteq R$ be forbidden in Γ. Then $A \notin \Gamma_0$, so $X_A^{(0)}$ is independent of S. Since the two component schemes are independent,

$$(X_A^{(0)}, X_A^{(1)}) \perp S.$$

If $A \cup \{p\}$ is forbidden, then $A \notin \Gamma_1$ and, since $\Gamma_0 \subseteq \Gamma_1$, also $A \notin \Gamma_0$. Hence

$$(X_A^{(0)}, X_A^{(1)}) \perp (S, Y).$$

Moreover, because S and Y are independent and uniform, $S - Y$ is independent of S. Therefore

$$(X_A^{(0)}, X_A^{(1)}, S - Y) \perp S,$$

so the scheme is perfect. Finally, $S-Y$ is uniform on the same alphabet as S, and the two component shares of each $r \in R$ are independent. Hence

$$x_p = 1, \qquad x_r = u_r^{(0)} + u_r^{(1)} \quad (r \in R).$$

The construction is scalar-linear (respectively, multilinear) whenever the two component schemes are so over the same field. In the multilinear case, independent repetitions may first be used to equalize their secret dimensions; in the scalar-linear case, both secret dimensions are already one. □

2.4 Substitution of access structures and vectors

We first define substitution for access structures and for convecs. Section 2.5 then shows that the resulting vector formula is exactly the one produced by a natural forward construction. Let Γ be an access structure on $P = R \sqcup \{p\}$ and let $\Delta \neq \varnothing$ be an access structure on a disjoint participant set Q. Following Martin [4], the substitution

$$\Omega = \Gamma[p \leftarrow \Delta]$$

is the access structure on $R \sqcup Q$ defined by

$$A \cup B \in \Omega \quad \Longleftrightarrow \quad A \in \Gamma \text{ or } (A \cup \{p\} \in \Gamma \text{ and } B \in \Delta), \tag{9}$$

for $A \subseteq R$ and $B \subseteq Q$.

For $x \in \mathbb{R}^P_{\geq 0}$ and $y \in \mathbb{R}^Q_{\geq 0}$, define *vector substitution* by

$$x[p \leftarrow y] = (x_R, (x_p y_q)_{q \in Q}). \tag{10}$$

For sets $X \subseteq \mathbb{R}^P_{\geq 0}$ and $Y \subseteq \mathbb{R}^Q_{\geq 0}$, write

$$X[p \leftarrow Y] = \{x[p \leftarrow y] : x \in X,\ y \in Y\}.$$

The meaning of the factor x_p becomes clear from the forward construction in the next subsection.

2.5 The forward construction

The vector operation above is the contribution-vector form of Martin's forward insertion construction [4], subject only to a compatibility condition on the distribution of the intermediate share.

Proposition 2.2 (Compatible forward construction)**.** *Let*

$$\Pi_\Gamma = (S, (X_r)_{r \in R}, X_p)$$

be a perfect scheme for Γ*, with convec* x*. Let*

$$\Pi_\Delta = (T, (Y_q)_{q \in Q})$$

be a perfect scheme for Δ*, with convec* y*, and assume that* T *has the same distribution as* X_p*. Then there is a perfect scheme for* $\Gamma[p \leftarrow \Delta]$ *with convec*

$$c = x[p \leftarrow y]. \tag{11}$$

Proof. Run the outer scheme. Instead of giving X_p to participant p, use the conditional distribution of the inner scheme given $T = X_p$ to generate the inner shares $(Y_q)_{q \in Q}$. An outer coalition that was qualified without p still reconstructs from its unchanged shares. If it needed p, then a qualified inner coalition first reconstructs X_p and the outer reconstruction then applies. Privacy follows in the same two cases from perfect privacy of the outer and inner schemes.

The untouched coordinates remain x_R. Since $H(T) = H(X_p) = x_p H(S)$ and $H(Y_q) = y_q H(T)$, the normalized inner coordinates are $x_p y_q$. Hence the composite convec is exactly (11). □

The identity (11) is the basic upper-bound construction associated with substitution. In particular, whenever the outer share X_p and the inner secret can be chosen with the same distribution, the composite convec is read directly from the two factor convecs.

Distribution compatibility. Because a convec specifies only normalized share entropies, not the distribution of the intermediate share, Proposition 2.2 does not by itself imply the unconditional inclusion

$$\overline{\Sigma}(\Gamma)[p \leftarrow \overline{\Sigma}(\Delta)] \subseteq \overline{\Sigma}(\Gamma[p \leftarrow \Delta]). \tag{12}$$

This issue does not affect the reverse results below, which start from a given composite scheme.

3 Reverse substitution and recursive lifting

Section 2 defined substitution and the corresponding forward construction. We now ask to what extent an arbitrary scheme for the composite access structure can be decomposed back into schemes for its factors. We first quantify the reverse loss for one replaced participant, then for several replaced participants simultaneously, and finally iterate the simultaneous bound to obtain recursive lower bounds.

3.1 The reverse-substitution factor

Let

$$\Omega = \Gamma[p \leftarrow \Delta], \qquad P(\Gamma) = R \sqcup \{p\},$$

and let $c = (c_R, c_Q) \in \overline{\Sigma}(\Omega)$. Define the *reverse-substitution factor* by

$$\rho(c) = \sup\left\{ r \in (0,1] : \begin{array}{l} \exists x \in \overline{\Sigma}(\Gamma),\ \exists y \in \overline{\Sigma}(\Delta) \\ \text{such that } r\, x[p \leftarrow y] \le c \end{array} \right\}. \tag{13}$$

The inequality is coordinatewise. Thus $\rho(c) = 1$ means that c dominates a substituted convec $x[p \leftarrow y]$ with $x \in \overline{\Sigma}(\Gamma)$ and $y \in \overline{\Sigma}(\Delta)$, without any multiplicative loss.

For non-dummy p, every $x \in \overline{\Sigma}(\Gamma)$ has $x_p \ge 1$; hence, by coordinatewise upward closure, exact domination is equivalent to exact representation: if $x[p \leftarrow y] \le c$, then after increasing the untouched coordinates of x to c_R and the coordinates of y to c_Q/x_p, one obtains $x' \in \overline{\Sigma}(\Gamma)$ and $y' \in \overline{\Sigma}(\Delta)$ with $c = x'[p \leftarrow y']$. It is therefore tempting to expect the reverse of (12), namely

$$\overline{\Sigma}(\Gamma[p \leftarrow \Delta]) \subseteq \overline{\Sigma}(\Gamma)[p \leftarrow \overline{\Sigma}(\Delta)].$$

This is false: Theorem 8.1 gives a scalar-linear composite convec with reverse-substitution factor $8/9$. Nevertheless, a factor of one half is always attainable. The following theorem is proved in Section 5.

Theorem 3.1 (Universal one-half bound)**.** *Assume that p is non-dummy in Γ, and let*

$$c = (c_R, c_Q) \in \overline{\Sigma}(\Gamma[p \leftarrow \Delta]).$$

There exist $x \in \overline{\Sigma}(\Gamma)$ and $y \in \overline{\Sigma}(\Delta)$ such that

$$x_p = 1, \qquad x_r \le 2c_r \quad (r \in R), \qquad y_q \le c_q \quad (q \in Q).$$

Consequently,

$$\rho(c) \ge \frac{1}{2}.$$

The definition of the reverse factor may also be restricted to a specified class of secret-sharing schemes, such as multilinear schemes over a fixed field. Unless a class is explicitly specified, we consider the unrestricted class of secret-sharing schemes.

3.2 Reversing multiple substitutions

The preceding subsection concerns substitution at a single participant. We now allow several outer participants to be replaced simultaneously. Let

$$I = \{p_1, \dots, p_k\} \subseteq P(\Gamma),$$

and, for each $p_i \in I$, let Δ_i be an access structure on a participant set disjoint from $P(\Gamma)$ and from the participant sets of the other Δ_j. We write

$$\Omega = \Gamma[I \leftarrow (\Delta_i)_{i\in I}]$$

for the access structure obtained by replacing each p_i by Δ_i. Simultaneous vector substitution is defined by performing the corresponding coordinate replacements at all participants in I.

Definition 3.2 (Simultaneous reverse factor)**.** For

$$c \in \overline{\Sigma}(\Gamma[I \leftarrow (\Delta_i)_{i\in I}]),$$

define the *simultaneous reverse factor*

$$\rho_I(c) = \sup\left\{ r \in (0,1] : \begin{array}{l} \exists x \in \overline{\Sigma}(\Gamma),\ \exists y^{(i)} \in \overline{\Sigma}(\Delta_i)\ (i \in I) \\ \text{such that } r\, x[I \leftarrow (y^{(i)})_{i\in I}] \le c \end{array} \right\}. \tag{14}$$

Thus $\rho_I(c)$ is the total factor for the simultaneous substitution; in particular, for $I = \{p\}$ it agrees with the single-participant factor $\rho(c)$.

To compare the simultaneous factor with the single-participant factors, fix an ordering $p_1, \ldots, p_k$ of I. For $i = 1, \ldots, k$, let

$$\Gamma^{(i)} = \Gamma[\{p_{i+1}, \ldots, p_k\} \leftarrow (\Delta_j)_{j=i+1}^{k}], \qquad \Omega^{(i)} = \Gamma^{(i)}[p_i \leftarrow \Delta_i]. \tag{15}$$

With $\Gamma^{(k)} = \Gamma$, we have $\Omega^{(1)} = \Omega$ and $\Omega^{(i)} = \Gamma^{(i-1)}$ for $i \ge 2$.

Proposition 3.3 (Sequential reversal)**.** *Let $\Gamma^{(i)}$ and $\Omega^{(i)}$ be as defined in* (15)*. Assume that, for each $i = 1, \ldots, k$, every $c \in \overline{\Sigma}(\Omega^{(i)})$ has reverse factor at least r with respect to*

$$\Omega^{(i)} = \Gamma^{(i)}[p_i \leftarrow \Delta_i],$$

for some $0 < r \le 1$. Then every $c \in \overline{\Sigma}(\Omega)$ has simultaneous reverse factor at least r^k, that is,

$$\rho_I(c) \ge r^k.$$

If p_i is dummy in the relevant outer access structure, reversing the substitution at p_i incurs no loss; if p_i is non-dummy, Theorem 3.1 gives reverse factor at least $1/2$. Hence Proposition 3.3 gives

$$\rho_I(c) \ge 2^{-k}. \tag{16}$$

Proof. Let $c^{(1)} = c \in \overline{\Sigma}(\Omega^{(1)})$. By the hypothesis for $i = 1$, there are $c^{(2)} \in \overline{\Sigma}(\Gamma^{(1)}) = \overline{\Sigma}(\Omega^{(2)})$ and $y_1 \in \overline{\Sigma}(\Delta_1)$ such that

$$r\, c^{(2)}[p_1 \leftarrow y_1] \le c^{(1)}.$$

Applying the hypothesis successively gives, for $i = 1, \ldots, k$, convecs

$$c^{(i+1)} \in \overline{\Sigma}(\Gamma^{(i)})$$

and $y_i \in \overline{\Sigma}(\Delta_i)$ such that

$$r\, c^{(i+1)}[p_i \leftarrow y_i] \le c^{(i)},$$

where $c^{(k+1)} \in \overline{\Sigma}(\Gamma^{(k)}) = \overline{\Sigma}(\Gamma)$.

Since vector substitution preserves coordinatewise inequalities, combining these inequalities yields

$$r^k\, c^{(k+1)}[I \leftarrow (y_i)_{i\in I}] \le c.$$

Hence

$$\rho_I(c) \ge r^k.$$

□

3.3 Recursive lifting

Proposition 3.3 controls one simultaneous substitution. We now iterate the same operation. Two quantities must be tracked through the recursion: the number of participants and the total contribution forced on the deepest substituted participants. We first derive the corresponding estimates and then determine when they yield a superlinear lower bound on the average information ratio.

Theorem 3.4 (Recursive lifting)**.** *Let Γ be an access structure with n participants, and let $I \subseteq P(\Gamma)$ be a distinguished set with $k = |I| \geq 2$, consisting of non-dummy participants. Set*

$$t := \inf_{x \in \overline{\Sigma}(\Gamma)} \sum_{p \in I} x_p. \tag{17}$$

Starting from $\Gamma_0 = \Gamma$, recursively set

$$\Gamma_{\ell+1} = \Gamma[I \leftarrow \Gamma_\ell], \tag{18}$$

and for $\ell \geq 0$ let L_ℓ denote the depth-ℓ descendants of I in Γ_ℓ; thus $L_0 = I$. Set

$$\tau_\ell := \inf_{c \in \overline{\Sigma}(\Gamma_\ell)} \sum_{q \in L_\ell} c_q, \qquad N_\ell := |P(\Gamma_\ell)|.$$

Thus $\tau_0 = t$ and $N_0 = n$.

Suppose that, for some $0 < r \leq 1$, every $c \in \overline{\Sigma}(\Gamma_{\ell+1})$ has simultaneous reverse factor at least r^k with respect to the decomposition

$$\Gamma_{\ell+1} = \Gamma[I \leftarrow \Gamma_\ell]$$

for every $\ell \geq 0$. Then, for every $\ell \geq 0$,

$$\tau_\ell \geq t\,(tr^k)^\ell, \qquad N_\ell \leq 2nk^\ell.$$

Consequently, for every $\ell \geq 0$,

$$\widetilde{\sigma}(\Gamma_\ell) \geq \frac{t}{2n} \left(\frac{tr^k}{k} \right)^\ell. \tag{19}$$

Proof. One recursive level retains the $n - k$ outer participants outside I and introduces k disjoint copies of Γ_ℓ, so

$$N_{\ell+1} = n - k + kN_\ell. \tag{20}$$

For the contribution recurrence, fix $\ell \geq 0$ and $c \in \overline{\Sigma}(\Gamma_{\ell+1})$, and let $\lambda < r^k$. By hypothesis, there are $x \in \overline{\Sigma}(\Gamma)$ and $y^{(p)} \in \overline{\Sigma}(\Gamma_\ell)$ for $p \in I$ such that

$$\lambda\, x[I \leftarrow (y^{(p)})_{p \in I}] \leq c.$$

Within the copy of Γ_ℓ replacing p, the descendants in $L_{\ell+1}$ form a copy of L_ℓ. Hence

$$\begin{aligned} \sum_{q \in L_{\ell+1}} c_q &\geq \lambda \sum_{p \in I} x_p \sum_{q \in L_\ell} y_q^{(p)} \\ &\geq \lambda\, t\, \tau_\ell. \end{aligned}$$

Taking the infimum over c and then letting $\lambda \uparrow r^k$ gives

$$\tau_{\ell+1} \geq t\, r^k \tau_\ell. \tag{21}$$

Since $\tau_0 = t$, iteration yields

$$\tau_\ell \geq t\,(tr^k)^\ell.$$

Solving (20), with $N_0 = n$, gives

$$N_\ell = k^\ell n + (n-k)\frac{k^\ell - 1}{k-1} \leq 2nk^\ell.$$

Finally,

$$\widetilde{\sigma}(\Gamma_\ell) \geq \frac{\tau_\ell}{N_\ell},$$

which gives (19). □

Corollary 3.5 (Superlinear lower-bound criterion)**.** *Under the hypotheses of Theorem 3.4, assume $t > 0$ and set*

$$a := \frac{\log(tr^k)}{\log k}.$$

If $a > 1$, then, for every $\ell \geq 0$,

$$\widetilde{\sigma}(\Gamma_\ell) \geq \frac{t}{(2n)^a}\, N_\ell^{a-1}. \tag{22}$$

In particular, this lower bound is superlinear in N_ℓ precisely when

$$tr^k > k^2. \tag{23}$$

Proof. Since $tr^k = k^a$, (19) gives

$$\widetilde{\sigma}(\Gamma_\ell) \geq \frac{t}{2n}\, k^{(a-1)\ell}.$$

When $a > 1$, the bound $N_\ell \leq 2nk^\ell$ from Theorem 3.4 therefore yields (22). Finally,

$$a - 1 > 1 \quad\Longleftrightarrow\quad a > 2 \quad\Longleftrightarrow\quad tr^k > k^2.$$

□

4 Recursive substitution of Csirmaz access structures

We apply the recursive lifting theorem to the Csirmaz access structures and determine the reverse-factor threshold for superlinear growth.

4.1 The Csirmaz family and its lifting parameters

For every $k \geq 2$, let $\mathcal{C}_k$ be the Csirmaz access structure described in Appendix A. It has

$$n_k = 2^k + k - 2$$

participants and a distinguished set I_k of size k satisfying

$$t_k := \inf_{x \in \overline{\Sigma}(\mathcal{C}_k)} \sum_{p \in I_k} x_p = 2^k - 1. \tag{24}$$

The lower bound is Csirmaz's distinguished-set inequality [5, Lemma 3.4], and the matching upper bound follows from Proposition A.1.

4.2 The recursive family and its reverse factor

We now specialize the recursion (18) of Section 3 to the Csirmaz family $\mathcal{C}_k$ of Section 4.1, substituting at the distinguished set I_k. For fixed k, define

$$\Gamma_{k,1} = \mathcal{C}_k, \qquad \Gamma_{k,\ell+1} = \mathcal{C}_k[I_k \leftarrow \Gamma_{k,\ell}] \quad (\ell \geq 1). \tag{25}$$

By (16), every $c \in \overline{\Sigma}(\Gamma_{k,\ell+1})$ has simultaneous reverse factor

$$\rho_{I_k}(c) \geq 2^{-k}$$

with respect to

$$\Gamma_{k,\ell+1} = \mathcal{C}_k[I_k \leftarrow \Gamma_{k,\ell}].$$

For each recursion depth $\ell \geq 1$, define

$$r_{k,\ell} := \inf_{c \in \overline{\Sigma}(\Gamma_{k,\ell+1})} \rho_{I_k}(c)^{1/k}, \qquad r_k := \inf_{\ell \geq 1} r_{k,\ell}. \tag{26}$$

Thus $r_{k,\ell}$ is the infimum of the k-th root of the reverse factor among convecs at recursion depth $\ell + 1$, while r_k is a lower bound that applies at every recursion depth. Hence,

$$r_{k,\ell} \geq \frac{1}{2}, \qquad r_k \geq \frac{1}{2}. \tag{27}$$

4.3 The critical reverse factor and a conjecture for the Csirmaz family

Section 4.2 defined r_k as a reverse factor that applies at every depth of the recursion (25). Combining this with the distinguished-set bound $t_k = 2^k - 1$ in (24), Corollary 3.5 gives the threshold at which the resulting lower bound on the average information ratio becomes superlinear.

Proposition 4.1 (Threshold for a superlinear lower bound)**.** *Fix $k \geq 2$ and put*

$$r_k^\star := \left(\frac{k^2}{2^k - 1}\right)^{1/k} = \frac{1}{2} + \frac{\log k}{k} + O\left(\frac{(\log k)^2}{k^2}\right). \tag{28}$$

If $r_k > r_k^\star$, then there exists $\varepsilon_k > 0$ such that the recursive family $(\Gamma_{k,\ell})_{\ell \geq 1}$ defined in (25) satisfies

$$\widetilde{\sigma}(\Gamma_{k,\ell}) = \Omega_k\Big(|P(\Gamma_{k,\ell})|^{1+\varepsilon_k}\Big) \qquad (\ell \to \infty). \tag{29}$$

Consequently, the maximum information ratio satisfies the same superlinear lower bound.

Proof. By Corollary 3.5, with $t = 2^k - 1$ and $r = r_k$, put

$$a_k := \frac{\log((2^k - 1) r_k^k)}{\log k}.$$

If $r_k > r_k^\star$, then

$$(2^k - 1) r_k^k > k^2,$$

so $a_k > 2$. Setting

$$\varepsilon_k := a_k - 2 > 0,$$

Corollary 3.5 gives

$$\widetilde{\sigma}(\Gamma_{k,\ell}) \geq \frac{2^k - 1}{(2n_k)^{a_k}} N_{k,\ell}^{1+\varepsilon_k}, \qquad N_{k,\ell} := |P(\Gamma_{k,\ell})|.$$

Since k is fixed, this is

$$\widetilde{\sigma}(\Gamma_{k,\ell}) = \Omega_k\Big(N_{k,\ell}^{1+\varepsilon_k}\Big) \qquad (\ell \to \infty).$$

Finally,

$$r_k^\star = \frac{1}{2} \exp\left(\frac{2\log k - \log(1 - 2^{-k})}{k}\right),$$

and the expansion in (28) follows. □

The expansion in (28) shows that the critical excess above one half is on the scale $(\log k)/k$. In particular, for every fixed $\eta > 1$,

$$\frac{1}{2} + \eta \frac{\log k}{k} > r_k^\star$$

for all sufficiently large k. This motivates the following conjecture.

Conjecture 4.2 (A conjecture for the Csirmaz family)**.** For the recursive Csirmaz family $(\Gamma_{k,\ell})$ defined in (25), there exist constants $\eta > 1$ and k_0 such that, for every $k \geq k_0$,

$$r_k \geq \frac{1}{2} + \eta \frac{\log k}{k}. \tag{30}$$

Equivalently, for every $k \geq k_0$, every $\ell \geq 1$, and every $c \in \overline{\Sigma}(\Gamma_{k,\ell+1})$,

$$\rho_{I_k}(c) \geq \left(\frac{1}{2} + \eta \frac{\log k}{k}\right)^k.$$

4.4 Reverse-factor gaps above one half and superpolynomial lower bounds

For the recursive Csirmaz family (25), stronger gaps of r_k above one half yield superpolynomial lower bounds. To obtain a one-parameter family, we let k vary and choose, for suitable k, a recursion depth ℓ sufficiently large.

Corollary 4.3 (Sufficient conditions for superpolynomial lower bounds)**.** *Let $(\Gamma_{k,\ell})$ be the recursive Csirmaz family defined in* (25)*, and let r_k be as defined in* (26)*. If*

$$\limsup_{k\to\infty} \frac{k(r_k - 1/2)}{\log k} = \infty,$$

then there exist $k_j \to \infty$ and recursion depths $\ell_j \geq 1$ such that, with

$$\Lambda_j := \Gamma_{k_j,\ell_j}, \qquad N_j := |P(\Lambda_j)|,$$

we have $N_j \to \infty$ and

$$\widetilde{\sigma}(\Lambda_j) \geq N_j^{\omega(1)}.$$

In particular, if

$$r_k \geq \frac{1}{2} + \delta$$

for some constant $\delta > 0$ and all sufficiently large k, then one may take

$$\Lambda_k := \Gamma_{k,\,1+\lfloor k/\log k\rfloor}.$$

Writing $N_k := |P(\Lambda_k)|$, this family satisfies

$$\widetilde{\sigma}(\Lambda_k) \geq N_k^{\Omega_\delta(\log N_k/\log\log N_k)}.$$

In both cases, the maximum information ratio satisfies the same lower bound.

Proof. Choose $k_j \to \infty$ such that

$$\frac{k_j(r_{k_j} - 1/2)}{\log k_j} \longrightarrow \infty,$$

and put

$$\delta_j := r_{k_j} - \frac{1}{2}.$$

With

$$a_{k_j} := \frac{\log\!\left((2^{k_j}-1)r_{k_j}^{k_j}\right)}{\log k_j},$$

we have

$$a_{k_j} = \frac{k_j \log(1+2\delta_j) + \log(1-2^{-k_j})}{\log k_j}.$$

Since $0 \leq \delta_j \leq 1/2$ and $\log(1+2\delta) \geq \delta$ on this interval,

$$a_{k_j} \geq \frac{k_j\delta_j}{\log k_j} + o(1) \longrightarrow \infty.$$

Corollary 3.5, with $t = 2^{k_j} - 1$, gives

$$\widetilde{\sigma}(\Gamma_{k_j,\ell}) \geq \frac{2^{k_j}-1}{(2n_{k_j})^{a_{k_j}}} N_{k_j,\ell}^{a_{k_j}-1}, \qquad N_{k_j,\ell} := |P(\Gamma_{k_j,\ell})|.$$

For each j, the prefactor is positive and independent of ℓ. Since $N_{k_j,\ell} \to \infty$ as $\ell \to \infty$, choose ℓ_j large enough that

$$\frac{2^{k_j}-1}{(2n_{k_j})^{a_{k_j}}} \geq N_{k_j,\ell_j}^{-1}.$$

Increasing ℓ_j if necessary, we may also assume that $N_{k_j,\ell_j} \to \infty$. Set

$$\Lambda_j := \Gamma_{k_j,\ell_j}, \qquad N_j := |P(\Lambda_j)|.$$

Then

$$\widetilde{\sigma}(\Lambda_j) \geq N_j^{a_{k_j}-2} = N_j^{\omega(1)}.$$

For the second assertion, suppose that

$$r_k \geq \frac{1}{2} + \delta$$

for all sufficiently large k, and set

$$\ell_k = 1 + \left\lfloor \frac{k}{\log k} \right\rfloor, \qquad \Lambda_k := \Gamma_{k,\ell_k}, \qquad N_k := |P(\Lambda_k)|.$$

Since

$$n_k = 2^k + k - 2,$$

Theorem 3.4 gives

$$n_k \le N_k \le 2n_k k^{\ell_k - 1},$$

and hence

$$\log N_k = \Theta(k).$$

Moreover,

$$\begin{aligned}\log\left(\frac{(2^k-1)r_k^k}{k}\right) &= k\log(2r_k) - \log k + \log(1-2^{-k}) \\ &= \Omega_\delta(k).\end{aligned}$$

Theorem 3.4, with $t = 2^k - 1$, therefore gives

$$\widetilde{\sigma}(\Lambda_k) \ge \frac{2^k-1}{2n_k}\left(\frac{(2^k-1)r_k^k}{k}\right)^{\ell_k-1}.$$

Since $(2^k-1)/(2n_k) = \Theta(1)$ and $\ell_k - 1 = \Theta(k/\log k)$,

$$\log\widetilde{\sigma}(\Lambda_k) \ge \Omega_\delta\left(\frac{k^2}{\log k}\right).$$

As $\log N_k = \Theta(k)$,

$$\widetilde{\sigma}(\Lambda_k) \ge N_k^{\Omega_\delta(\log N_k/\log\log N_k)}.$$

The maximum information ratio is at least the average information ratio. □

Optimality of the Csirmaz distinguished-set bound. For every access structure Λ and every set $I \subseteq P(\Lambda)$, Proposition A.1 gives

$$\inf_{x\in\overline{\Sigma}(\Lambda)} \sum_{p\in I} x_p \le 2^{|I|} - 1.$$

The Csirmaz access structure $\mathcal{C}_k$ attains equality for its distinguished set I_k. Thus the Csirmaz family gives the largest possible distinguished-set bound available to the recursive lifting theorem.

5 Proof of the universal one-half bound (Theorem 3.1)

Fix

$$\Omega = \Gamma[p \leftarrow \Delta], \qquad c = (c_R, c_Q) \in \overline{\Sigma}(\Omega),$$

with p non-dummy in Γ. We prove that every such composite convec has reverse factor at least $1/2$.

Section 5.1 directly extracts inner and outer convecs from the composite convec, but their relative scales need not be compatible with reverse substitution. Section 5.2 replaces the extracted outer convec by one with p-coordinate one, increasing each untouched outer coordinate by at most a factor of two. Together with the extracted inner convec, this gives

$$\rho(c) \ge \frac{1}{2}.$$

5.1 Direct extraction of the inner and outer convecs

We first use Martin's contraction construction [4], expressed here in terms of convecs. Conditioning on a forbidden coalition produces a scheme for the contracted access structure on the remaining participants without increasing any remaining contribution. This will give the inner convec; the outer convec will then be obtained by grouping the entire replacing block.

Lemma 5.1 (Contraction bound)**.** *Let Λ be an access structure on P, let $T \subseteq P$ be forbidden, and let*

$$\Lambda/T = \{A \subseteq P \setminus T : A \cup T \in \Lambda\}.$$

If $c \in \Sigma(\Lambda)$, then there is a vector $d \in \overline{\Sigma}(\Lambda/T)$ satisfying

$$d_i \le c_i \qquad (i \in P \setminus T).$$

The same statement holds when $c \in \overline{\Sigma}(\Lambda)$.

Proof. Consider first a scheme $(S, (X_i))$ with convec c. Because T is forbidden, S is independent of X_T. For each value t in the support of X_T, the conditional distribution given $X_T = t$ therefore has the same secret distribution. It is a perfect scheme for Λ/T: reconstruction and privacy follow directly from the corresponding properties of $A \cup T$ in the original scheme.

Let $d(t)$ be the convec of the conditional scheme. Convexity of $\overline{\Sigma}(\Lambda/T)$ implies that the average vector $d = \mathbb{E}[d(X_T)]$ belongs to $\overline{\Sigma}(\Lambda/T)$. Moreover,

$$d_i = \frac{H(X_i \mid X_T)}{H(S)} \le \frac{H(X_i)}{H(S)} = c_i.$$

The closed-region statement follows by approximation. □

We apply the contraction bound to the composite scheme to extract an inner convec.

Proposition 5.2 (Extracting the inner scheme)**.** *Assume that p is non-dummy in Γ, and let*

$$c = (c_R, c_Q) \in \overline{\Sigma}(\Gamma[p \leftarrow \Delta]).$$

Then there exists $y \in \overline{\Sigma}(\Delta)$ such that

$$y \le c_Q. \tag{31}$$

Proof. Since p is non-dummy, there exists $A \subseteq R$ with $A \notin \Gamma$ and $A \cup \{p\} \in \Gamma$. Conditioning on the shares of A induces exactly Δ on the inner participants. Lemma 5.1 therefore gives an inner convec $y \in \overline{\Sigma}(\Delta)$ with $y \le c_Q$. □

We next extract an outer convec directly from the same composite scheme. The idea is to regard the entire replacing block as the share of p. This preserves the untouched outer coordinates exactly, while the p-coordinate becomes the normalized entropy of the entire replacing block.

Proposition 5.3 (Grouping the inner block)**.** *Let $\Pi_\Omega = (S, (X_r)_{r\in R}, (Y_q)_{q\in Q})$ be a scheme for $\Omega = \Gamma[p \leftarrow \Delta]$ with convec $c = (c_R, c_Q)$. Then*

$$\Pi_\Gamma = (S, (X_r)_{r\in R}, X_p), \qquad X_p := Y_Q = (Y_q)_{q\in Q},$$

is a scheme for Γ, with convec (c_R, a), where

$$a = \frac{H(Y_Q)}{H(S)} \le \sum_{q\in Q} c_q.$$

Consequently, for every $c = (c_R, c_Q) \in \overline{\Sigma}(\Omega)$ there is a point $(c_R, a) \in \overline{\Sigma}(\Gamma)$ with $a \le \sum_{q\in Q} c_q$.

Proof. If $A \subseteq R$ is qualified without p, then X_A reconstructs S in Π_Ω. If $A \cup \{p\}$ is qualified, then $A \cup Q$ is qualified in Ω, so (X_A, Y_Q) reconstructs S. If $A \cup \{p\}$ is forbidden, $A \cup Q$ is forbidden in Ω, and (X_A, Y_Q) is independent of S. Coalitions forbidden without p inherit privacy from Π_Ω. This proves that Π_Γ is perfect. Subadditivity gives the displayed bound on a.

For a closed-region convec c, take schemes with convecs converging to c. The bounds on their p-coordinates give a convergent subsequence, whose limit lies in $\overline{\Sigma}(\Gamma)$. □

Anchored inner structures. If Δ has a singleton-qualified participant a, then Y_a can be used in place of the entire tuple Y_Q in the construction above. Section 7.1 uses this observation to show that, in minimizing the reverse factor, it suffices to consider anchored inner access structures.

5.2 Constructing a compatible outer convec

Propositions 5.2 and 5.3 give convecs

$$y \le c_Q, \qquad x = (c_R, a) \in \overline{\Sigma}(\Gamma),$$

but their scales need not be compatible with reverse substitution, since the substituted inner block is ay.

We avoid this mismatch by constructing instead an outer convec with p-coordinate one, while increasing each untouched outer coordinate by at most a factor of two. Together with $y \le c_Q$, this yields the reverse factor $1/2$.

Proof of Theorem 3.1. By Proposition 5.2, there is already an inner convec $y \in \overline{\Sigma}(\Delta)$ with $y \le c_Q$. Thus it remains to construct an outer convec $x \in \overline{\Sigma}(\Gamma)$ satisfying

$$x_p = 1, \qquad x_R \le 2c_R.$$

Once such an x is obtained,

$$\frac{1}{2} x[p \leftarrow y] \le c,$$

and hence $\rho(c) \ge 1/2$.

Recall Γ_0 and Γ_1 defined in (8). Restriction of the composite to R realizes Γ_0, so Γ_0 has a convec at most c_R. If $\{p\} \notin \Gamma$, choose any qualified inner coalition $B \in \Delta$. Then B itself is forbidden in the composite, and conditioning on B induces Γ_1 on R. A second application of Lemma 5.1 therefore gives a Γ_1-convec at most c_R.

These are the two component convecs required by the construction of Lemma 2.1. At this stage, however, they have only been obtained as points of the closed convec regions; Lemma 2.1 requires actual schemes whose secrets are uniform on the same finite alphabet. Appendix D shows that the two bounds can be approximated simultaneously by such compatible schemes. Applying Lemma 2.1 and passing to the limit then gives $x_p = 1$ and $x_R \le 2c_R$.

If $\{p\} \in \Gamma$, this compatibility issue does not arise: every coalition containing p is qualified. Give p the secret itself and use the restricted Γ_0 scheme on R. Then $x_p = 1$ and in fact $x_R \le c_R$.

This completes the construction of the required outer convec and proves the theorem. □

6 Outer scale and inner capacity

Let

$$\Omega = \Gamma[p \leftarrow \Delta], \qquad c = (c_R, c_Q) \in \overline{\Sigma}(\Omega).$$

The only loss in Theorem 3.1 comes from enlarging the untouched outer coordinates from c_R to at most $2c_R$. To improve on the factor $1/2$, we keep these coordinates fixed at c_R and measure two quantities: the smallest p-coordinate compatible with c_R, and the largest scaling of an inner convec that fits below c_Q. Their interaction determines how far the reverse factor can exceed $1/2$.

6.1 The minimum outer scale

Proposition 5.3 shows that there is an outer convec of the form (c_R, a). We minimize its p-coordinate while keeping the coordinates on R fixed at c_R.

Definition 6.1 (Minimum outer scale)**.** For $u_R \in \mathbb{R}^R_{\geq 0}$, define

$$\mu_\Gamma(u_R) = \inf\{t \geq 0 : (u_R, t) \in \overline{\Sigma}(\Gamma)\}. \tag{32}$$

For the composite vector c, write

$$\mu = \mu_\Gamma(c_R).$$

The value μ is finite by Proposition 5.3; in fact $\mu \leq \sum_{q \in Q} c_q$.

The minimum outer scale also gives a lower bound on each important coordinate of the replacing block.

Proposition 6.2 (Inner-coordinate lower bound)**.** *For every important inner participant q,*

$$c_q \geq \mu_\Gamma(c_R) = \mu. \tag{33}$$

Proof. Choose $B \subseteq Q \setminus \{q\}$ with $B \notin \Delta$ and $B \cup \{q\} \in \Delta$. The coalition B is forbidden in the composite. After conditioning on B and restricting to $R \cup \{q\}$, the induced access structure is Γ, with q in the role of p. By Lemma 5.1, this gives an outer convec whose untouched coordinates are at most c_R and whose substituted coordinate is at most c_q. Upward closure on the untouched coordinates then gives $\mu_\Gamma(c_R) \leq c_q$. □

6.2 The inner capacity

Proposition 5.2 gives an inner convec $y \in \overline{\Sigma}(\Delta)$ with $y \leq c_Q$, so unit scale is always feasible. We now ask for the largest scale at which an inner convec can still fit below c_Q.

Definition 6.3 (Inner capacity)**.** For $v_Q \in \mathbb{R}^Q_{\geq 0}$, define

$$\kappa_\Delta(v_Q) = \sup\{t \geq 0 : \exists y \in \overline{\Sigma}(\Delta) \text{ with } ty \leq v_Q\}. \tag{34}$$

For the composite vector c, write

$$\kappa = \kappa_\Delta(c_Q).$$

Proposition 5.2 gives $\kappa \geq 1$. Thus μ measures the outer scale required when the untouched coordinates are fixed, while κ measures the inner capacity supported by the replacing block.

6.3 Improving the reverse factor using outer scale and inner capacity

The quantities μ and κ measure, respectively, the outer scale required at p when the coordinates on R are fixed at c_R, and the inner scale supported by c_Q. If $\kappa \geq \mu$, these two scales are compatible and exact reverse domination is possible. The remaining case is $1 \leq \kappa < \mu$. There, Theorem 3.1 provides the outer point $(2c_R, 1)$, while the definition of μ provides (c_R, μ). Interpolating between these two points until the p-coordinate reaches κ gives the following bound.

Theorem 6.4 (Reverse factor strictly greater than one half)**.** *Assume that p is non-dummy in Γ. Then every fixed composite convec c satisfies*

$$\rho(c) > \frac{1}{2}.$$

More precisely, $\mu \geq 1$ and $\kappa \geq 1$. If $\kappa \geq \mu$, then

$$\rho(c) = 1.$$

Otherwise, $1 \leq \kappa < \mu$, and

$$\rho(c) \geq \frac{\mu + \kappa - 1}{2\mu - 1} = \frac{1}{2} + \frac{2\kappa - 1}{2(2\mu - 1)}. \tag{35}$$

Proof. Because p is non-dummy, there is a forbidden coalition A such that $A \cup \{p\}$ is qualified. For every outer scheme,

$$H(X_p) \geq I(S; X_p \mid X_A) = H(S),$$

so every outer convec has p-coordinate at least one and hence $\mu \geq 1$. Proposition 5.2 gives $\kappa \geq 1$.

The minimum in the definition of μ is attained because $\overline{\Sigma}(\Gamma)$ is closed. Likewise, the feasible scales in the definition of κ form a downward-closed set whose positive endpoint is attained: if $t_j \to t > 0$ and $t_j y^{(j)} \leq c_Q$, then the vectors $y^{(j)}$ are bounded, and closedness of $\overline{\Sigma}(\Delta)$ gives a limiting feasible convec. Hence, if $\kappa \geq \mu$, there are $(c_R, \mu) \in \overline{\Sigma}(\Gamma)$ and $y \in \overline{\Sigma}(\Delta)$ with $\mu y \leq c_Q$. Thus

$$(c_R, \mu)[p \leftarrow y] \leq c,$$

so $\rho(c) = 1$.

It remains to consider $1 \leq \kappa < \mu$. By Theorem 3.1 and upward closure, $(2c_R, 1) \in \overline{\Sigma}(\Gamma)$, while $(c_R, \mu) \in \overline{\Sigma}(\Gamma)$. For $0 \leq \theta \leq 1$, convexity gives

$$\big((2 - \theta)c_R,\ 1 + \theta(\mu - 1)\big) \in \overline{\Sigma}(\Gamma).$$

Choose $y \in \overline{\Sigma}(\Delta)$ with $\kappa y \leq c_Q$. A factor λ is feasible whenever

$$\lambda \leq \frac{1}{2 - \theta}, \qquad \lambda \leq \frac{\kappa}{1 + \theta(\mu - 1)}.$$

Equating the two bounds gives

$$\theta = \frac{2\kappa - 1}{\mu + \kappa - 1}$$

and the common value in (35). Strictness follows from $\kappa \geq 1$ and $\mu < \infty$. □

6.4 Families approaching one half

For each fixed composite, Theorem 6.4 gives a strict gap above $1/2$. To understand whether such a gap can hold uniformly, we examine sequences whose reverse factors approach $1/2$. The next corollary shows that this can happen only if the minimum outer scale diverges while the inner capacity becomes negligible relative to it.

Corollary 6.5 (Necessary conditions for a near-half sequence)**.** *Let*

$$\Omega_n = \Gamma_n[p_n \leftarrow \Delta_n], \qquad c_n = (c_{R_n}, c_{Q_n}) \in \overline{\Sigma}(\Omega_n),$$

where p_n is non-dummy in Γ_n. Put

$$\mu_n = \mu_{\Gamma_n}(c_{R_n}), \qquad \kappa_n = \kappa_{\Delta_n}(c_{Q_n}).$$

If

$$\rho(c_n) \longrightarrow \frac{1}{2},$$

then

$$\mu_n \longrightarrow \infty, \qquad \frac{\kappa_n}{\mu_n} \longrightarrow 0.$$

Proof. The correction term in (35) is at least $1/(2(2\mu_n - 1))$, so $\mu_n \to \infty$. Dividing the first expression in (35) by μ_n shows that a positive lower limit of κ_n/μ_n would keep $\rho(c_n)$ uniformly above $1/2$. □

The next theorem shows that the reverse factor cannot approach $1/2$ while the inner access structure remains fixed.

Theorem 6.6 (Fixed-inner gap)**.** *Fix an access structure Δ on Q, after deleting its dummy participants. For every access structure Γ, every non-dummy participant $p \in P(\Gamma)$, and every*

$$c = (c_R, c_Q) \in \overline{\Sigma}(\Gamma[p \leftarrow \Delta]),$$

one has

$$\kappa_\Delta(c_Q) \geq \max\left\{1, \frac{\mu_\Gamma(c_R)}{\sigma(\Delta)}\right\}, \qquad \rho(c) \geq \frac{\sigma(\Delta)}{2\sigma(\Delta) - 1} > \frac{1}{2}. \tag{36}$$

Consequently, any sequence with $\rho(c_n) \to 1/2$ satisfies $\sigma(\Delta_n) \to \infty$.

Proof. By Proposition 6.2, every important inner coordinate satisfies $c_q \geq \mu$. Choose $y \in \overline{\Sigma}(\Delta)$ with $\max_q y_q$ arbitrarily close to $\sigma(\Delta)$. Then $(\mu/\sigma(\Delta))y \leq c_Q$ up to an arbitrarily small endpoint error, so $\kappa \geq \mu/\sigma(\Delta)$. Combine this with $\kappa \geq 1$ and Theorem 6.4. The worst value over μ occurs when the two lower bounds meet, at $\mu = \sigma(\Delta)$. □

The fixed-inner gap has a useful consequence for the recursive Csirmaz family of Section 4.2. For every fixed k and finite depth ℓ, the inner access structure $\Gamma_{k,\ell}$ is fixed, with maximum information ratio $\sigma(\Gamma_{k,\ell})$. Hence Theorem 6.6 gives a strict reverse gap above $1/2$ at every finite depth.

Corollary 6.7 (Uniform gap at each fixed Csirmaz depth)**.** *Let $(\Gamma_{k,\ell})$ be the recursive Csirmaz family defined in* (25)*, and let $r_{k,\ell}$ and r_k be as defined in* (26)*. For every fixed $k \geq 2$ and $\ell \geq 1$,*

$$r_{k,\ell} \geq \frac{\sigma(\Gamma_{k,\ell})}{2\sigma(\Gamma_{k,\ell}) - 1} > \frac{1}{2}. \tag{37}$$

Consequently, if $r_k = 1/2$ for some fixed k, then there exists a sequence $\ell_j \to \infty$ such that

$$r_{k,\ell_j} \longrightarrow \frac{1}{2}.$$

Proof. At each step of a sequential reversal of

$$\Gamma_{k,\ell+1} = \mathcal{C}_k[I_k \leftarrow \Gamma_{k,\ell}],$$

the inner structure is a copy of $\Gamma_{k,\ell}$. Theorem 6.6 therefore gives the single-participant factor

$$\frac{\sigma(\Gamma_{k,\ell})}{2\sigma(\Gamma_{k,\ell}) - 1}$$

at every step. Proposition 3.3 gives the k-th power of this factor for simultaneous reversal. Taking the k-th root and then the infimum over c proves (37).

If $r_k = 1/2$, then by the definition of r_k there is a sequence of depths ℓ_j such that

$$r_{k,\ell_j} \longrightarrow \frac{1}{2}.$$

Since (37) gives $r_{k,\ell} > 1/2$ for every fixed ℓ, this sequence may be chosen with $\ell_j \to \infty$. □

When the inner structure is nearly ideal, i.e., its maximum information ratio is one, Theorem 6.6 already gives exact reverse factorization, or equivalently, reverse factor one. The same conclusion holds when the outer structure is ideal, as follows from the more general bound below.

Corollary 6.8 (Exact reverse factorization with a nearly-ideal factor)**.** *Let $\Omega = \Gamma[p \leftarrow \Delta]$, where p is non-dummy in Γ. For every $c \in \overline{\Sigma}(\Omega)$,*

$$\rho(c) \geq \max\left\{\frac{1}{2}, \frac{1}{\sigma(\Gamma)}\right\}. \tag{38}$$

In particular, $\rho(c) = 1$ if either Γ or Δ is nearly ideal.

Proof. Every important participant $r \neq p$ of Γ remains important after substitution. Indeed, let A be forbidden in Γ with $A \cup \{r\}$ qualified. If $p \notin A$, the same witness works in the composite. If $p \in A$, replace p by any qualified inner coalition. Hence every normalized composite convec satisfies $c_r \geq 1$ for important untouched r.

Fix $\varepsilon > 0$ and choose $x \in \overline{\Sigma}(\Gamma)$ with every important coordinate at most $\sigma(\Gamma) + \varepsilon$; dummy coordinates may be taken to be zero. Proposition 5.2 gives $y \in \overline{\Sigma}(\Delta)$ with $y \leq c_Q$. Since $x_p \leq \sigma(\Gamma) + \varepsilon$,

$$\frac{1}{\sigma(\Gamma) + \varepsilon}\, x[p \leftarrow y] \leq c.$$

Letting $\varepsilon \downarrow 0$ and combining with Theorem 3.1 proves (38). If Γ is nearly ideal, then $\sigma(\Gamma) = 1$, so (38) gives $\rho(c) = 1$. If Δ is nearly ideal, then $\sigma(\Delta) = 1$, and Theorem 6.6 also gives $\rho(c) = 1$. □

7 Inner capacity and the Shannon barrier

Corollary 6.5 shows that any sequence of composite convecs with reverse factors tending to $1/2$ must satisfy

$$\mu \to \infty, \qquad \frac{\kappa}{\mu} \to 0.$$

This section studies whether these two necessary conditions can occur. We first show that the infimum of the reverse factor over all substitutions and composite convecs is unchanged if the inner

access structure is required to contain a singleton-qualified participant. For such anchored inner structures, we then characterize the inner capacity in terms of a weighted variant of the information ratio of the inner access structure; see (43). Finally, returning to the critical reverse factor $r_k^\star$ of Proposition 4.1, we show that, in the Shannon-polymatroid relaxation, the depth-uniform reverse factor for the recursive Csirmaz family is at most $r_k^\star$. Hence Shannon inequalities alone cannot prove a depth-uniform reverse factor exceeding $r_k^\star$, which is required for a superlinear lower bound on the average, and hence maximum, information ratio of the recursive Csirmaz family.

7.1 Anchoring without changing the minimum reverse factor

We begin by adjoining to the inner structure a new participant a that is qualified by itself. Define the anchored structure $\Delta + a$ on $Q \cup \{a\}$ by

$$\Delta + a = \{B \subseteq Q \cup \{a\} : a \in B \text{ or } B \cap Q \in \Delta\}. \tag{39}$$

Since $\{a\}$ is qualified, its share alone can be used as the p-share in the grouping construction of Proposition 5.3. Hence, for every

$$\widetilde{c} = (c_R, c_a, c_Q) \in \overline{\Sigma}(\Gamma[p \leftarrow (\Delta + a)]),$$

we have

$$(c_R, c_a) \in \overline{\Sigma}(\Gamma), \qquad \mu_\Gamma(c_R) \le c_a. \tag{40}$$

Conversely, adjoining the inner secret itself as the share of a extends any scheme for Δ to a scheme for $\Delta + a$.

Lemma 7.1 (Inner capacity after anchoring)**.** *For every nonnegative vector (u_a, u_Q),*

$$\kappa_{\Delta+a}(u_a, u_Q) = \min\{u_a, \kappa_\Delta(u_Q)\}. \tag{41}$$

Proof. In every perfect scheme for $\Delta + a$, the singleton $\{a\}$ reconstructs the secret, so its normalized contribution is at least one. Restriction to Q is a perfect scheme for Δ. These facts give the upper bound. Conversely, adjoining to any perfect scheme for Δ an anchor equal to the secret gives a perfect scheme for $\Delta + a$; scaling and closure give the reverse inequality. □

Lemma 7.1 describes how anchoring changes the inner capacity. We now show that adjoining an anchor leaves the infimum of the reverse factor unchanged and that the same infimum is obtained after restricting to Pareto-minimal composite convecs, which we define next.

Pareto-minimal convecs. A convec $x \in \overline{\Sigma}(\Gamma)$ is *Pareto-minimal* if there is no $x' \in \overline{\Sigma}(\Gamma)$ with $x' \le x$ coordinatewise and $x' \ne x$.

Theorem 7.2 (Anchoring preserves the infimum reverse factor)**.** *Let*

$$\rho^* := \inf_{\Gamma,\Delta,p,c} \rho(c),$$

where the infimum ranges over all access structures Γ, Δ on disjoint participant sets, all non-dummy participants $p \in P(\Gamma)$, and all

$$c \in \overline{\Sigma}(\Gamma[p \leftarrow \Delta]).$$

Then the same value ρ^* is obtained if the infimum is restricted to substitutions whose inner access structure is anchored. The value is also unchanged if one further restricts to Pareto-minimal composite convecs.

Proof. First take an actual scheme $\Pi_\Omega = (S, X_R, Y_Q)$ for $\Gamma[p \leftarrow \Delta]$, with convec $c = (c_R, c_Q)$. Add an anchor with share $J_a = Y_Q$, the entire inner share tuple. The enlarged scheme realizes $\Gamma[p \leftarrow (\Delta + a)]$ and has convec $\widetilde{c} = (c_R, c_a, c_Q)$, where $c_a = H(Y_Q)/H(S)$.

Any reverse witness for $\widetilde{c}$ restricts on Q to a reverse witness for c, so $\rho(c) \geq \rho(\widetilde{c})$. Conversely, let $r < \rho(c)$ and choose $x \in \overline{\Sigma}(\Gamma)$ and $y \in \overline{\Sigma}(\Delta)$ with $r\, x[p \leftarrow y] \leq c$. Then $r x_p$ is feasible in the definition of $\kappa_\Delta(c_Q)$. Every feasible value in the definition of the inner capacity is at most each important coordinate of c_Q, while $c_a \geq c_q$ for every q; hence $r x_p \leq c_a$. Adjoin the inner secret as the anchor share to y, obtaining $y^a \in \overline{\Sigma}(\Delta + a)$ with $y^a_a = 1$. Then

$$r\, x[p \leftarrow y^a] \leq \widetilde{c}.$$

Thus $\rho(\widetilde{c}) \geq r$, and letting $r \uparrow \rho(c)$ proves equality. Approximation extends the argument to the closed regions.

Now fix an anchored vector $\widetilde{c}$. The set

$$\{d \in \overline{\Sigma}(\Gamma[p \leftarrow (\Delta + a)]) : d \leq \widetilde{c}\}$$

is nonempty and compact. A point minimizing the sum of the coordinates is Pareto-minimal. Decreasing the composite vector can only decrease the set of feasible reverse witnesses, so its value of ρ is at most that of $\widetilde{c}$. Taking infima proves the second assertion. □

7.2 Characterizing the inner capacity in terms of weighted information ratios

For an anchored composite $\widetilde{c} = (c_R, c_a, c_Q)$, put

$$\kappa = \kappa_\Delta(c_Q), \qquad \widetilde{\kappa} = \kappa_{\Delta+a}(c_a, c_Q), \qquad \mu = \mu_\Gamma(c_R).$$

Equations (40) and (41) give

$$\mu \leq c_a, \qquad \widetilde{\kappa} = \min\{c_a, \kappa\}.$$

Along any anchored sequence with reverse factor tending to $1/2$, Corollary 6.5 gives $\kappa/\mu \to 0$. Hence eventually

$$\kappa < \mu \leq c_a,$$

and therefore $\widetilde{\kappa} = \kappa$. Thus the quantity that must be controlled is the capacity $\kappa_\Delta(c_Q)$ supported by the non-anchor inner coordinates Q. To prevent

$$\frac{\kappa_\Delta(c_Q)}{\mu_\Gamma(c_R)}$$

from tending to zero, it would suffice to prove a uniform lower bound

$$\kappa_\Delta(c_Q) \geq \eta\, \mu_\Gamma(c_R) \tag{42}$$

for some $\eta > 0$.

We therefore characterize $\kappa_\Delta(c_Q)$ in terms of weighted information ratios of Δ. For a weight vector $w \in \mathbb{R}^Q_{\geq 0}$ with

$$\sum_{q \in Q} w_q = 1,$$

define

$$\sigma_w(\Delta) := \inf_{y \in \overline{\Sigma}(\Delta)} w \cdot y. \tag{43}$$

Thus $\sigma_w(\Delta)$ is the minimum weighted average information ratio of Δ under the weights w. For the uniform weight, it equals $\widetilde{\sigma}(\Delta)$.

Theorem 7.3 (Inner capacity from weighted information ratios)**.** *For every $c_Q \geq 0$,*

$$\kappa_\Delta(c_Q) = \inf_{\substack{w \geq 0,\ \sum_{q \in Q} w_q = 1 \\ \sigma_w(\Delta) > 0}} \frac{w \cdot c_Q}{\sigma_w(\Delta)}. \tag{44}$$

Proof. Write $K = \overline{\Sigma}(\Delta)$. Since K is upward closed,

$$\kappa_\Delta(c_Q) = \sup\{t \geq 0 : c_Q/t \in K\}.$$

If $c_Q/t \in K$, then for every $w \geq 0$ with $\sum_{q \in Q} w_q = 1$ and $\sigma_w(\Delta) > 0$,

$$\frac{w \cdot c_Q}{t} \geq \sigma_w(\Delta),$$

which gives one inequality in (44). Conversely, fix $t > 0$ smaller than the right-hand side. Then $w \cdot (c_Q/t) \geq \sigma_w(\Delta)$ for every $w \geq 0$ with $\sum_{q \in Q} w_q = 1$. By homogeneity, the same inequality holds for every nonnegative weight vector w. A closed convex upward set is the intersection of its supporting half-spaces with nonnegative normals: a separating normal with a negative coordinate would contradict upward closure. Hence $c_Q/t \in K$. Thus t is feasible, and taking the supremum proves equality. □

Suppose that, for some fixed $0 < \eta \leq 1$, every composite in a given class satisfies

$$w \cdot c_Q \geq \eta\, \mu\, \sigma_w(\Delta) \qquad \text{for every } w \geq 0 \text{ with } \sum_{q \in Q} w_q = 1 \text{ and } \sigma_w(\Delta) > 0. \tag{45}$$

By Theorem 7.3,

$$\kappa \geq \eta\mu.$$

Together with $\kappa \geq 1$, Theorem 6.4 then gives

$$\rho(c) \geq \frac{1}{2 - \eta} > \frac{1}{2}.$$

Thus a uniform weighted estimate of the form (45) is sufficient for a uniform reverse-factor gap above $1/2$.

7.3 The Shannon barrier

We now show that no uniform estimate of the form (45), and hence no uniform reverse-factor gap above $1/2$, can be obtained from Shannon inequalities alone.

The Shannon relaxation. Let Λ be an access structure on P, with dealer 0. Define $\overline{\Sigma}^{\mathrm{Sh}}(\Lambda)$ as the set of vectors

$$(h(\{i\}))_{i \in P},$$

where h is a nonnegative, monotone, submodular function on $\{0\} \cup P$ satisfying

$$h(\varnothing) = 0, \qquad h(\{0\}) = 1,$$

and, for every $A \subseteq P$,

$$h(A \cup \{0\}) - h(A) = \begin{cases} 0, & A \in \Lambda, \\ 1, & A \notin \Lambda. \end{cases}$$

We call these the normalized Shannon-polymatroid convecs; see, for example, [5, 13, 14].

Define $\rho^{\mathrm{Sh}}(c)$ as in (13), with $\overline{\Sigma}(\Gamma)$, $\overline{\Sigma}(\Delta)$, and $\overline{\Sigma}(\Gamma[p \leftarrow \Delta])$ replaced by their respective Shannon-polymatroid regions. For a simultaneous composite

$$\Omega = \Gamma[I \leftarrow (\Delta_i)_{i\in I}],$$

define $\rho_I^{\mathrm{Sh}}(c)$ analogously from (14).

Theorem 7.4 (Sharp Shannon threshold)**.** *For every substitution $\Omega = \Gamma[p \leftarrow \Delta]$ with p non-dummy and every $c \in \overline{\Sigma}^{\mathrm{Sh}}(\Omega)$,*

$$\rho^{\mathrm{Sh}}(c) \geq \frac{1}{2}.$$

Moreover,

$$\inf_{\Gamma,\Delta,p,c} \rho^{\mathrm{Sh}}(c) = \frac{1}{2},$$

where the infimum ranges over all such substitutions and composite Shannon-polymatroid convecs.

Proof. Restriction to a subset of elements and contraction by a forbidden coalition preserve the polymatroid axioms and the normalized perfectness equalities. As in the proof of Theorem 3.1, they give an inner Shannon convec $y \leq c_Q$ and two induced outer component convecs, each bounded by c_R. Lemma C.1 combines the two outer components into a Shannon-polymatroid convec x with

$$x_p = 1, \qquad x_R \leq 2c_R.$$

Hence $\frac{1}{2}x[p \leftarrow y] \leq c$, proving the lower bound.

Sharpness. Suppose that some $r > 1/2$ worked for all composite Shannon convecs. Sequential reversal applies to polymatroid convecs. The proof of Theorem 3.4 uses only simultaneous reverse domination, the distinguished-set inequality, and the participant recurrence, so the same recurrence applies in the Shannon-polymatroid model. Thus, for the Csirmaz recursion $\Gamma_{k,\ell}$,

$$\tau_{\ell+1}^{\mathrm{Sh}} \geq (2^k - 1)r^k \tau_\ell^{\mathrm{Sh}},$$

where τ_ℓ^{Sh} is the minimum total contribution on the depth-ℓ descendants of I_k over Shannon-polymatroid convecs of $\Gamma_{k,\ell}$. Choose k so large that

$$M_k := (2^k - 1)r^k > k^2.$$

Then

$$\tau_\ell^{\mathrm{Sh}} \geq (2^k - 1)M_k^{\ell-1}, \qquad N_{k,\ell} \leq 2n_k k^{\ell-1},$$

and therefore

$$\frac{\tau_\ell^{\mathrm{Sh}}}{N_{k,\ell}^2} \geq \frac{2^k - 1}{4n_k^2} \left(\frac{M_k}{k^2}\right)^{\ell-1} \longrightarrow \infty.$$

On the other hand, Csirmaz's Shannon-polymatroid construction [5, Theorem 3.5] supplies, for every access structure on N participants, a normalized Shannon-polymatroid function h satisfying $h(\{i\}) \leq N$ for every participant i, and hence

$$\sum_i h(\{i\}) \leq N^2.$$

Applied to $\Gamma_{k,\ell}$, this gives

$$\tau_\ell^{\mathrm{Sh}} \leq N_{k,\ell}^2,$$

contradicting the preceding conclusion that $\tau_\ell^{\mathrm{Sh}}/N_{k,\ell}^2 \to \infty$. □

7.4 Shannon bound for the depth-uniform Csirmaz reverse factor

Let $(\Gamma_{k,\ell})$ be the recursive Csirmaz family defined in (25). Theorem 7.4 rules out a universal improvement over $1/2$ in the Shannon relaxation. We now bound the reverse factor that can hold uniformly over all depths of this family.

The Shannon reverse factor. Define

$$r_k^{\mathrm{Sh}} := \inf_{\ell \geq 1} \inf_{c \in \overline{\Sigma}^{\mathrm{Sh}}(\Gamma_{k,\ell+1})} \rho_{I_k}^{\mathrm{Sh}}(c)^{1/k}. \tag{46}$$

Sequential application of Theorem 7.4 gives $r_k^{\mathrm{Sh}} \geq 1/2$. The next corollary gives the upper bound

$$r_k^{\mathrm{Sh}} \leq r_k^{\star}.$$

Corollary 7.5 (Shannon upper bound on the depth-uniform Csirmaz reverse factor)**.** *For every $k \geq 2$,*

$$\frac{1}{2} \leq r_k^{\mathrm{Sh}} \leq r_k^{\star} = \left(\frac{k^2}{2^k - 1}\right)^{1/k} = \frac{1}{2} + \frac{\log k}{k} + O\left(\frac{(\log k)^2}{k^2}\right). \tag{47}$$

Consequently, a Shannon-polymatroid lower bound of the form

$$r_k^{\mathrm{Sh}} \geq \frac{1}{2} + \gamma \frac{\log k}{k} + o\left(\frac{\log k}{k}\right)$$

requires $\gamma \leq 1$.

Proof. The lower bound follows from Theorem 7.4 and sequential reversal. For the upper bound, suppose $r_k^{\mathrm{Sh}} > r_k^{\star}$. Choose r with $r_k^{\star} < r < r_k^{\mathrm{Sh}}$. Then every depth and every Shannon-polymatroid convec in the recursion satisfies $\rho_{I_k}^{\mathrm{Sh}}(c) \geq r^k$. The proof of Proposition 4.1 uses only simultaneous reverse domination and the distinguished-set inequality, so it applies in the Shannon-polymatroid relaxation and forces a total contribution growing faster than $N_{k,\ell}^2$. This contradicts the bound $\sum_i h(\{i\}) \leq N_{k,\ell}^2$ supplied by Csirmaz's Shannon-polymatroid construction and used in the proof of Theorem 7.4. Hence $r_k^{\mathrm{Sh}} \leq r_k^{\star}$. The expansion is given in (28). □

In particular, the Shannon relaxation cannot establish Conjecture 4.2, whose coefficient satisfies $\eta > 1$. This raises the natural question whether the upper bound in (47) is attained, that is, whether

$$r_k^{\mathrm{Sh}} = r_k^{\star}$$

for the recursive Csirmaz family.

Bounds from non-Shannon inequalities. Beimel and Orlov showed that the non-Shannon information inequalities known at the time do not improve the $O(N^2)$ upper bound underlying Csirmaz's Shannon-polymatroid barrier [9]. More generally, Martín, Padró, and Yang proved that any family of rank inequalities involving at most r variables yields feasible normalized polymatroids satisfying

$$h(\{i\}) = O(N^{r-2})$$

for every participant i of an access structure on N participants [11, Theorem 6.2]. Consequently,

$$\sum_{i \in P} h(\{i\}) = O(N^{r-1}).$$

These results are instances of the following general consequence of the recursive lifting argument. Suppose that a relaxation $\mathcal{R}$ has the property that every access structure on N participants admits a feasible normalized polymatroid h with $\sum_{i\in P} h(\{i\}) = O(N^c)$, for some fixed c. If $r_k^{\mathcal{R}}$ denotes the corresponding depth-uniform reverse factor for the recursive Csirmaz family, then

$$(2^k - 1)(r_k^{\mathcal{R}})^k \le k^c,$$

and therefore

$$r_k^{\mathcal{R}} \le \left(\frac{k^c}{2^k - 1}\right)^{1/k} = \frac{1}{2} + \frac{c}{2}\frac{\log k}{k} + O_c\left(\frac{(\log k)^2}{k^2}\right).$$

Indeed, if $(2^k - 1)(r_k^{\mathcal{R}})^k > k^c$, the recursive lifting argument would force the total contribution of $\Gamma_{k,\ell}$ eventually to exceed $O(N_{k,\ell}^c)$.

For the Beimel–Orlov relaxations above, $c = 2$, so the resulting upper bound is exactly $r_k^\star$. For the bounded-variable rank inequalities treated by Martín, Padró, and Yang, one has $c = r - 1$. Thus no fixed bounded-variable relaxation of this kind can prove either

$$r_k^{\mathcal{R}} \ge \frac{1}{2} + \delta$$

for some constant $\delta > 0$ and all sufficiently large k, or

$$\limsup_{k\to\infty} \frac{k(r_k^{\mathcal{R}} - 1/2)}{\log k} = \infty.$$

Attainment of the Shannon upper bound. It remains open whether the recursive Csirmaz family attains the Shannon upper bound

$$r_k^{\mathrm{Sh}} = r_k^\star.$$

If equality holds, the recursive lifting theorem yields a linear lower bound on the average information ratio of the recursive Csirmaz family.

This would provide a second explicit route to linear information-ratio lower bounds from Shannon inequalities. Williamson recently obtained such a lower bound for a different explicit family of access structures, whose average and maximum information ratios are both linear in the number of participants [22].

Corollary 7.6 (Linear lower bound from attainment of the Shannon upper bound)**.** *Fix $k \ge 2$. If $r_k^{\mathrm{Sh}} = r_k^\star$, then, for every $\ell \ge 1$,*

$$\widetilde{\sigma}(\Gamma_{k,\ell}) \ge \frac{2^k - 1}{4(2^k + k - 2)^2}\, N_{k,\ell}.$$

In particular, the recursive Csirmaz family has average, and hence maximum, information ratio $\Omega_k(N_{k,\ell})$.

Proof. Put

$$t_k = 2^k - 1, \qquad n_k = 2^k + k - 2.$$

Equality $r_k^{\mathrm{Sh}} = r_k^\star$ implies that, at every recursion depth, the simultaneous Shannon reverse factor is at least $(r_k^\star)^k$. The proof of Corollary 3.5 uses only the participant and contribution recurrences and therefore applies to Shannon-polymatroid convecs. Since

$$t_k (r_k^\star)^k = k^2,$$

its $a = 2$ case gives

$$\inf_{c \in \overline{\Sigma}^{\mathrm{Sh}}(\Gamma_{k,\ell})} \frac{1}{N_{k,\ell}} \sum_{i \in P(\Gamma_{k,\ell})} c_i \geq \frac{t_k}{4n_k^2} N_{k,\ell}.$$

Every perfect secret-sharing convec is a Shannon-polymatroid convec, so the same lower bound holds for $\widetilde{\sigma}(\Gamma_{k,\ell})$. □

8 Failure of exact reverse substitution

Corollary 6.8 shows that the reverse factor is one whenever either the inner or the outer access structure is nearly ideal. In this section we show that exact reversal fails in general. More precisely, although the precise value of the universal minimum reverse factor ρ^* from Theorem 7.2 remains unknown, we prove that

$$\frac{1}{2} \leq \rho^* \leq \frac{8}{9}.$$

The lower bound follows from the universal one-half bound of Theorem 3.1. The upper bound is witnessed by a counterexample lying already in the multilinear class, whose composite convec is scalar-linearly realizable over every finite field.

Let

$$\Delta = q_1 q_2 + q_2 q_3 + q_1 q_3 q_4$$

be the second Csirmaz structure. Its convec region has two extreme points,

$$\alpha = (1, 2, 1, 1), \qquad \beta = (2, 1, 2, 1),$$

both of which are multilinearly realizable over every finite field. More precisely, β is scalar-linearly realizable over every finite field, whereas α is scalar-linearly realizable in odd characteristic and has a two-dimensional multilinear realization in characteristic 2; see Appendix B.

Let Γ be the relabeling of Δ to the participant set $\{o_1, o_2, p, o_4\}$:

$$\Gamma = o_1 o_2 + o_2 p + o_1 p o_4.$$

Let

$$\Delta^+ = \Delta + a$$

be the anchored extension of Δ obtained by adding the singleton-qualified participant a.

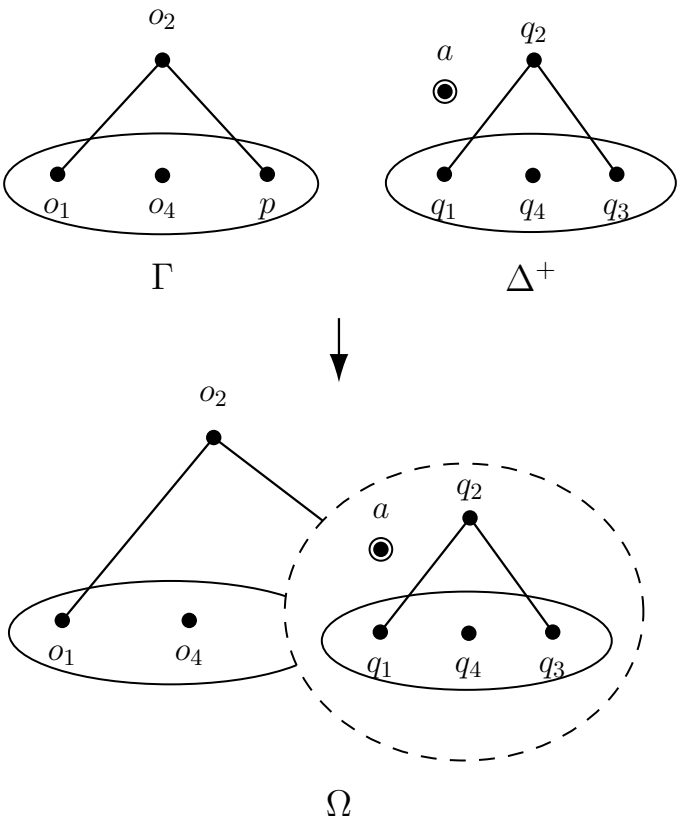

Figure 1: The exact-reversal counterexample. Minimal qualified sets are shown by hyperedges in Γ and Δ^+. The dashed boundary marks the inner copy Δ^+ replacing the outer participant p.

Csirmaz's lower bound for $\mathcal{C}_2$ shows that every contribution vector

$$(x_{o_1}, x_{o_2}, x_p, x_{o_4}) \in \overline{\Sigma}(\Gamma)$$

satisfies

$$x_{o_1} + x_{o_2} \geq 3, \qquad x_{o_2} + x_p \geq 3,$$

where the second inequality follows from the automorphism exchanging the first and third participants of $\mathcal{C}_2$.

Theorem 8.1 (Exact reversal fails)**.** *Let Γ and Δ^+ be the access structures shown in Figure 1. For the composite access structure*

$$\Omega = \Gamma[p \leftarrow \Delta^+],$$

we use the coordinate order

$$(o_1, o_2, o_4;\ a;\ q_1, q_2, q_3, q_4).$$

The vector

$$c^\star = (3, 1, 1;\ 2;\ 3, 2, 3, 2) \tag{48}$$

belongs to $\overline{\Sigma}(\Omega)$ and is realized by a scalar-linear perfect scheme over every finite field. Its reverse factor with respect to the substitution $\Omega = \Gamma[p \leftarrow \Delta^+]$ is

$$\rho(c^\star) = \frac{8}{9}. \tag{49}$$

Consequently, exact reverse substitution fails for Ω, even though the inner access structure Δ^+ is anchored and $c^\star$ is scalar-linearly realizable over every finite field.

Proof. The explicit scalar-linear realization of $c^\star$ is given in Appendix B. For the lower bound, set

$$x = \frac{1}{8}\alpha + \frac{7}{8}\beta = \left(\frac{15}{8}, \frac{9}{8}, \frac{15}{8}, 1\right),$$

and

$$y = \frac{1}{5}\alpha + \frac{4}{5}\beta = \left(\frac{9}{5}, \frac{6}{5}, \frac{9}{5}, 1\right), \qquad y^+ = (1; y).$$

By convexity and relabeling, $x \in \overline{\Sigma}(\Gamma)$ and $y \in \overline{\Sigma}(\Delta)$; adjoining the anchor gives $y^+ \in \overline{\Sigma}(\Delta^+)$. Directly,

$$\frac{8}{9}x[p \leftarrow y^+] = \left(\frac{5}{3}, 1, \frac{8}{9}; \frac{5}{3}; 3, 2, 3, \frac{5}{3}\right) \le c^\star,$$

so $\rho(c^\star) \ge 8/9$.

Conversely, suppose

$$r\, x'[p \leftarrow y'] \le c^\star, \qquad y' = (y'_a, y'_Q) \in \overline{\Sigma}(\Delta^+),$$

for arbitrary perfect outer and inner convecs. Restricting y' to q_1, q_2, q_3, q_4 gives $y'_Q \in \overline{\Sigma}(\Delta)$. The coordinate bound $c^\star_{o_2} = 1$ gives

$$r\, x'_{o_2} \le 1.$$

The bounds $c^\star_{q_2} = 2$ and $c^\star_{q_3} = 3$, together with the Csirmaz lower bound

$$y'_{q_2} + y'_{q_3} \ge 3 \qquad \text{for every } y'_Q \in \overline{\Sigma}(\Delta),$$

give

$$3r\, x'_p \le r\, x'_p(y'_{q_2} + y'_{q_3}) \le 5,$$

and hence

$$r x'_p \le \frac{5}{3}.$$

Similarly, the Csirmaz lower bound for the outer convec gives

$$x'_{o_2} + x'_p \ge 3.$$

Since $r x'_{o_2} \le 1$, it follows that

$$3r \le r x'_{o_2} + r x'_p \le 1 + \frac{5}{3} = \frac{8}{3}.$$

Therefore $r \le 8/9$.

□

We remark that the proof of Theorem 8.1 shows that exact reverse decomposition can fail even within the multilinear class and even when the inner access structure is anchored.

9 Conclusion and open problems

We introduced reverse substitution as a way to recover outer and inner convecs from a convec of a substituted access structure. Theorem 3.1 gives the universal factor $1/2$, Corollary 6.5 identifies the necessary conditions for this factor to be approached, and Theorem 3.4 relates simultaneous reverse factors to lower bounds under recursive substitution. Theorem 7.2 reduces the universal minimum reverse factor ρ^* to the anchored, Pareto-minimal setting, while Theorem 8.1 gives

$$\frac{1}{2} \le \rho^* \le \frac{8}{9}.$$

Its exact value remains open. In particular, it is unknown whether $\rho^* > 1/2$, equivalently, whether there exists an absolute $\delta > 0$ such that every single-participant substitution satisfies $\rho(c) \ge 1/2 + \delta$. For the recursive Csirmaz family, a second question is whether

$$\limsup_{k\to\infty} \frac{k(r_k - 1/2)}{\log k} = \infty.$$

By Corollary 4.3, a positive answer would yield superpolynomial lower bounds on the information ratio. Finally, Corollary 7.5 raises the question whether the Shannon upper bound is attained, that is, whether

$$r_k^{\mathrm{Sh}} = r_k^\star$$

for some, or for all sufficiently large, k. Determining the exact value of r_k^{Sh} would determine how far Shannon inequalities alone can push the recursive Csirmaz construction.

AI-use disclosure. Generative AI tools were used for mathematical discussion, including the development and expansion of ideas appearing in two earlier versions of this work [23, 24], and for language and editorial polishing. All mathematical claims, proofs, computations, citations, and final formulations were reviewed and verified by the author, who takes full responsibility for the contents of the paper.

A The Csirmaz family and the universal distinguished-set bound

Section 4 uses the explicit Csirmaz access structure $\mathcal{C}_k$ together with a universal upper bound for any prescribed set of k participants. We begin with the definition of $\mathcal{C}_k$, and then prove the upper bound.

Let

$$A = \{a_1, \dots, a_k\},$$

and enumerate the subsets of A as

$$A = A_0, A_1, \dots, A_{2^k-1} = \varnothing$$

so that $i < j$ implies $A_i \not\subseteq A_j$. Introduce participants $b_1, \dots, b_{2^k-2}$ and set

$$B_i = \{b_1, \dots, b_i\}, \qquad B_0 = \varnothing.$$

The Csirmaz access structure $\mathcal{C}_k$ has minimal qualified sets

$$A_i \cup B_i \qquad (0 \le i \le 2^k - 2),$$

and distinguished set

$$I_k = A.$$

Moreover,

$$B_i \cup A_{i+1}$$

is forbidden for every $0 \le i \le 2^k - 2$; see Csirmaz [5, proof of Theorem 3.2 and Lemma 3.3].

The following proposition gives the universal upper bound used together with Csirmaz's lower bound in Section 4.

Proposition A.1 (Universal $2^k - 1$ distinguished-set bound)**.** *Let Λ be an access structure, let*

$$I = (p_1, \dots, p_k)$$

be an ordering of k distinct participants, and let $\mathbb{F}$ be any finite field. Then Λ admits a perfect scalar-linear scheme over $\mathbb{F}$ such that

$$x_{p_i} = 2^{k-i}, \qquad i = 1, \dots, k.$$

Consequently,

$$\inf_{x \in \overline{\Sigma}(\Lambda)} \sum_{p \in I} x_p \le 2^k - 1. \tag{50}$$

Proof. We argue by induction on k. The case $k = 0$ is immediate. Let $p = p_k$.

Suppose first that $\{p\} \notin \Lambda$, and let Λ_0, Λ_1 be the two induced access structures defined in (8). Apply the induction hypothesis to each of them with the ordered set $(p_1, \dots, p_{k-1})$, using scalar-linear schemes over the same field $\mathbb{F}$. Lemma 2.1 combines these schemes into a scalar-linear scheme for Λ with

$$x_p = 1$$

and, for $i < k$,

$$x_{p_i} = 2^{k-1-i} + 2^{k-1-i} = 2^{k-i}.$$

Suppose now that $\{p\} \in \Lambda$. Give p the secret itself, and apply the induction hypothesis to the restriction of Λ to the remaining participants. For each $i < k$, append independent uniform randomness of the same dimension as the existing share of p_i. This preserves reconstruction and privacy and doubles its contribution, giving

$$x_p = 1, \qquad x_{p_i} = 2^{k-i} \quad (i < k).$$

Therefore

$$\sum_{i=1}^{k} x_{p_i} = 1 + 2 + \cdots + 2^{k-1} = 2^k - 1,$$

which proves (50). □

B Multilinear realizations used in the proof of Theorem 8.1

B.1 Extreme convecs of $\overline{\Sigma}(\mathcal{C}_2)$

Recall that $\mathcal{C}_2$ is the second member of the Csirmaz family. Its convec region $\overline{\Sigma}(\mathcal{C}_2)$ has the two extreme convecs

$$\alpha = (1, 2, 1, 1), \qquad \beta = (2, 1, 2, 1).$$

The proof of Theorem 8.1 uses rational convex combinations of these two convecs. We give explicit multilinear realizations of α and β over every finite field. All displayed secrets and random variables are independent and uniform over $\mathbb{F}$.

convec	field	shares
β	arbitrary	$S = s$, with r_1, r_2, r_3 random; $X_1 = (r_2, r_3)$, $X_2 = s + r_3$, $X_3 = (r_3, s + r_1 + r_2)$, $X_4 = r_1$.
α	odd characteristic	$S = s$, with r_1, r_2 random; $X_1 = s + r_1 - r_2$, $X_2 = (r_1 - s, r_2 - s)$, $X_3 = r_1 + r_2$, $X_4 = r_2 - s$.
α	characteristic 2	$S = (s_1, s_2)$, with r_1, r_2, r_3, r_4 random; $X_1 = (r_2 + r_3,\ s_1 + s_2 + r_1 + r_2)$; $X_2 = (r_1,\ s_1 + r_2 + r_3,\ r_3 + r_4,\ s_1 + r_1 + r_3)$; $X_3 = (s_1 + s_2 + r_1 + r_3 + r_4,\ s_1 + r_1 + r_2 + r_3 + r_4)$; $X_4 = (s_1 + r_3,\ s_1 + r_4)$.

Table 1: Explicit realizations of $\alpha = (1, 2, 1, 1)$ and $\beta = (2, 1, 2, 1)$, the extreme convecs of $\overline{\Sigma}(\mathcal{C}_2)$. In the characteristic-2 row the secret and share dimensions are 2 and $(2, 4, 2, 2)$, respectively, so the normalized convec is α.

For β, reconstruction is given by

$$12:\ X_2 - X_{1,2}, \qquad 23:\ X_2 - X_{3,1}, \qquad 134:\ X_{3,2} - X_{1,1} - X_4,$$

and privacy for $13, 14, 24, 34$, respectively, follows from the following shifts (in each case, the shift changes the secret while leaving all shares held by the corresponding coalition unchanged):

$$(s, r_1) += (t, -t), \qquad s += t, \qquad (s, r_3) += (t, -t), \qquad (s, r_2) += (t, -t).$$

For the odd-characteristic realization of α, reconstruction is given by

$$12:\ X_1 - X_{2,1} + X_{2,2}, \qquad 23:\ \tfrac{1}{2}(X_3 - X_{2,1} - X_{2,2}), \qquad 134:\ -X_1 + X_3 - 2X_4,$$

while privacy for $13, 14, 24, 34$ follows from the shifts

$$(2t, -t, t), \qquad (t, 0, t), \qquad (t, t, t), \qquad (t, -t, t)$$

in (s, r_1, r_2), respectively.

For the characteristic-2 realization of α, the two secret coordinates are reconstructed by

	s_1	s_2
12	$X_{1,1} + X_{2,2}$	$X_{1,1} + X_{1,2} + X_{2,4}$
23	$X_{2,2} + X_{2,3} + X_{2,4} + X_{3,2}$	$X_{2,1} + X_{2,2} + X_{2,4} + X_{3,1} + X_{3,2}$
134	$X_{1,1} + X_{1,2} + X_{3,1} + X_{4,2}$	$X_{1,2} + X_{3,2} + X_{4,1} + X_{4,2}$

and privacy is certified by adding t to the following variables, with all unlisted variables fixed:

	s_1-direction	s_2-direction
13	s_1, r_1	s_2, r_2, r_3
14	s_1, r_2, r_3, r_4	s_2, r_1
24	s_1, r_3, r_4	s_2
34	s_1, r_1, r_3, r_4	s_2, r_1, r_2

All coefficients in the last two displays lie in $\mathbb{F}_2$, so these reconstruction and privacy identities hold over every field of characteristic 2. Hence α and β are multilinearly realizable over every finite field.

Direct sums, after clearing denominators, realize every rational convex combination of α and β over the same field. In particular, the convecs x and y used in the proof of Theorem 8.1 are multilinearly realizable over every finite field.

B.2 A scalar-linear realization of $c^\star$

We now give, over an arbitrary finite field $\mathbb{F}$, an explicit scalar-linear perfect scheme for

$$\Omega = \Gamma[p \leftarrow \Delta^+]$$

with convec

$$c^\star = (3, 1, 1;\ 2;\ 3, 2, 3, 2).$$

This proves the realizability assertion in Theorem 8.1.

Take independent uniform field elements

$$s, r_1, r_2, r_3, r_4, r_1', r_2', r_3', r_4'$$

over $\mathbb{F}$, with secret $S = s$, and set

$$\begin{aligned}
X_{o_1} &= (r_1, r_4, s + r_1 + r_2 + r_3),\\
X_{o_2} &= s + r_1,\\
X_{o_4} &= r_2,\\
X_a &= (r_1, r_3),\\
X_{q_1} &= (r_1', r_2', r_3'),\\
X_{q_2} &= (r_1 + r_2' + r_3',\ r_1 + r_3 + r_1' + r_2' + r_4),\\
X_{q_3} &= (r_2' + r_3',\ r_1 + r_1' + r_2' + r_4,\ r_1 + r_3 + r_1' + r_4'),\\
X_{q_4} &= (r_4, r_4').
\end{aligned}$$

The resulting share dimensions are

$$(3, 1, 1;\ 2;\ 3, 2, 3, 2) = c^\star.$$

For reconstruction, denote the components of a vector share by subscripts. The following identities recover s from every minimal qualified coalition of Ω:

minimal qualified set	reconstruction of s
$o_1 o_2$	$-X_{o_1,1} + X_{o_2}$
$o_2 a$	$X_{o_2} - X_{a,1}$
$o_2 q_1 q_2$	$X_{o_2} + X_{q_1,2} + X_{q_1,3} - X_{q_2,1}$
$o_2 q_2 q_3$	$X_{o_2} - X_{q_2,1} + X_{q_3,1}$
$o_2 q_1 q_3 q_4$	$X_{o_2} + X_{q_1,1} + X_{q_1,2} - X_{q_3,2} + X_{q_4,1}$
$o_1 o_4 a$	$-X_{o_1,1} + X_{o_1,3} - X_{o_4} - X_{a,2}$
$o_1 o_4 q_1 q_2$	$X_{o_1,2} + X_{o_1,3} - X_{o_4} + X_{q_1,1} + X_{q_1,2} - X_{q_2,2}$
$o_1 o_4 q_2 q_3$	$-X_{o_1,1} + X_{o_1,3} - X_{o_4} - X_{q_2,2} + X_{q_3,2}$
$o_1 o_4 q_1 q_3 q_4$	$X_{o_1,3} - X_{o_4} + X_{q_1,1} - X_{q_3,3} + X_{q_4,2}$

For privacy it suffices to check the maximal forbidden coalitions. In each row below, simultaneously adding an arbitrary $t \in \mathbb{F}$ according to the displayed shifts changes the secret from s to $s+t$ while leaving every share held by the listed coalition unchanged. Since the underlying random variables are uniform, this proves perfect privacy over every finite field.

maximal forbidden set	nonzero shifts
$o_1o_4q_1q_3$	$s+=t,\ r_3-=t,\ r_4'+=t$
$o_1o_4q_1q_4$	$s+=t,\ r_3-=t$
$o_1o_4q_2q_4$	$s+=t,\ r_3-=t,\ r_1'+=t$
$o_1o_4q_3q_4$	$s+=t,\ r_3-=t,\ r_1'+=t,\ r_2'-=t,\ r_3'+=t$
$o_2o_4q_1q_3$	$s+=t,\ r_1-=t,\ r_3+=t,\ r_4+=t$
$o_2o_4q_1q_4$	$s+=t,\ r_1-=t$
$o_2o_4q_2q_4$	$s+=t,\ r_1-=t,\ r_2'+=t$
$o_2o_4q_3q_4$	$s+=t,\ r_1-=t,\ r_1'+=t$
$o_1q_1q_2q_3q_4a$	$s+=t,\ r_2-=t$
$o_4q_1q_2q_3q_4a$	$s+=t$

Thus the displayed scalar-linear scheme realizes Ω over every finite field and has convec $c^\star$.

C The unit-share construction in the Shannon relaxation

The proof of Theorem 7.4 requires the unit-share construction of Lemma 2.1 in the Shannon-polymatroid relaxation. The following lemma gives this extension.

Lemma C.1 (Unit-share construction for Shannon polymatroids)**.** *Let Γ be an access structure on $R \sqcup \{p\}$ with $\{p\} \notin \Gamma$, and let*

$$\Gamma_0 = \{A \subseteq R : A \in \Gamma\}, \qquad \Gamma_1 = \{A \subseteq R : A \cup \{p\} \in \Gamma\}.$$

If

$$u^{(0)} \in \overline{\Sigma}^{\mathrm{Sh}}(\Gamma_0), \qquad u^{(1)} \in \overline{\Sigma}^{\mathrm{Sh}}(\Gamma_1),$$

then there exists $x \in \overline{\Sigma}^{\mathrm{Sh}}(\Gamma)$ such that

$$x_p = 1, \qquad x_r = u_r^{(0)} + u_r^{(1)} \quad (r \in R).$$

Proof. Choose normalized Shannon polymatroids h_0, h_1 realizing the two component vectors, with independent rank-one secret elements s_0, s_1, and let H be their direct sum. Before grouping the two copies of each participant in R, adjoin a rank-one element p by defining

$$H(U \cup \{p\}) = \min\{H(U) + 1,\ H(U \cup \{s_0, s_1\})\}. \tag{51}$$

Set

$$g(U) = \min\{1, H(\{s_0, s_1\} \mid U)\},$$

so that

$$H(U \cup \{p\}) = H(U) + g(U).$$

The function g is nonincreasing under inclusion, and the perfectness equalities of the two components imply

$$g(U) \in \{0, 1\}.$$

We verify submodularity only in the cases involving p. If at most one of two sets contains p, ordinary submodularity of H, together with $g(U) \geq g(U \cup V)$, gives the required inequality. If both contain p, the only case not already implied by submodularity of H is

$$g(U) = g(V) = 0, \qquad g(U \cap V) = 1, \qquad g(U \cup V) = 0.$$

Then some s_i is spanned by both U and V but not by $U \cap V$. Applying submodularity of H to $U \cup \{s_i\}$ and $V \cup \{s_i\}$ gives

$$H(U) + H(V) \geq H(U \cap V) + 1 + H(U \cup V),$$

which supplies the required unit.

Monotonicity is similar. If

$$g(U) = 1, \qquad g(U \cup \{x\}) = 0,$$

then x spans some s_i not spanned by U, and therefore

$$H(U \cup \{x\}) \geq H(U \cup \{s_i\}) = H(U) + 1.$$

Thus (51) defines a monotone submodular extension.

It remains to verify the access structure with secret s_0. Put

$$a = h_0(s_0 \mid A_0), \qquad b = h_1(s_1 \mid A_1).$$

After adjoining p,

$$H(s_0 \mid A, p) = a + \min\{1, b\} - \min\{1, a + b\}.$$

Since $a, b \in \{0, 1\}$, this conditional rank is zero precisely when $A \in \Gamma_0$ or when $A \in \Gamma_1$ and p is present. Hence the resulting polymatroid realizes Γ. The singleton value of p is one, and grouping the two copies of each $r \in R$ gives

$$x_r = u_r^{(0)} + u_r^{(1)}.$$

□

D Common-secret realization of the extracted convecs

The proof of Theorem 3.1 extracts a Γ_0-convec and a Γ_1-convec, each bounded coordinatewise by c_R. To apply Lemma 2.1, these convecs must be approximated by actual schemes whose secrets are uniform on the same alphabet. We verify that compatibility here.

Retain the notation

$$c = (c_R, c_Q)$$

from Theorem 3.1, and let Γ_0, Γ_1 be as in (8). Assume $\{p\} \notin \Gamma$.

Choose composite schemes with convecs

$$c^{(n)} \longrightarrow c$$

and, using the uniform-secret reduction recalled in Section 2, take each secret to be uniform. For fixed n, restriction to R gives a Γ_0-scheme with the same secret alphabet. The conditional slices used to obtain the Γ_1-convec also have the same uniform secret distribution.

Approximate the convex weights of these slices by rational weights and realize the resulting convex combination by independent repetitions. Repeat the restricted Γ_0-scheme by the same total multiplicity. The resulting Γ_0- and Γ_1-schemes then have secrets uniform on the same product alphabet, so Lemma 2.1 applies. It produces a scheme for Γ with

$$x_p = 1$$

and with each coordinate on R bounded by the sum of the corresponding coordinates of the two component convecs. Passing to the limit in the closed convec region gives

$$x_R \leq 2c_R.$$

This is the outer convec used in the proof of Theorem 3.1.

References

[1] A. Shamir, How to share a secret, *Communications of the ACM* 22 (1979), no. 11, 612–613.

[2] G. R. Blakley, Safeguarding cryptographic keys, in *Proceedings of the National Computer Conference*, vol. 48, 313–317, 1979.

[3] M. Ito, A. Saito, and T. Nishizeki, Secret sharing scheme realizing general access structure, *Electronics and Communications in Japan, Part III* 72 (1989), no. 9, 56–64.

[4] K. M. Martin, New secret sharing schemes from old, *J. Combin. Math. Combin. Comput.* 14 (1993), 65–77.

[5] L. Csirmaz, The size of a share must be large, *Journal of Cryptology* 10 (1997), no. 4, 223–231.

[6] C. Blundo, A. De Santis, and U. Vaccaro, On secret sharing schemes, *Information Processing Letters* 65 (1998), no. 1, 25–32.

[7] Z. Zhang and R. W. Yeung, On characterization of entropy function via information inequalities, *IEEE Transactions on Information Theory* 44 (1998), no. 4, 1440–1452.

[8] A. Beimel, N. Livne, and C. Padró, Matroids can be far from ideal secret sharing, in *Theory of Cryptography Conference (TCC 2008)*, 194–212, 2008.

[9] A. Beimel and I. Orlov, Secret sharing and non-Shannon information inequalities, *IEEE Transactions on Information Theory* 57 (2011), no. 9, 5634–5649.

[10] T. Kaced, Equivalence of two proof techniques for non-Shannon-type inequalities, in *2013 IEEE International Symposium on Information Theory (ISIT)*, 236–240, 2013.

[11] S. Martín, C. Padró, and A. Yang, Secret sharing, rank inequalities, and information inequalities, *IEEE Transactions on Information Theory* 62 (2016), no. 1, 599–609.

[12] O. Farràs, T. Kaced, S. Martín, and C. Padró, Improving the linear programming technique in the search for lower bounds in secret sharing, *IEEE Transactions on Information Theory* 66 (2020), no. 11, 7088–7100.

[13] R. W. Yeung, A framework for linear information inequalities, *IEEE Transactions on Information Theory* 43 (1997), no. 6, 1924–1934.

[14] J. Martí-Farré and C. Padró, On secret sharing schemes, matroids and polymatroids, *Journal of Mathematical Cryptology* 4 (2010), no. 2, 95–120.

[15] C. Padró, Lecture notes in secret sharing, IACR Cryptology ePrint Archive, Report 2012/674, 2012.

[16] A. Beimel, A. Gál, and M. Paterson, Lower bounds for monotone span programs, *Computational Complexity* 6 (1997), no. 1, 29–45.

[17] L. Babai, A. Gál, and A. Wigderson, Superpolynomial lower bounds for monotone span programs, *Combinatorica* 19 (1999), no. 3, 301–319.

[18] A. Beimel, A. Ben-Efraim, C. Padró, and I. Tyomkin, Multi-linear secret-sharing schemes, in *Theory of Cryptography Conference (TCC 2014)*, 394–418, 2014.

[19] T. Pitassi and R. Robere, Lifting Nullstellensatz to monotone span programs over any field, in *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2018)*, 1207–1219, 2018.

[20] O. Nir, Resolving the worst-case complexity of linear secret sharing, ECCC Report TR26-146, revision 1, 2026.

[21] S. Khazaei, Rank measures and exponential lower bounds for multilinear secret sharing, IACR Cryptology ePrint Archive, Report 2026/1769, 2026.

[22] C. Williamson, Secret sharing at the Shannon ceiling, arXiv:2608.17047, 2026.

[23] S. Khazaei, Conjecturally superpolynomial lower bound for share size, IACR Cryptology ePrint Archive, Report 2018/143, 2018.

[24] S. Khazaei, A candidate access structure for super-polynomial lower bound on information ratio, IACR Cryptology ePrint Archive, Report 2019/597, 2019.