

Component-Dual Compression and the Exact Characteristic-Two Contribution Region of the Relaxed Non-Fano Port

Shahram Khazaei and Maghsoud Parviz

Department of Mathematical Sciences, Sharif University of Technology, Tehran, Iran
shahram.khazaei@sharif.ir, maghsoud.parviz@gmail.com

Abstract. Jafari and Khazaei (Journal of Cryptology, 2021) introduced a kernel-based lower-bound method for linear secret-sharing schemes by fixing one minimal qualified coalition and comparing its participant components with those arising from auxiliary minimal qualified coalitions. These comparisons form a star. We extend the same mechanism from stars to coalition-labelled trees and obtain new characteristic-two inequalities for the relaxed-line non-Fano port $\hat{N}$. For this access structure, the tree method is strictly stronger than the star method, yielding facet inequalities not implied by the star inequalities. We also show that the tree method does not determine the full contribution region.

To complete the analysis of $\hat{N}$, we introduce component-dual compression (CDC). CDC replaces each share by the span of the components selected from minimal reconstructions and realizes the duals of these compressed spaces in a common coordinate system indexed by the original minimal coalitions. This yields the remaining lower-bound inequalities. Together with matching constructions, the star, tree, and CDC bounds determine the complete characteristic-two linear contribution region of $\hat{N}$, with maximum and average linear information ratios $5/4$.

Keywords: linear secret sharing · component-dual compression · contribution regions · tree-kernel method · non-Fano port · matroid ports

1 Introduction

Secret sharing, introduced independently by Shamir and Blakley [14,3], distributes a secret among participants so that qualified coalitions can reconstruct it while unqualified coalitions obtain no information. This paper studies linear secret-sharing schemes over a common finite field, in which the secret and each participant share are represented by finite-dimensional vector spaces. These dimensions may vary from participant to participant and may be larger than one; this is the multilinear model considered throughout the paper. Scheme efficiency is measured by the share dimensions relative to the secret dimension. Normalizing each participant dimension by the secret dimension gives a *contribution vector*, and the feasible contribution vectors form a convex, upward-comprehensive contribution region.

Main result and approach. The target access structure is the relaxed-line non-Fano port

$$\widehat{N} = 25 + 36 + 123 + 124 + 134 + 145 + 146 + 156 + 246 + 345. \quad (1.1)$$

In characteristic two we determine its complete linear contribution region. Consequently, both the maximum and the average linear information ratios are exactly $5/4$. Matching schemes attain every vertex orbit of the region.

From the JK star to trees. Jafari and Khazaei (JK) [8] showed that every minimal qualified coalition contains a secret-dimensional component in each participating share and that these components decompose the secret. Their Kernel Lemma compares the components of one fixed minimal coalition with those from auxiliary minimal coalitions sharing the relevant participants. The resulting comparison is a star; the Fano instance is shown in Figure 3.1.

The same edgewise comparison can be chained while allowing the centre to move. Minimal coalitions then become vertices and shared-participant comparisons become labelled edges; an acyclic configuration is a tree. The nonstar tree used for $\widehat{N}$ is shown in Figure 3.2. The resulting tree-kernel theorem contains the JK star as a special case and yields characteristic-two lower bounds for $\widehat{N}$ that the star inequalities alone do not provide.

Why the ordinary comparison stops. The ordinary JK/tree edge-difference mechanism has a sharp rank limitation. For a connected comparison graph with vertex set V and edge set $\mathcal{E}$, a rank argument based only on the edge-difference map can improve the unit-share bound by at most $|V| - |\mathcal{E}|$. Hence a graph containing a cycle has no positive surplus. For $\widehat{N}$, the exact region nevertheless requires

$$c_1 + c_4 + c_5 + c_6 \geq 5. \quad (1.2)$$

Any ordinary comparison graph for this left-hand side has four edges, labelled 1, 4, 5, 6. Thus a candidate reaching right-hand side 5 must be a five-vertex tree. An exhaustive check of the admissible such trees on $\widehat{N}$ and $\widehat{N}^*$ finds none that yields (1.2). Therefore the ordinary one-edge/one-share comparison does not determine this facet. CDC supplies additional compatible coordinates in which components from different minimal reconstructions can be compared.

Component-dual compression and the cycle. Standard linear duality uses all correctness and privacy relations of a scheme, but it does not distinguish the participant subspaces selected by individual minimal reconstructions. CDC first keeps only the span of those selected subspaces and then realizes their duals in a direct sum with one coordinate copy for each original minimal coalition. A participant has zero coordinates in copies indexed by coalitions that do not contain it, while projection onto every incident copy is surjective. When an original minimal coalition and a dual minimal coalition meet in a single participant, the corresponding projection of that participant component is the identity. This provides compatible readings for components coming from different reconstructions.

For $\widehat{N}$, the four minimal coalitions in Figure 5.1 form the required one-cycle configuration. The CDC coordinate identities make the three comparisons through

participants 1, 5, and 6 compatible, and the participant-4 comparison closes the cycle. One traversal defines a linear return map on the secret-dual space. The deviation of this return map from the identity is bounded in two independent ways, and the two estimates combine to give (1.2). Its automorphism orbit—the inequalities obtained by permuting participant labels with automorphisms of $\hat{N}$ —gives the other three CDC facets.

Complete region and constructions. The unit-share inequalities, the JK star bounds, the nonstar-tree bounds, and the cyclic CDC bounds are all sharp. Most extremal contribution vectors are realized by (λ, ω) -decompositions [16], while the remaining few are given by direct linear constructions. Together they give the complete characteristic-two linear contribution region of $\hat{N}$ and both information ratios $5/4$.

The other non-Fano port. JK also analyzed the standard non-Fano port N in characteristic two [8]. Their lower-bound polyhedron had one unrealized automorphism orbit, represented by

$$v_N = \left(\frac{5}{3}, 1, 1, \frac{4}{3}, \frac{4}{3}, \frac{4}{3} \right).$$

The binary construction in Appendix C realizes this point, and the automorphisms of N give the other two points in its orbit. Thus the JK lower bounds also give the complete characteristic-two linear contribution region of the standard port N . This completion is independent of CDC.

Related work. For general background on secret sharing and its share-size problem, see Beimel’s survey [2]. Lower bounds have been developed through entropy and polymatroid inequalities [5,10,7], and through subspace and linear-rank inequalities for linear schemes [9]. Characteristic-dependent linear-rank inequalities provide a complementary way to distinguish field characteristics [6,12]. Jafari and Khazaei [8] introduced the minimal-subspace and kernel method used here to obtain characteristic-dependent secret-sharing bounds for the Fano and non-Fano ports. Peña-Macias subsequently used this access-structure viewpoint as a starting point for constructing characteristic-dependent linear-rank inequalities [11]. Matroid ports connect these questions with representability and ideal secret sharing [4,17,1].

Paper organization. Section 2 fixes the notation and background used by both lower-bound mechanisms. Section 3 develops the JK star, its tree extension, and the rank limitation of ordinary edge-difference comparison. Section 4 develops CDC and the coordinate identities used by the one-cycle calculation in Section 5; Section 6 converts those identities into (1.2). Finally, Sections 7 and 8 give the matching constructions and the complete region. After the references, the appendices list the remaining star inequalities and construction witnesses and give the short completion of the standard port N .

2 Preliminaries

This section fixes the linear-scheme, duality, and minimal-decomposition notation used later, and then specifies the relaxed-line non-Fano port and its symmetries.

2.1 Access structures and linear schemes

An *access structure* on participants $[n] = \{1, \dots, n\}$ is an upward-closed family $\Gamma \subseteq 2^{[n]}$: if $A \in \Gamma$ and $A \subseteq A'$, then $A' \in \Gamma$. Its members are *qualified*; the remaining coalitions are *unqualified*. We write $\min \Gamma$ for the family of minimal qualified coalitions. Its *dual access structure* Γ^* is defined by

$$A \in \Gamma^* \iff [n] \setminus A \notin \Gamma.$$

A linear secret-sharing scheme for Γ over a finite field $\mathbb{F}$ is a collection

$$\Pi = (E; T_0, (T_i)_{i \in [n]}),$$

where E is a finite-dimensional $\mathbb{F}$ -vector space and $T_0, T_1, \dots, T_n \subseteq E$. The subspace T_0 is the secret space and T_i is the share space of participant i . For $A \subseteq [n]$, put $T_A = \sum_{i \in A} T_i$. The scheme realizes Γ perfectly if

$$A \in \Gamma \implies T_0 \subseteq T_A, \tag{2.1}$$

$$A \notin \Gamma \implies T_0 \cap T_A = \{0\}. \tag{2.2}$$

We call (2.1) and (2.2) the correctness and privacy conditions, respectively.

Let $d_0 = \dim T_0$ and $d_i = \dim T_i$. The contribution vector of Π is

$$c(\Pi) = (c_1, \dots, c_n), \quad c_i = \frac{d_i}{d_0}.$$

For a prime p , let $\Sigma_{\text{lin}}^p(\Gamma)$ be the closure of contribution vectors of linear schemes over finite fields of characteristic p . The maximum and average characteristic- p linear information ratios are

$$\sigma_{\max}^{(p)}(\Gamma) = \min_{c \in \Sigma_{\text{lin}}^p(\Gamma)} \max_{i \in [n]} c_i, \quad \sigma_{\text{av}}^{(p)}(\Gamma) = \frac{1}{n} \min_{c \in \Sigma_{\text{lin}}^p(\Gamma)} \sum_{i=1}^n c_i.$$

Direct sums show that $\Sigma_{\text{lin}}^p(\Gamma)$ is convex; private padding, obtained by adding independent coordinates to shares, makes it upward comprehensive.

2.2 Finite-dimensional duality and annihilators

The CDC construction later dualizes selected component spans and places their duals in a common block-coordinate space. The finite-dimensional duality and annihilator conventions needed for that construction are fixed here.

For a finite-dimensional $\mathbb{F}$ -vector space V , write

$$V^* = \text{Hom}_{\mathbb{F}}(V, \mathbb{F})$$

for its algebraic dual. For a linear map $f : V \rightarrow W$, write

$$f^* : W^* \rightarrow V^*, \quad f^*(\varphi) = \varphi \circ f.$$

We use the standard finite-dimensional identities

$$(g \circ f)^* = f^* \circ g^*, \quad \text{rank } f^* = \text{rank } f. \quad (2.3)$$

For a finite family $(V_j)_{j \in J}$, identify $(\bigoplus_j V_j)^*$ with $\bigoplus_j V_j^*$ through the canonical isomorphism

$$\Theta((\varphi_j)_{j \in J})(v) = \sum_{j \in J} \varphi_j(v_j), \quad v = (v_j)_{j \in J}. \quad (2.4)$$

If $\iota_A : V_A \hookrightarrow \bigoplus_j V_j$ is the inclusion of the A th summand, the corresponding *block projection* is

$$\text{pr}_A := \iota_A^* : \left(\bigoplus_{j \in J} V_j \right)^* \longrightarrow V_A^*. \quad (2.5)$$

Thus $\text{pr}_A \Theta((\varphi_j)_j) = \varphi_A$.

For $X \leq V$ and $L \leq V^*$, write

$$X^\circ = \{\varphi \in V^* : \varphi(X) = 0\}, \quad L^\circ = \{x \in V : \varphi(x) = 0 \text{ for every } \varphi \in L\}.$$

Using the natural identification $V \cong V^{**}$, we shall use

$$(\text{im } f^*)^\circ = \ker f, \quad (X^\circ)^\circ = X, \quad (L^\circ)^\circ = L. \quad (2.6)$$

In particular, annihilators reverse inclusions:

$$L_1^\circ \subseteq L_2^\circ \implies L_2 \subseteq L_1.$$

2.3 The standard dual linear scheme

The standard dual construction starts from all linear relations among the secret and participant spaces. Participant i is represented by the functionals induced by the i th coordinate projection on this relation space; annihilators then translate missing coordinates into reconstruction and privacy statements.

Let $\Pi = (E; T_0, (T_i)_{i \in [n]})$ be a linear scheme for Γ . Its *global relation space* is

$$\mathcal{C}_\Pi = \left\{ (t_0, t_1, \dots, t_n) \in \bigoplus_{i=0}^n T_i : \sum_{i=0}^n t_i = 0 \right\}. \quad (2.7)$$

For $0 \leq i \leq n$, let $p_i : \mathcal{C}_\Pi \rightarrow T_i$ be the i th coordinate projection and define

$$S_i := \text{im } p_i^* \subseteq \mathcal{C}_\Pi^*. \quad (2.8)$$

By the first identity in (2.6), each of these spaces is described by its annihilator inside $\mathcal{C}_\Pi$:

$$S_i^\circ = (\text{im } p_i^*)^\circ = \ker p_i \quad (0 \leq i \leq n). \quad (2.9)$$

Thus a relation vector annihilates S_i exactly when its i th coordinate vanishes, and, by double annihilation, a sum $\sum_{i \in B} S_i$ is controlled by the intersection $\bigcap_{i \in B} \ker p_i$. This is the mechanism behind the dual scheme, and Section 4 uses it again in the compressed setting.

The tuple

$$\Pi^* = (\mathcal{C}_\Pi^*; S_0, S_1, \dots, S_n)$$

is the standard dual linear scheme and realizes Γ^* [8, Section 7]. The full share space T_i enters through the map

$$p_i^* : T_i^* \longrightarrow \mathcal{C}_\Pi^*.$$

Thus $\dim S_i = \text{rank } p_i^* = \text{rank } p_i \leq d_i$ by (2.3). Since $[n]$ is qualified, every $s \in T_0$ has the form $s = \sum_i t_i$ with $t_i \in T_i$; hence $(s, -t_1, \dots, -t_n) \in \mathcal{C}_\Pi$, so p_0 is surjective and $\dim S_0 = d_0$.

It follows that every contribution vector c for Γ gives a contribution vector $c' \leq c$ for Γ^* . Since contribution regions are upward comprehensive, $\Sigma_{\text{lin}}^p(\Gamma) \subseteq \Sigma_{\text{lin}}^p(\Gamma^*)$. Applying the construction to Γ^* gives the reverse inclusion. Consequently, for every prime p ,

$$\Sigma_{\text{lin}}^p(\Gamma) = \Sigma_{\text{lin}}^p(\Gamma^*). \quad (2.10)$$

Component-dual compression refines this construction by replacing each full share space T_i with the span of its selected minimal components and by retaining the block from which each component originates.

2.4 Minimal secret decompositions

The structural input for both main constructions is Jafari–Khazaei’s Minimal Subspace Lemma [8, Lemma 4.1]. It states that a minimal qualified coalition contains, inside each participating share, a full-dimensional component copy of the secret, and that these components give a decomposition of every secret vector.

Lemma 2.1 (Minimal Subspace Lemma). *Let A be a minimal qualified coalition of a linear scheme $(T_0, T_1, \dots, T_n)$. There are subspaces $M_i^A \subseteq T_i$ for $i \in A$ such that*

- (i) $\dim M_i^A = d_0$ for every $i \in A$;
- (ii) $M_j^A \cap \sum_{i \in A \setminus \{j\}} T_i = \{0\}$ for every $j \in A$;
- (iii) $T_0 \subseteq \bigoplus_{i \in A} M_i^A$;
- (iv) the projection $T_0 \rightarrow M_i^A$ induced by the direct sum in (iii) is an isomorphism for every $i \in A$.

Proof. Choose a basis $s_1, \dots, s_{d_0}$ of T_0 . Reconstruction by A lets us write

$$s_r = \sum_{i \in A} u_{i,r}, \quad u_{i,r} \in T_i,$$

and set $M_i^A = \text{span}\{u_{i,1}, \dots, u_{i,d_0}\}$. Suppose a linear combination $u = \sum_r \alpha_r u_{j,r}$ lies in $\sum_{i \in A \setminus \{j\}} T_i$. Then

$$\sum_r \alpha_r s_r = u + \sum_{i \in A \setminus \{j\}} \sum_r \alpha_r u_{i,r} \in T_0 \cap T_{A \setminus \{j\}}.$$

The set $A \setminus \{j\}$ is unqualified, so privacy makes this intersection zero. Hence all $\alpha_r = 0$. This simultaneously gives $\dim M_j^A = d_0$ and the independence in (ii). The displayed decompositions give (iii), and the coordinate projection of s_r to M_i^A is $u_{i,r}$, hence an isomorphism.

Write

$$\mu_{A,i} : T_0 \longrightarrow M_i^A$$

for the projection isomorphism. Thus every secret s has the chosen decomposition

$$s = \sum_{i \in A} \mu_{A,i}(s). \quad (2.11)$$

Whenever participant i belongs to some $A \in \min \Gamma$, Lemma 2.1(i) gives a d_0 -dimensional subspace $M_i^A \subseteq T_i$, and therefore $d_i \geq d_0$ and $c_i \geq 1$. We call inequalities obtained in this way *unit-share inequalities*.

2.5 The relaxed-line non-Fano port

Minimal qualified coalitions will be written by concatenating participant labels; for example, 123 denotes $\{1, 2, 3\}$, and $+$ denotes upward closure. The access structure studied throughout the paper is the relaxed-line non-Fano port

$$\widehat{N} = 25 + 36 + 123 + 124 + 134 + 145 + 146 + 156 + 246 + 345. \quad (2.12)$$

Its maximal unqualified coalitions are

$$14, \quad 126, \quad 135, \quad 234, \quad 456, \quad (2.13)$$

and its dual is

$$\widehat{N}^* = 123 + 156 + 246 + 345 + 2356. \quad (2.14)$$

The name is justified as follows. Let M be the rank-three matroid on $\{0, 1, \dots, 6\}$ whose three-point lines are

$$\{0, 2, 5\}, \{0, 3, 6\}, \{1, 2, 6\}, \{1, 3, 5\}, \{2, 3, 4\}, \{4, 5, 6\}. \quad (2.15)$$

These six lines meet pairwise in at most one point, and a rank-three matroid on seven points with six three-point lines is the non-Fano matroid, obtained from the Fano plane by relaxing one circuit-hyperplane. The points lying on only two of the lines in (2.15) are 0, 1, 4, so $\{0, 1, 4\}$ is the relaxed line. The *port* of M at a point p is the access structure on the remaining six points whose minimal qualified coalitions are the sets $C \setminus \{p\}$ for the circuits C of M containing p . Taking $p = 0$, a point *on* the relaxed line, gives exactly $\widehat{N}$; taking a point off that line gives the standard non-Fano port

$$N = 14 + 25 + 36 + 123 + 156 + 246 + 345 + 456,$$

and taking the corresponding point of the Fano matroid gives the Fano port F of Section 7. Thus F , N and $\widehat{N}$ are the three ports occurring in this paper, and $\widehat{N}$ is the one attached to the relaxed line. The characteristic behaviour of the Fano and non-Fano configurations is classical [13]. The body below studies $\widehat{N}$; the short characteristic-two completion of the standard port N is recorded in Appendix C. An *automorphism* of an access structure is a permutation of the participants that preserves qualification. The automorphism group of $\widehat{N}$ has order eight and is generated by

$$\text{Aut}(\widehat{N}) = \langle (23)(56), (25)(36), (14)(36) \rangle. \quad (2.16)$$

All orbit statements below refer to this action on participant coordinates. Every participant of $\widehat{N}$ occurs in a minimal qualified coalition in (2.12), so all six unit-share inequalities $c_i \geq 1$ apply.

3 Component Comparison and Acyclic Bounds

The lower-bound analysis begins with the ordinary JK component comparison. Extending it from stars to trees gives the nonstar bounds for $\widehat{N}$; the final subsection identifies the rank ceiling that leaves the cyclic inequality to CDC.

3.1 Unit and star facets; the Fano star as model

For the target access structure $\widehat{N}$, every participant occurs in a minimal qualified coalition, so Lemma 2.1 gives the six unit-share inequalities $c_i \geq 1$. Under $\text{Aut}(\widehat{N})$ these split into two participant orbits.

To recall the JK star mechanism, consider the Fano port

$$F = 14 + 25 + 36 + 123 + 156 + 246 + 345.$$

The JK Kernel Lemma [8, Lemma 4.3] compares, for a fixed central minimal coalition A , its participant components with components belonging to auxiliary minimal coalitions $A_i \ni i$. The resulting shared-participant comparisons form a star. In Figure 3.1, the centre is 123 and the leaves are 14, 25, 36, labelled by 1, 2, 3, respectively:

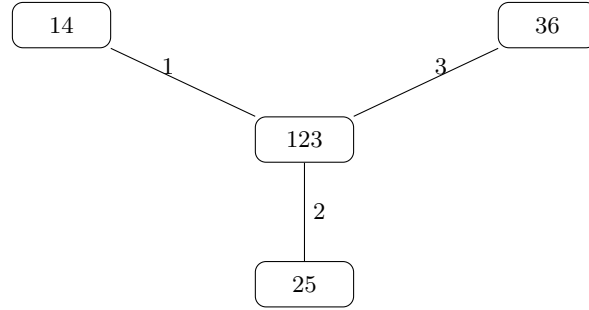


Fig. 3.1. The Jafari–Khazaei star comparison for the Fano port $F = 14 + 25 + 36 + 123 + 156 + 246 + 345$. The centre is 123, the leaves are 14, 25, 36, and the edge labels are 1, 2, 3. The tree construction keeps the same edgewise rule but allows the comparison centre to move.

A tuple of node secrets satisfying these three edge-comparison equations will be called a *kernel tuple* in this example. In vertex order $(123, 14, 25, 36)$, the three edge comparisons leave residual supports 234, 135, 126, and the collective cancellation leaves 456. These four coalitions are unqualified in F , so privacy gives three pairwise relations identifying the node secrets and one collective relation. Their coefficient matrix is

$$R_F = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & -1 \\ 1 & -1 & -1 & -1 \end{pmatrix}, \quad \det R_F = -2.$$

Thus the familiar characteristic dependence of this star is encoded by privacy relations among node secrets. Applying the Kernel Lemma to $\widehat{N}^* = 123 + 156 + 246 + 345 + 2356$ and reducing under automorphisms gives sixteen irredundant star inequalities in two orbits, represented by

$$c_3 + c_4 + c_5 + c_6 \geq 5, \quad c_3 + c_4 + 2c_5 \geq 5.$$

For comparison, the same JK mechanism applied to the standard non-Fano port N gives, among others,

$$c_1 + c_2 + c_3 + c_4 \geq 5, \quad c_1 + 2c_5 + c_6 \geq 5.$$

These belong to the lower-bound system of [8]; Appendix C supplies the previously missing construction needed to make that system exact. All sixteen star inequalities for $\widehat{N}$ are listed in Appendix A.

3.2 Acyclic diagrams: the tree comparison theorem

A component-comparison diagram represents each selected minimal reconstruction by a vertex; write $A(v)$ for the minimal coalition labelling vertex v . An edge vw

is labelled by a participant $i \in A(v) \cap A(w)$ and compares the two i -component maps. When the diagram is acyclic, this data forms a coalition-labelled tree.

A *coalition-labelled tree* for an access structure Γ is

$$\mathcal{T} = (V, \mathcal{E}; A, \ell),$$

where $(V, \mathcal{E})$ is a tree, $A(v) \in \min \Gamma$ for every vertex, and $\ell(vw) \in A(v) \cap A(w)$ for every edge. Choose a minimal decomposition at each vertex and write $\mu_{v,i} : T_0 \rightarrow T_i$ for its participant component maps. Let m_i be the number of edges labelled i and define

$$F_{\mathcal{T}} : T_0^V \longrightarrow \bigoplus_{e \in \mathcal{E}} T_{\ell(e)}, \quad (F_{\mathcal{T}}(s))_{vw} = \mu_{v,\ell(vw)}(s_v) - \mu_{w,\ell(vw)}(s_w). \quad (3.1)$$

The codomain is the *edge-indexed external direct sum*: two different edges bearing the same participant label contribute two distinct copies of that participant space. Hence the codomain dimension is $\sum_i m_i d_i$.

The privacy relations must be closed componentwise. Edges labelled i identify i -components only within a connected component of the i -labelled subgraph, so cancellation has to be tested separately on each such component. Fix participant i . On the graph with vertex set $V_i = \{v : i \in A(v)\}$ and only the i -labelled tree edges, let $\mathcal{C}_i$ be the vertex sets of the maximal connected components, including isolated vertices. For $x = (x_v) \in \mathbb{F}^V$, define the residual participant support

$$Q_{\mathcal{T}}(x) = \left\{ i : \text{for some } C \in \mathcal{C}_i, \sum_{v \in C} x_v \neq 0 \right\}. \quad (3.2)$$

The sums are taken separately on the maximal i -components; a global count of occurrences of i is not sufficient.

Lemma 3.1 (Privacy closure). *If $s = (s_v) \in \ker F_{\mathcal{T}}$, then for every $x \in \mathbb{F}^V$,*

$$\sum_v x_v s_v \in T_{Q_{\mathcal{T}}(x)}.$$

If $Q_{\mathcal{T}}(x)$ is unqualified, then $\sum_v x_v s_v = 0$.

Proof. For a fixed i and maximal component $C \in \mathcal{C}_i$, the edge equations make $\mu_{v,i}(s_v)$ equal for all $v \in C$; call the common vector $u_{i,C} \in T_i$. Expanding each s_v by its minimal decomposition, the contribution of C to $\sum_v x_v s_v$ is $(\sum_{v \in C} x_v)u_{i,C}$. Summing over i and C gives the claimed residual support. The same vector lies in T_0 , so privacy makes it zero when that support is unqualified.

Let

$$\mathcal{R}_{\mathcal{T}} = \text{span}_{\mathbb{F}}\{x \in \mathbb{F}^V : Q_{\mathcal{T}}(x) \text{ is unqualified}\}, \quad \rho_{\mathcal{T}} = \dim \mathcal{R}_{\mathcal{T}}.$$

By Lemma 3.1, every $r = (r_v) \in \mathcal{R}_{\mathcal{T}}$ satisfies

$$\sum_v r_v s_v = 0 \quad (s \in \ker F_{\mathcal{T}}). \quad (3.3)$$

Choose a basis of $\mathcal{R}_{\mathcal{T}}$ and let $R_{\mathcal{T}} \in \mathbb{F}^{\rho_{\mathcal{T}} \times |V|}$ be the matrix with these basis vectors as rows. Define the T_0 -valued map

$$\Psi_{\mathcal{T}} : T_0^V \rightarrow T_0^{\rho_{\mathcal{T}}}, \quad \Psi_{\mathcal{T}}(s) = R_{\mathcal{T}}s,$$

and the *privacy-null space*

$$W_{\mathcal{T}} := \ker \Psi_{\mathcal{T}}. \quad (3.4)$$

Equation (3.3) gives $\ker F_{\mathcal{T}} \subseteq W_{\mathcal{T}}$. In scalar coordinates, $\Psi_{\mathcal{T}}$ is the direct sum of k copies of $R_{\mathcal{T}}$, so

$$\dim W_{\mathcal{T}} = (|V| - \rho_{\mathcal{T}})d_0, \quad \ker F_{\mathcal{T}} \subseteq W_{\mathcal{T}}. \quad (3.5)$$

Theorem 3.2 (Tree-kernel rank inequality). *For every coalition-labelled tree,*

$$\sum_i m_i d_i \geq \rho_{\mathcal{T}} d_0 + \text{rank}(F_{\mathcal{T}}|_{W_{\mathcal{T}}}). \quad (3.6)$$

Here $F_{\mathcal{T}}|_{W_{\mathcal{T}}}$ is the restriction of the edge-difference map to the privacy-null space $W_{\mathcal{T}}$.

In particular, if $\rho_{\mathcal{T}} = |V| - 1$, $\ker R_{\mathcal{T}} = \langle \lambda \rangle$, and some edge vw has exactly one of λ_v, λ_w equal to zero, then $F_{\mathcal{T}}$ is injective and

$$\sum_i m_i c_i \geq |V|. \quad (3.7)$$

Over $\mathbb{F}_2$, the edge criterion is equivalently $\lambda_v \neq \lambda_w$.

Proof. Since $\ker F_{\mathcal{T}} \subseteq W_{\mathcal{T}}$,

$$\ker(F_{\mathcal{T}}|_{W_{\mathcal{T}}}) = \ker F_{\mathcal{T}}.$$

Rank-nullity for the restricted map therefore gives

$$\dim \ker F_{\mathcal{T}} = \dim W_{\mathcal{T}} - \text{rank}(F_{\mathcal{T}}|_{W_{\mathcal{T}}}).$$

Using (3.5),

$$\begin{aligned} \text{rank } F_{\mathcal{T}} &= |V|d_0 - \dim \ker F_{\mathcal{T}} \\ &= \rho_{\mathcal{T}}d_0 + \text{rank}(F_{\mathcal{T}}|_{W_{\mathcal{T}}}). \end{aligned}$$

The codomain dimension of (3.1) gives (3.6). In the codimension-one case every $s \in W_{\mathcal{T}}$ has the form $s_v = \lambda_v t$ for one $t \in T_0$. If $F_{\mathcal{T}}(s) = 0$ and an edge vw has, say, $\lambda_v = 0$ and $\lambda_w \neq 0$, its edge equation gives $\mu_{w, \ell(vw)}(t) = 0$. The component map is an isomorphism onto its image, so $t = 0$. Hence $F_{\mathcal{T}}$ is injective, and the edge-indexed codomain gives (3.7).

A star is the special case in which all edges share one centre, so the theorem extends the same comparison mechanism rather than introducing a separate lower-bound principle. The Fano computation above is the instance $|V| = 4$ with $\rho_{\mathcal{T}} = 4$ in odd characteristic.

3.3 The four nonstar tree facets of $\widehat{N}$

For this application it is useful to display both access structures in Sperner notation:

$$\begin{aligned}\widehat{N} &= 25 + 36 + 123 + 124 + 134 + 145 \\ &\quad + 146 + 156 + 246 + 345,\end{aligned}$$

$$\widehat{N}^* = 123 + 156 + 246 + 345 + 2356.$$

By (2.10), it suffices to work on $\widehat{N}^*$. The five minimal qualified coalitions of $\widehat{N}^*$ form the tree in Figure 3.2:

$$345 \xleftrightarrow{3} 2356, \quad 156 \xleftrightarrow{6} 2356, \quad 2356 \xleftrightarrow{2} 246, \quad 246 \xleftrightarrow{2} 123.$$

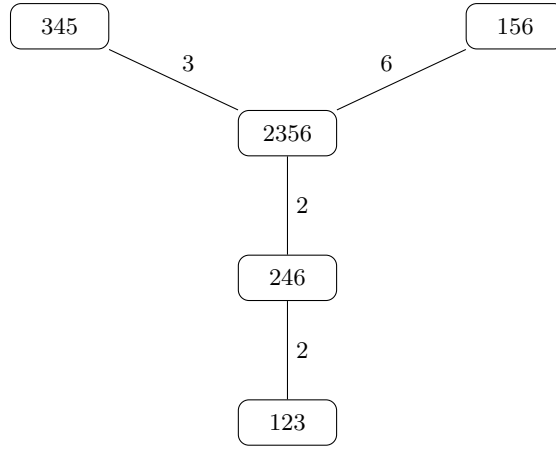


Fig. 3.2. The five-vertex tree on $\widehat{N}^*$ used, via canonical duality, to derive the nonstar bound for $\widehat{N}$. The comparison centre changes from 2356 to 246 on the final edge.

Thus $m_2 = 2$ and $m_3 = m_6 = 1$. In characteristic two, the componentwise privacy closure gives the following four relations for $s \in \ker F_{\mathcal{T}}$:

$$\begin{aligned}s_{2356} + s_{345} + s_{246} &= 0 & (Q = 456), \\ s_{2356} + s_{345} + s_{156} &= 0 & (Q = 1245), \\ s_{246} + s_{123} &= 0 & (Q = 1346), \\ s_{2356} + s_{156} + s_{123} &= 0 & (Q = 135).\end{aligned}$$

All four residual supports are unqualified in $\widehat{N}^*$. In the vertex order $(2356, 345, 246, 156, 123)$, the four displayed relations have coefficient vectors

$$(1, 1, 1, 0, 0), (1, 1, 0, 1, 0), (0, 0, 1, 0, 1), (1, 0, 0, 1, 1),$$

which are linearly independent over $\mathbb{F}_2$. Hence $\rho_{\mathcal{T}} \geq 4$. If $\rho_{\mathcal{T}} = 5$, Theorem 3.2 already gives the required lower bound $2d_2 + d_3 + d_6 \geq 5d_0$. Otherwise $\rho_{\mathcal{T}} = 4$, the four vectors above form a basis of the privacy-relation space, and their common nullspace is

$$\langle (0, 1, 1, 1, 1)^T \rangle.$$

The edge $345 \xrightarrow{3} 2356$ joins a zero and a nonzero coordinate of this null vector, so the codimension-one clause of Theorem 3.2 again gives $2d_2 + d_3 + d_6 \geq 5d_0$.

Proposition 3.3 (Nonstar tree facets). *Every characteristic-two linear scheme for $\hat{N}$ satisfies the four-inequality automorphism orbit represented by*

$$2c_2 + c_3 + c_6 \geq 5. \quad (3.8)$$

Proof. The tree above and Theorem 3.2 give

$$5d_0 \leq 2d_2 + d_3 + d_6$$

for $\hat{N}^*$. Canonical duality transfers the same inequality to the common contribution region of $\hat{N}$ and $\hat{N}^*$. The remaining three inequalities follow from (2.16).

3.4 Limitation of ordinary component comparison

The tree theorem extends the Jafari–Khazaei star without changing the underlying one-edge/one-share comparison rule. The next proposition gives a general rank ceiling for that rule. For the missing compression facet, this ceiling excludes all cyclic candidates, while an exhaustive finite check excludes the remaining tree candidates.

Let $\mathcal{G} = (V, \mathcal{E})$ be a connected participant-labelled comparison graph and let m_i be the number of edges labelled i . Extending (3.1) verbatim gives

$$F_{\mathcal{G}} : T_0^V \longrightarrow \bigoplus_{e \in \mathcal{E}} T_{\ell(e)}.$$

The unit-share inequalities give the baseline

$$\sum_i m_i c_i \geq \sum_i m_i = |\mathcal{E}|. \quad (3.9)$$

Proposition 3.4 (Pairwise rank surplus). *Suppose a rank argument based only on $F_{\mathcal{G}}$ proves $\text{rank } F_{\mathcal{G}} \geq \beta d_0$. Then*

$$\sum_i m_i c_i \geq \beta, \quad \beta - |\mathcal{E}| \leq |V| - |\mathcal{E}|.$$

Consequently, a tree can improve the unit-share baseline by at most one, whereas a connected graph containing a cycle has no positive rank surplus under this ordinary one-edge/one-share comparison rule.

Proof. The codomain dimension gives $\sum_i m_i d_i \geq \text{rank } F_{\mathcal{G}} \geq \beta d_0$, which yields the first inequality after division by d_0 . The domain has dimension $|V|d_0$, so $\beta \leq |V|$. Subtracting (3.9) gives the second claim. For a tree, $|\mathcal{E}| = |V| - 1$; for a connected graph containing a cycle, $|\mathcal{E}| \geq |V|$.

The compression facet proved in Section 6 is

$$c_1 + c_4 + c_5 + c_6 \geq 5. \quad (3.10)$$

Any ordinary comparison graph that yields the left-hand side of (3.10) has four edges, labelled 1, 4, 5, 6. If it contains a cycle, then $|V| \leq 4$, so Proposition 3.4 cannot improve the unit-share baseline $c_1 + c_4 + c_5 + c_6 \geq 4$ to right-hand side 5. Thus any ordinary connected comparison graph that could reach (3.10) must have five vertices and four edges, and hence must be a tree. An exhaustive enumeration of the admissible five-vertex coalition-labelled trees with edge-label multiset $\{1, 4, 5, 6\}$, on both $\hat{N}$ and $\hat{N}^*$, finds no instance whose ordinary comparison map yields right-hand side 5.

The four-node CDC configuration used later reaches the missing bound because it retains compatibility information between components arising from different minimal reconstructions that is absent from the ordinary edge-difference comparison. This additional structure makes it possible to compare the components consistently around a cycle and obtain the final inequality.

4 Component-Dual Compression

The rank ceiling from Section 3.4 leaves the cyclic inequality unresolved. CDC supplies coalition-indexed coordinates without increasing participant dimensions; the properties established here are exactly those used by the cycle in Section 5.

4.1 The compressed dual construction

Fix a linear scheme $\Pi = (E; T_0, (T_i)_{i \in [n]})$ for an access structure Γ . For every $A \in \min \Gamma$, fix one family of injective linear maps

$$\mu_{A,i} : T_0 \longrightarrow T_i \quad (i \in A) \quad (4.1)$$

given by the Minimal Subspace Lemma, so that $M_i^A = \text{im } \mu_{A,i}$ and

$$\sum_{i \in A} \mu_{A,i}(s) = s \quad (s \in T_0)$$

in the ambient space E . Such a family exists but may not be unique. From this point onward the family $(\mu_{A,i})_{A,i}$ is fixed, and every object in the CDC construction is defined from it by an explicit formula.

For participant i , define the *component span*

$$U_i := \sum_{\substack{A \in \min \Gamma \\ i \in A}} M_i^A \subseteq T_i. \quad (4.2)$$

The spaces $(E; T_0, (U_i)_{i \in [n]})$ still realize Γ : reconstruction follows from a minimal qualified subcoalition, and privacy from $U_i \subseteq T_i$. Thus compression replaces T_i by U_i , the span of the component subspaces selected by the fixed decompositions, and uses U_i as the participant data for the dual construction.

For every $A \in \min \Gamma$, let $T_{0,A}$ be the formal copy of T_0 labelled by A , with its tautological identification with T_0 , and put

$$\mathcal{V} = \bigoplus_{A \in \min \Gamma} T_{0,A}.$$

For each participant define the surjection

$$\bar{\pi}_i : \mathcal{V} \longrightarrow U_i, \quad \bar{\pi}_i((s_A)_A) = \sum_{A \ni i} \mu_{A,i}(s_A). \quad (4.3)$$

Its image is U_i by definition. Set

$$H_i := \text{im } \bar{\pi}_i^* \subseteq \mathcal{V}^*.$$

Because $\bar{\pi}_i$ is onto, $\bar{\pi}_i^* : U_i^* \rightarrow \mathcal{V}^*$ is injective, so it identifies U_i^* canonically with H_i . In particular,

$$H_i \cong U_i^*, \quad \dim H_i = \dim U_i \leq d_i. \quad (4.4)$$

Thus the participant-side compression has the schematic form

$$T_i \supseteq U_i \longrightarrow U_i^* \cong H_i,$$

where U_i is the span of the component subspaces selected by the fixed minimal decompositions, and the second map realizes U_i^* inside the common block-coordinate space. Every vector of H_i is supported only on blocks $A \ni i$.

Define also

$$\Sigma : \mathcal{V} \rightarrow T_0, \quad \Sigma((s_A)_A) = \sum_A s_A, \quad J := \text{im } \Sigma^* \subseteq \mathcal{V}^*.$$

Under the finite direct-sum identification (2.4), and after identifying each $T_{0,A}^*$ with T_0^* ,

$$J = \{(\varphi, \dots, \varphi) : \varphi \in T_0^*\}, \quad \dim J = d_0.$$

Theorem 4.1 (Scheme-wise component-dual compression). *For the fixed minimal-decomposition maps (4.1), the spaces defined above form a perfect linear scheme*

$$\Pi^c = (\mathcal{V}^*; J, H_1, \dots, H_n)$$

for Γ^* . Once the maps $(\mu_{A,i})_{A,i}$ are fixed, the scheme Π^c is determined. It satisfies

$$\dim H_i = \dim U_i \leq d_i \quad (4.5)$$

for every participant. Moreover, for every incidence $i \in A \in \min \Gamma$, the coordinate projection

$$\text{pr}_A : H_i \longrightarrow T_{0,A}^*$$

is surjective. Hence $\dim H_i \geq d_0$ whenever i occurs in a minimal qualified coalition.

For correctness we show $H_B^\circ \subseteq J^\circ$ for $B \in \Gamma^*$ and then dualize this inclusion. Privacy follows from a minimal original block that is absent from every participant in an unqualified coalition of Γ^* .

Proof. The dimension statement is (4.4). Under the identification $H_i \cong U_i^*$, the A -block projection is the dual of the component embedding:

$$\text{pr}_A(\bar{\pi}_i^* \varphi) = \varphi \circ \mu_{A,i}.$$

Here $\mu_{A,i}$ is read through the tautological identification $T_{0,A} \cong T_0$, and hence is an injective map $T_{0,A} \rightarrow U_i$. In finite dimensions, every functional on $T_{0,A}$ extends from $\mu_{A,i}(T_{0,A})$ to U_i , so pr_A is onto.

For correctness, take arbitrary $B \in \Gamma^*$ and put $D = [n] \setminus B$. By definition of the dual access structure, $D \notin \Gamma$. Let

$$H_B = \sum_{i \in B} H_i \subseteq \mathcal{V}^*$$

and take $x = (s_A)_A \in H_B^\circ$. Then $x \in H_i^\circ$ for every $i \in B$, and the annihilator identity (2.6) gives

$$H_i^\circ = (\text{im } \bar{\pi}_i^*)^\circ = \ker \bar{\pi}_i.$$

Thus $\bar{\pi}_i(x) = 0$ for $i \in B$. Summing the chosen minimal decompositions in the original ambient space E yields

$$\begin{aligned} \Sigma(x) &= \sum_A s_A = \sum_A \sum_{i \in A} \mu_{A,i}(s_A) = \sum_{i \in [n]} \bar{\pi}_i(x) \\ &= \sum_{i \in D} \bar{\pi}_i(x) \in T_0 \cap \sum_{i \in D} U_i \subseteq T_0 \cap T_D = \{0\}, \end{aligned}$$

where privacy of the original scheme is used in the last equality. Hence $x \in \ker \Sigma = J^\circ$, so $H_B^\circ \subseteq J^\circ$. Double annihilation gives $J \subseteq H_B$, which is correctness.

If $C \notin \Gamma^*$, then $[n] \setminus C \in \Gamma$ and therefore contains some $A_0 \in \min \Gamma$. Since $A_0 \cap C = \emptyset$, each H_i with $i \in C$ has zero A_0 -coordinate. Every nonzero vector of the diagonal space J has a nonzero A_0 -coordinate. Thus

$$J \cap \sum_{i \in C} H_i = \{0\},$$

which proves privacy.

4.2 Relation to standard duality and pullback

The CDC scheme is a participant-wise image of the standard dual. This comparison explains both the dimension decrease and the pullback of nonnegative lower bounds to the original scheme.

Proposition 4.2 (CDC as a componentwise image of the standard dual).

Let $S_i = \text{im } p_i^* \subseteq C_\Pi^*$ be the standard dual spaces of Section 2.3. There is a natural linear map

$$\eta^* : C_\Pi^* \longrightarrow \mathcal{V}^*$$

such that

$$\eta^*(S_0) = J, \quad \eta^*(S_i) = H_i \quad (1 \leq i \leq n).$$

Moreover,

$$S_0 \xrightarrow[\cong]{\eta^*} J, \quad S_i \xrightarrow{\eta^*} H_i,$$

so $\dim H_i \leq \dim S_i \leq d_i$ for every participant.

Proof. Let $\iota_i : U_i \hookrightarrow T_i$ be the inclusion and define

$$\eta : \mathcal{V} \longrightarrow C_\Pi, \quad \eta(x) = (-\Sigma(x), \iota_1 \bar{\pi}_1(x), \dots, \iota_n \bar{\pi}_n(x)).$$

The minimal-decomposition identities give

$$-\Sigma(x) + \sum_{i=1}^n \iota_i \bar{\pi}_i(x) = 0,$$

so $\eta(x) \in C_\Pi$. Dualizing, for every participant i ,

$$\eta^* p_i^* = \bar{\pi}_i^* \iota_i^*.$$

Since $\iota_i^* : T_i^* \twoheadrightarrow U_i^*$ is surjective and $\bar{\pi}_i^* : U_i^* \rightarrow H_i$ is an isomorphism onto its image,

$$\eta^*(S_i) = \text{im}(\bar{\pi}_i^* \iota_i^*) = H_i.$$

Thus $\eta^*|_{S_i} : S_i \twoheadrightarrow H_i$ and $\dim H_i \leq \dim S_i \leq d_i$.

For the secret coordinate, the zeroth component of η is $-\Sigma$, hence $\eta^*(S_0) = J$. Since $\dim S_0 = d_0 = \dim J$, this restriction is an isomorphism. Therefore CDC preserves the secret space and may further compress each participant space.

The proposition makes the distinction with ordinary duality precise. The standard dual uses the full share space T_i before passing to S_i , whereas CDC first passes to the component span U_i and realizes U_i^* in the minimal-coalition block space. In addition, every vector of H_i has zero coordinates on blocks $A \not\equiv i$, and every incident-block projection is surjective.

Corollary 4.3 (CDC pullback principle). *Fix a class of base fields and let $a_1, \dots, a_n \geq 0$ and $\beta \in \mathbb{R}$. Suppose that for every linear scheme Π for Γ over this class, there exists a choice of minimal decompositions whose CDC image*

$$\Pi^c = (\mathcal{V}^*; J, H_1, \dots, H_n)$$

satisfies

$$\sum_i a_i \dim H_i \geq \beta d_0,$$

then every such scheme Π satisfies

$$\sum_i a_i d_i \geq \beta d_0.$$

Proof. For the chosen CDC image of Π , Theorem 4.1 gives $\dim H_i \leq d_i$ for every i . Since $a_i \geq 0$,

$$\sum_i a_i d_i \geq \sum_i a_i \dim H_i \geq \beta d_0.$$

4.3 Singleton-intersection normalization

The cyclic argument needs one precise coordinate identity: when an original minimal coalition and a dual minimal coalition meet in exactly one participant, that participant component projects to the identity on the corresponding coordinate copy. The following two lemmas state this identity and its dimension consequence.

Lemma 4.4 (Support-forcing identity). *Let $(J, H_1, \dots, H_n)$ be a CDC image for Γ^* , put $K = T_0^*$, and let*

$$j : K \longrightarrow J, \quad j(\varphi) = (\varphi)_{A \in \min \Gamma},$$

be the diagonal secret isomorphism, where each $T_{0,A}^*$ is identified with $T_0^* = K$ through the tautological identification $T_{0,A} \cong T_0$.

Fix $B \in \min \Gamma^*$. Since Π^c is a perfect linear scheme for Γ^* with secret space J , the Minimal Subspace Lemma applied to Π^c at the minimal qualified coalition B supplies subspaces $M_i^B \subseteq H_i$ and isomorphisms

$$\mu_{B,i}^c : J \longrightarrow M_i^B \subseteq H_i \quad (i \in B), \quad \psi = \sum_{i \in B} \mu_{B,i}^c(\psi) \quad (\psi \in J).$$

Define the typed component maps of B by

$$\nu_{B,i} := \mu_{B,i}^c \circ j : K \longrightarrow M_i^B \subseteq H_i \subseteq \mathcal{V}^* \quad (i \in B). \quad (4.6)$$

Each $\nu_{B,i}$ is injective, being a composite of two injective maps, and

$$j = \sum_{i \in B} \nu_{B,i} \quad (4.7)$$

as an identity of linear maps $K \rightarrow \mathcal{V}^*$; the common ambient space $\mathcal{V}^*$ is what makes the sum meaningful, since j takes values in J and each $\nu_{B,i}$ takes values in H_i . The family $(\nu_{B,i})_{i \in B}$ depends on the choice of Minimal Subspace Lemma decomposition for Π^c at B and is not unique.

If $A \in \min \Gamma$, then

$$\sum_{i \in A \cap B} \text{pr}_A \nu_{B,i} = I_K, \quad (4.8)$$

in particular, if $A \cap B = \{i\}$, then

$$\text{pr}_A \nu_{B,i} = I_K, \quad (4.9)$$

where $\text{pr}_A : \mathcal{V}^* \rightarrow T_{0,A}^* \cong K$ is the block projection (2.5). In particular, the left-hand sides of (4.8) and (4.9) do not depend on the choice made in (4.6).

Proof. For $j \in B \setminus A$, block support gives $\text{pr}_A(H_j) = 0$ and hence $\text{pr}_A \nu_{B,j} = 0$. Applying pr_A to (4.7) therefore leaves

$$\sum_{i \in A \cap B} \text{pr}_A \nu_{B,i} = I_K,$$

the last equality holds because j is diagonal. The right-hand side is independent of the chosen decomposition, which proves the final assertion.

Lemma 4.5 (Identity-block splitting). *Let $B \in \min \Gamma^*$, let $i \in B$, and let $\nu_{B,i} : K \rightarrow H_i$ be a typed component map from Lemma 4.4. If $A \in \min \Gamma$ satisfies $A \cap B = \{i\}$, put*

$$Q_{A,i} := \ker(\text{pr}_A : H_i \rightarrow K).$$

Then

$$H_i = \nu_{B,i}(K) \oplus Q_{A,i}, \quad \dim Q_{A,i} = \dim H_i - d_0.$$

Proof. By Lemma 4.4, $\text{pr}_A \nu_{B,i} = I_K$. For $h \in H_i$,

$$h = \nu_{B,i}(\text{pr}_A h) + (h - \nu_{B,i}(\text{pr}_A h)),$$

and the second summand lies in $Q_{A,i}$. If $\nu_{B,i}(s) \in Q_{A,i}$, then $s = \text{pr}_A \nu_{B,i}(s) = 0$, so the sum is direct. The dimension formula follows.

4.4 Comparison edges with CDC coordinates

The singleton-intersection identity lets an edge comparison be read in specified coalition coordinates. Two edge types are needed later: anchored discrepancies for the three nonclosing edges and a two-coordinate transition for the closing edge.

At a selected vertex v , choose $B_v \in \min \Gamma^*$ and a Minimal Subspace Lemma decomposition

$$j = \sum_{i \in B_v} \nu_{v,i}, \quad \nu_{v,i} : K \rightarrow H_i.$$

A *CDC block-comparison diagram* is a finite undirected participant-labelled comparison diagram together with the block readings $\text{pr}_A \nu_{v,i}$, where $A \in \min \Gamma$. Forgetting these readings leaves only the ordinary component-comparison skeleton.

Anchored defect edges. Let an edge $e = \{v, w\}$ be labelled by $i \in B_v \cap B_w$. Choose an ordered presentation (v, w) of the edge and an original block A such that

$\text{pr}_A \nu_{w,i} = I_K$. We use the A -reading of the v -component as the comparison coefficient and subtract the corresponding w -component; the resulting discrepancy has zero A -block. Define

$$R_{A;v,w} := \nu_{v,i} - \nu_{w,i}(\text{pr}_A \nu_{v,i}). \quad (4.10)$$

Then $\text{pr}_A R_{A;v,w} = 0$, so, with the notation of Lemma 4.5,

$$R_{A;v,w}(K) \subseteq Q_{A,i}.$$

For another block A' , the map $\text{pr}_{A'} R_{A;v,w}$ is a block readout of this discrepancy. Thus the discrepancy depends not only on the edge but also on the anchor block A and on which endpoint carries the identity reading. In characteristic two the minus sign in (4.10) is a plus sign.

Two-block transition edges. Let an edge $e = \{v, w\}$ be labelled by i , and suppose that two original blocks A_0, A_1 satisfy

$$\text{pr}_{A_1} \nu_{v,i} = I_K, \quad \text{pr}_{A_0} \nu_{w,i} = I_K.$$

Set

$$M_0 := \text{pr}_{A_0} \nu_{v,i}, \quad M_1 := \text{pr}_{A_1} \nu_{w,i}. \quad (4.11)$$

If $\nu_{v,i}(s) = \nu_{w,i}(t)$, reading this equality in the two blocks gives

$$t = M_0 s, \quad s = M_1 t = M_1 M_0 s.$$

Thus $M_1 M_0$ is the return map associated with the two block readings; when the edge closes a cycle, $I + M_1 M_0$ is the cycle-closing defect in characteristic two.

Lemma 4.6 (Transition-edge defect bound). *In the setting above, suppose $\dim K = d_0$ and $\dim H_i = d_0 + e_i$. Then*

$$\text{rank}(I - M_1 M_0) \leq e_i.$$

In characteristic two this becomes

$$\text{rank}(I + M_1 M_0) \leq e_i.$$

Proof. The injective component maps $\nu_{v,i}, \nu_{w,i} : K \rightarrow H_i$ have d_0 -dimensional images, so

$$\dim(\nu_{v,i}(K) \cap \nu_{w,i}(K)) \geq d_0 - e_i.$$

If $\nu_{v,i}(s) = \nu_{w,i}(t)$, the two block readings give $t = M_0 s$ and $s = M_1 t$. Hence $s \in \ker(I - M_1 M_0)$. Since $\nu_{v,i}$ is injective, the intersection embeds into this kernel. Therefore $\dim \ker(I - M_1 M_0) \geq d_0 - e_i$, which is equivalent to the rank bound.

5 The One-Cycle Diagram on a CDC Image

The CDC identities are now specialized to the four-coalition cycle for $\hat{N}^*$ in Figure 5.1. The calculation isolates the three nonclosing defects and the closing rank bound needed by Section 6.

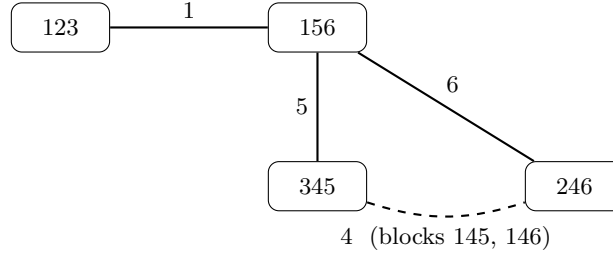


Fig. 5.1. The full comparison diagram for the compression facet. The three solid edges form the channel star centred at 156. The dashed participant-4 edge closes the unique cycle; its readings at blocks 145 and 146 give the transition maps M_0 and M_1 . Starting with $s \in K$, one traversal of the cycle returns $M_1 M_0 s$ to the original copy of K . Thus $M_1 M_0$ is the cycle return map, and $D = I + M_1 M_0$ is the cycle-closing defect in characteristic two.

5.1 Coalition coordinates on the four vertices

Fix a characteristic-two scheme for $\hat{N}$ and pass to its CDC image. The four dual minimal coalitions in Figure 5.1 are now decomposed in the common coalition-indexed coordinate space.

Start from an arbitrary characteristic-two linear scheme for $\hat{N}$ with secret dimension d_0 and share dimensions d_i , and apply Theorem 4.1. We obtain a scheme

$$(J, H_1, \dots, H_6)$$

for $\hat{N}^*$ with

$$h_i := \dim H_i \leq d_i, \quad \dim J = d_0.$$

For $i \in \{1, 4, 5, 6\}$ put

$$e_i = h_i - d_0.$$

Each of these participants occurs in a minimal qualified coalition of $\hat{N}$, so coordinate surjectivity in Theorem 4.1 gives $e_i \geq 0$. Moreover, whenever $A \in \min \hat{N}$ contains i , the projection $H_i \rightarrow T_{0,A}^*$ has kernel dimension e_i .

Put $K = T_0^*$ and let $j : K \rightarrow J$ be the diagonal isomorphism from Lemma 4.4. Thus $\text{pr}_A j = I_K$ for every $A \in \min \hat{N}$. Choose Minimal Subspace Lemma decompositions of J for the four minimal qualified coalitions 156, 123, 345, 246 of

$\widehat{N}^*$. We name their component maps according to the coalition in which they occur:

$$\begin{aligned} 156 : \quad & \alpha_1 : K \rightarrow H_1, \alpha_5 : K \rightarrow H_5, \alpha_6 : K \rightarrow H_6, & j = \alpha_1 + \alpha_5 + \alpha_6, \\ 123 : \quad & \beta_1 : K \rightarrow H_1, \beta_2 : K \rightarrow H_2, \beta_3 : K \rightarrow H_3, & j = \beta_1 + \beta_2 + \beta_3, \\ 345 : \quad & \gamma_3 : K \rightarrow H_3, \gamma_4 : K \rightarrow H_4, \gamma_5 : K \rightarrow H_5, & j = \gamma_3 + \gamma_4 + \gamma_5, \\ 246 : \quad & \delta_2 : K \rightarrow H_2, \delta_4 : K \rightarrow H_4, \delta_6 : K \rightarrow H_6, & j = \delta_2 + \delta_4 + \delta_6. \end{aligned}$$

For example $\alpha_1 = \nu_{156,1}$. These are equalities of linear maps into $\mathcal{V}^*$. For $f : K \rightarrow H_i$ and $A \in \min \widehat{N}$, write

$$[f]_A := \text{pr}_A f \in \text{End}(K)$$

for its typed A -block coordinate.

For each component used below, the support-forcing rule Lemma 4.4 gives the identity coordinates in the third column:

component map	dual coalition B	original blocks A with $A \cap B = \{i\}$
α_1	156	123, 124, 134
β_1	123	145, 146, 156
α_5	156	25, 345
γ_5	345	25, 156
α_6	156	36, 246
δ_6	246	36, 156
γ_4	345	124, 146, 246
δ_4	246	134, 145, 345

(5.1)

The third column lists exactly the singleton intersections. Hence Lemma 4.4 gives the identity on every listed block; for example, $123 \cap 156 = \{1\}$ gives $[\alpha_1]_{123} = I_K$. Write $I = I_K$ below.

5.2 The three nonclosing defect channels

The three solid edges of Figure 5.1 are anchored defect edges in the sense above. From this point to the end of the three-channel calculation, it is useful to abbreviate the block readings by

$$X_{A,v,i} := \text{pr}_A \nu_{v,i}. \quad (5.2)$$

The general kernel and discrepancy notation now specializes as

$$\begin{aligned} Q_1 &:= Q_{156,1}, \quad R_1 := R_{156;156,123}, \quad X := X_{156,156,1} = [\alpha_1]_{156}, \\ Q_5 &:= Q_{25,5}, \quad R_5 := R_{25;156,345}, \\ Q_6 &:= Q_{36,6}, \quad R_6 := R_{36;156,246}. \end{aligned}$$

By Lemma 4.5, $\dim Q_1 = e_1$, $\dim Q_5 = e_5$, and $\dim Q_6 = e_6$. Moreover, (4.10) and the identity readings in (5.1) give, in characteristic two,

$$R_1 = \alpha_1 + \beta_1 X, \quad R_5 = \alpha_5 + \gamma_5, \quad R_6 = \alpha_6 + \delta_6,$$

with $R_j : K \rightarrow Q_j$ for $j \in \{1, 5, 6\}$. Thus the three channels are instances of the general anchored-discrepancy construction rather than new definitions.

For participant 1, the observable coordinates

$$C = \text{pr}_{145} R_1, \quad C' = \text{pr}_{146} R_1$$

factor through R_1 . Since $[\beta_1]_{145} = [\beta_1]_{146} = I$,

$$[\alpha_1]_{145} = X + C, \quad [\alpha_1]_{146} = X + C'. \quad (5.3)$$

For participant 5, define

$$B_5 = \text{pr}_{145} |_{Q_5} : Q_5 \rightarrow K, \quad E = B_5 R_5 = [R_5]_{145}.$$

For participant 6, define

$$F = \text{pr}_{146} R_6.$$

Thus F factors through R_6 .

The remaining observable is

$$N = [R_5]_{156} + [R_6]_{156}.$$

It factors through (R_5, R_6) and hence through $R = (R_1, R_5, R_6)$. Projecting the 156 decomposition onto the 156 block gives

$$X + [\alpha_5]_{156} + [\alpha_6]_{156} = I.$$

The table gives $[\gamma_5]_{156} = [\delta_6]_{156} = I$, and therefore

$$[\alpha_5]_{156} = I + [R_5]_{156}, \quad [\alpha_6]_{156} = I + [R_6]_{156}.$$

In characteristic two this yields

$$N = I + X. \quad (5.4)$$

At the 145 block, the 156 decomposition and block support give

$$[\alpha_5]_{145} = I + X + C.$$

Since $E = [\alpha_5 + \gamma_5]_{145}$,

$$[\gamma_5]_{145} = I + X + C + E = N + C + E. \quad (5.5)$$

By Lemma 4.5, applied to γ_5 and the block 25,

$$H_5 = \gamma_5(K) \oplus Q_5.$$

Moreover, $\text{pr}_{145} : H_5 \rightarrow K$ is surjective by Theorem 4.1. Hence (5.5) implies

$$K = \text{im}(N + C) + \text{im } B_5, \quad (5.6)$$

because $E = B_5 R_5$ already has image in $\text{im } B_5$.

5.3 The closing participant-4 comparison

For the 345 decomposition, the 145- and 146-coordinates of γ_4 are

$$([\gamma_4]_{145}, [\gamma_4]_{146}) = (M_0, I), \quad M_0 := X + C + E = I + N + C + E. \quad (5.7)$$

Indeed, $[\gamma_4]_{145} = I + [\gamma_5]_{145}$, while $[\gamma_4]_{146} = I$ follows directly from Lemma 4.4.

For the 246 decomposition, Lemma 4.4 gives $[\delta_4]_{145} = I$. To obtain its 146-coordinate, project the 156 decomposition onto block 146:

$$[\alpha_1]_{146} + [\alpha_5]_{146} + [\alpha_6]_{146} = I.$$

Here $[\alpha_1]_{146} = X + C'$ by (5.3), while $[\alpha_5]_{146} = 0$ by block support. Therefore

$$[\alpha_6]_{146} = I + X + C'.$$

Since $F = [\alpha_6 + \delta_6]_{146}$,

$$[\delta_6]_{146} = F + I + X + C'.$$

Finally, $[\delta_2]_{146} = 0$ by block support, so the 146-coordinate of $j = \delta_2 + \delta_4 + \delta_6$ gives

$$[\delta_4]_{146} = I + [\delta_6]_{146} = X + C' + F.$$

Thus

$$([\delta_4]_{145}, [\delta_4]_{146}) = (I, M_1), \quad M_1 := X + C' + F = I + N + C' + F. \quad (5.8)$$

The participant-4 edge is a two-block transition edge with $v = 345$, $w = 246$, $A_0 = 145$, $A_1 = 146$, and $\dim H_4 = d_0 + e_4$. Therefore Lemma 4.6 gives

$$\text{rank}(I + M_1 M_0) \leq e_4,$$

which supplies the closing-edge rank bound.

The calculation above is used in the next section only through the following interface.

Proposition 5.1 (One-cycle data). *Let $(J, H_1, \dots, H_6)$ be a characteristic-two CDC image of $\tilde{N}$, put $K = T_0^*$, $h_i = \dim H_i$ and $e_i = h_i - d_0$. Then there exist spaces Q_1, Q_5, Q_6 of dimensions e_1, e_5, e_6 , maps $R_j : K \rightarrow Q_j$, endomorphisms N, C, C', F of K and a map $B_5 : Q_5 \rightarrow K$ such that*

- (i) N factors through $R = (R_1, R_5, R_6)$.
- (ii) C and C' factor through R_1 .
- (iii) F factors through R_6 , and $E := B_5 R_5$.
- (iv) $K = \text{im}(N + C) + \text{im } B_5$;
- (v) with $M_0 = I + N + C + E$ and $M_1 = I + N + C' + F$,

$$\text{rank}(I + M_1 M_0) \leq e_4.$$

The notation in the proposition has four roles:

role	objects
defect channels	R_1, R_5, R_6
channel spaces	Q_1, Q_5, Q_6
block readouts	C, C', E, F, N
transition maps	M_0, M_1

The map $B_5 : Q_5 \rightarrow K$ is the readout used both in $E = B_5 R_5$ and in the spanning condition.

Proof. Items (i)–(iii) are established in Section 5.2; the spanning identity in item (iv) is (5.6); and item (v) is the transition-edge bound from Section 5.3.

6 A Three-Defect Rank Lemma and the Compression Facet

The one-cycle calculation has reduced the remaining lower bound to a linear-algebraic rank estimate. This section proves that estimate and then applies it immediately to obtain the CDC facet.

6.1 The three-defect rank lemma

The scalar case. Before the general statement, take $d_0 = 1$, so that $K = \mathbb{F}$ and every endomorphism is a scalar. A channel of dimension zero forces the corresponding map to vanish. If $e_1 = e_5 = e_6 = 0$ then $N = C = C' = E = F = 0$, so $M_0 = M_1 = 1$ and $D = 1 + 1 = 0$; but the spanning condition (6.1) reads $\mathbb{F} = \{0\}$, which is false. Hence at least one channel is nonzero, that is $e_1 + e_5 + e_6 \geq 1 = d_0$, and the lemma below is exactly this statement in general dimension. The contribution vector $D_1 = (1, 1, 2, 1, 1, 2)$ of Section 7 realizes $\hat{N}$ with $d_0 = 1$ and attains $c_1 + c_4 + c_5 + c_6 = 5$ with equality, so the scalar case is already tight.

The proof is a single idea: *a kernel element of D is reconstructible from its readings in the three channels, so the kernel cannot be larger than the total channel dimension.* The triple (a, η, ζ) constructed in the proof is precisely that reading.

Lemma 6.1 (Three-defect rank lemma; cycle closing). *Let d_0 be a positive integer and let K be a d_0 -dimensional vector space over a field of characteristic two. Let Q_1, Q_5, Q_6 have dimensions r_1, r_5, r_6 , and let*

$$R_j : K \rightarrow Q_j \quad (j = 1, 5, 6).$$

Set

$$R = (R_1, R_5, R_6) : K \rightarrow Q_1 \oplus Q_5 \oplus Q_6.$$

Let $N, C, C', F \in \text{End}(K)$ and $B_5 : Q_5 \rightarrow K$ be linear maps such that N factors through R , both C and C' factor through R_1 , and F factors through R_6 . Put

$$\begin{aligned} E &= B_5 R_5, \\ M_0 &= I + N + C + E, \\ M_1 &= I + N + C' + F, \\ D &= I + M_1 M_0. \end{aligned}$$

If

$$K = \text{im}(N + C) + \text{im } B_5, \quad (6.1)$$

then

$$\text{rank } D + r_1 + r_5 + r_6 \geq d_0. \quad (6.2)$$

Proof. Let

$$Y = \text{im } R, \quad t = \dim Y, \quad P = N + C.$$

Because N factors through R and C factors through R_1 , the map P factors through R . Hence there is a well-defined surjective map

$$\Lambda : Y \rightarrow W := \text{im } P, \quad \Lambda(Rz) = Pz.$$

Write $s = \dim W$.

All of N, C, C', E, F vanish on $\ker R$. Hence M_0 and M_1 act as the identity on $\ker R$, and, in characteristic two, $D = I + M_1 M_0$ vanishes there. Therefore D factors through R :

$$D = \tilde{D}R$$

for a unique map $\tilde{D} : Y \rightarrow K$. Here the codomain of R has been restricted to $Y = \text{im } R$, so $R : K \twoheadrightarrow Y$ is surjective. Consequently,

$$\text{im } D = \tilde{D}(R(K)) = \tilde{D}(Y) = \text{im } \tilde{D},$$

and hence

$$\text{rank } D = \text{rank } \tilde{D}. \quad (6.3)$$

Put $Z = \ker \tilde{D}$.

The spanning hypothesis (6.1) says that the induced map

$$\overline{B}_5 : Q_5 \rightarrow K/W$$

is surjective. Therefore

$$\dim \ker \overline{B}_5 = r_5 - (d_0 - s). \quad (6.4)$$

Choose linear right inverses

$$\sigma : K/W \rightarrow Q_5 \quad \text{of } \overline{B}_5, \quad \tau : W \rightarrow Y \quad \text{of } \Lambda.$$

Take $y \in Z$, choose $z \in K$ with $Rz = y$, and put $u = M_0z$. Since $Dz = 0$, we have $M_1u = z$. Write $\Delta = C' + C$. The two equations become

$$u + z = Pz + B_5R_5z, \quad (6.5)$$

$$u + z = Pu + \Delta u + Fu. \quad (6.6)$$

Because Δ factors through R_1 and F factors through R_6 , the class of $\Delta u + Fu$ depends only on

$$a = (R_1u, R_6u) \in Q_1 \oplus Q_6.$$

Reducing (6.5)–(6.6) modulo W gives

$$\overline{B}_5(R_5z) = \overline{\Delta u + Fu}.$$

Denote the right-hand side by $\theta(a)$ and set

$$\eta = R_5z - \sigma\theta(a) \in \ker \overline{B}_5. \quad (6.7)$$

Thus R_5z is determined by (a, η) .

Put $p = R_5z$. Substituting (6.5) into (6.6) and cancelling common terms gives

$$P^2z = (I + P)B_5p + \Delta u + Fu =: w. \quad (6.8)$$

The vector $w \in W$ is determined linearly by (a, η) . Since

$$\Lambda(R(Pz)) = P(Pz) = P^2z = w,$$

define

$$\zeta = R(Pz) - \tau w \in \ker \Lambda. \quad (6.9)$$

Equations (6.7)–(6.9) give a linear map

$$\Phi : Z \rightarrow Q_1 \oplus Q_6 \oplus \ker \overline{B}_5 \oplus \ker \Lambda, \quad y \mapsto (a, \eta, \zeta),$$

independent of the chosen lift z , because changing z by an element of $\ker R$ changes none of the displayed quantities.

We claim that Φ is injective. If $a = \eta = \zeta = 0$, then (6.7) gives $R_5z = 0$. Equation (6.8) gives $w = 0$, and (6.9) gives $R(Pz) = 0$. Equation (6.5) now reduces to $u = z + Pz$. Since $R_1u = R_6u = 0$ and $R(Pz) = 0$, we obtain $R_1z = R_6z = 0$. Together with $R_5z = 0$, this gives $Rz = 0$, hence $y = 0$.

Using (6.4) and $\dim \ker \Lambda = t - s$,

$$\begin{aligned} \dim Z &\leq r_1 + r_6 + (r_5 - (d_0 - s)) + (t - s) \\ &= r_1 + r_5 + r_6 - d_0 + t. \end{aligned}$$

Therefore, by (6.3),

$$\text{rank } D = \text{rank } \tilde{D} = t - \dim Z \geq d_0 - (r_1 + r_5 + r_6),$$

which is (6.2).

Necessity of the spanning hypothesis. Without (6.1) the conclusion fails outright. Take $R_1 = R_5 = R_6 = 0$. Then $N = C = C' = E = F = 0$, so $M_0 = M_1 = I$ and, in characteristic two, $D = I + I = 0$. The left-hand side of (6.2) is 0, so the inequality asserts $0 \geq d_0$, which is false for every $d_0 \geq 1$. What fails is precisely (6.1), since $\text{im}(N + C) + \text{im } B_5 = \{0\} \neq K$. Thus the spanning condition is a hypothesis of the lemma and not a technical convenience. In the application to $\hat{N}$, (6.1) is supplied in Section 5 by the surjectivity of pr_{145} on H_5 , which is part of Theorem 4.1.

6.2 The compression inequality

Theorem 6.2 (Compression inequality). *Every characteristic-two linear scheme for $\hat{N}$ satisfies the four-inequality automorphism orbit of*

$$c_1 + c_4 + c_5 + c_6 \geq 5. \quad (6.10)$$

Proof. Apply Theorem 4.1 to the given scheme and let $(J, H_1, \dots, H_6)$, h_i , e_i be as in Proposition 5.1. Items (i)–(iv) of that proposition supply the hypotheses of Lemma 6.1 with $(r_1, r_5, r_6) = (e_1, e_5, e_6)$ and $D = I + M_1 M_0$, so (6.2) gives

$$\text{rank}(I + M_1 M_0) + e_1 + e_5 + e_6 \geq d_0.$$

Combining this with item (v) yields

$$e_1 + e_4 + e_5 + e_6 \geq d_0,$$

and therefore

$$h_1 + h_4 + h_5 + h_6 = 4d_0 + e_1 + e_4 + e_5 + e_6 \geq 5d_0.$$

Since $h_i \leq d_i$ by Theorem 4.1, we get $d_1 + d_4 + d_5 + d_6 \geq 5d_0$. Dividing by d_0 proves (6.10); the other three inequalities follow from the automorphism group (2.16).

6.3 Scope of the rank lemma

The bound is confined to a narrow window on both sides. On one side, (6.2) is automatic when $r_1 + r_5 + r_6 \geq d_0$. On the other, (6.1) gives

$$d_0 \leq \text{rank}(N + C) + \text{rank } B_5 \leq (r_1 + r_5 + r_6) + r_5,$$

so the nontrivial range is

$$r_1 + r_5 + r_6 < d_0 \leq r_1 + 2r_5 + r_6.$$

A complementary lower bound shows that no substantially stronger conclusion is available. If $M_0 x = x$ and $M_1 x = x$, then $M_1 M_0 x = x$ and hence $Dx = 0$; therefore

$$\begin{aligned} \dim \ker D &\geq \dim(\ker(M_0 + I) \cap \ker(M_1 + I)) \\ &\geq d_0 - \text{rank}(M_0 + I) - \text{rank}(M_1 + I) \\ &\geq d_0 - 2(r_1 + r_5 + r_6). \end{aligned}$$

because $M_0 + I$ and $M_1 + I$ both factor through R . Comparing this with the conclusion $\dim \ker D \leq r_1 + r_5 + r_6$ of (6.2) shows that the hypotheses already force $d_0 \leq 3(r_1 + r_5 + r_6)$, and (6.1) sharpens this to $d_0 \leq r_1 + 2r_5 + r_6$. In this sense the constant in (6.2) cannot be improved by more than a bounded factor without further hypotheses.

Finally, the map B_5 appears both in the defect term $E = B_5 R_5$ and in the spanning condition (6.1); this coincidence is used twice in the proof, once to absorb E into $\text{im } B_5$ and once in (6.4), and is therefore part of the statement rather than a normalization.

Both mechanisms are needed for the main theorem. The four inequalities in the orbit of (6.10) and the four tree inequalities of Proposition 3.3 are irredundant facets of the region determined in Section 8, so neither family is implied by the remaining inequalities.

7 Constructions for $\widehat{N}$

To prove sharpness, it remains to realize the vertex orbits of the lower-bound polyhedron. Most are obtained by (λ, ω) -decompositions; the few remaining orbits use direct linear schemes.

7.1 (λ, ω) -decompositions

The (λ, ω) -decomposition of van Dijk, Jackson, and Martin [16] generalizes Stinson's earlier decomposition construction [15]. It combines component access structures so that every qualified coalition is covered at least λ times while every unqualified coalition is covered at most ω times; the difference $\lambda - \omega$ becomes the effective secret multiplicity.

Let $\Gamma_1, \dots, \Gamma_m$ be access structures on the same participant set. They form a (λ, ω) -decomposition of a target Γ if

$$|\{j : A \in \Gamma_j\}| \geq \lambda \quad (A \in \Gamma), \quad |\{j : B \in \Gamma_j\}| \leq \omega \quad (B \notin \Gamma),$$

where $0 \leq \omega < \lambda$. If each Γ_j has a linear scheme with contribution vector $c^{(j)}$, over fields of one common characteristic, then [16] the target Γ has a linear scheme with contribution vector

$$\frac{1}{\lambda - \omega} \sum_{j=1}^m c^{(j)}. \tag{7.1}$$

7.2 Direct schemes and exact checks

Checking criterion. For every direct construction below, correctness and privacy can be checked without enumerating all coalitions. By monotonicity, it is enough

to test correctness on the minimal qualified coalitions and privacy on the maximal unqualified coalitions. In the vector-space model these are the exact rank tests

$$\begin{aligned} \text{rank}(T_A + T_0) &= \text{rank } T_A & (A \in \min \Gamma), \\ \text{rank}(T_B + T_0) &= \text{rank } T_B + d_0 & (B \text{ maximal unqualified}). \end{aligned}$$

All finite-field verification claims below refer to these two tests and use exact row reduction over the displayed field.

A direct extremal scheme. The contribution vector

$$D_1 = (1, 1, 2, 1, 1, 2)$$

is realized over $\mathbb{F}_4 = \mathbb{F}_2[\omega]/(\omega^2 + \omega + 1)$. For scalar secret s and independent uniform r_1, r_2, r_3 , give

participant share	
P_1	$r_1 + r_2 + \omega^2 r_3$
P_2	$s + \omega r_1 + r_2$
P_3	$s + \omega^2 r_3, r_2 + \omega r_3$
P_4	$s + \omega r_1 + \omega^2 r_2 + \omega^2 r_3$
P_5	$r_1 + \omega^2 r_2$
P_6	$s + r_2 + \omega^2 r_3, r_1 + \omega r_2$

For the ten minimal qualified coalitions in (2.12), exact row reduction gives $\text{rank}(T_A + T_0) = \text{rank } T_A$; for the five maximal unqualified coalitions in (2.13), it gives $\text{rank}(T_B + T_0) = \text{rank } T_B + 1$. Hence the displayed spaces form a perfect scheme for $\widehat{N}$. A second direct construction is given in Appendix B.

7.3 Extremal contribution vectors

The uniform point. Appendix B.1 gives five scalar perfect schemes $A_0, \dots, A_4$ whose access structures are

$$F, \quad \widehat{N} + 456, \quad \widehat{N} + 234, \quad \widehat{N} + 135, \quad \widehat{N} + 126,$$

where

$$F := 14 + 25 + 36 + 123 + 156 + 246 + 345$$

is the Fano port. Every qualified coalition of $\widehat{N}$ is qualified in all five components, whereas each unqualified coalition is qualified in at most one, because the five added coalitions are exactly the maximal unqualified sets in (2.13). Applying (7.1) with $(\lambda, \omega) = (5, 1)$ gives a scheme with secret dimension four and every share dimension five. Hence

$$U = (5/4, \dots, 5/4) \in \Sigma_{\text{lin}}^2(\widehat{N}). \quad (7.2)$$

Table 7.1 lists five orbit representatives of the eleven extremal contribution vectors.

Table 7.1. Orbit representatives of the eleven constructed contribution vectors for $\widehat{N}$. The location column points to the displayed witness or to the appendix where its component schemes are specified.

label	representative	orbit	construction	location
D_1	(1, 1, 2, 1, 1, 2)	2	direct $\mathbb{F}_4$ scheme	§7.2
D_2	(1, 1, 2, 2, 2, 1)	4	(2, 1) decomposition	App. B.2
U	$(5/4)^6$	1	(5, 1) decomposition	§7.3; App. B.1
H	(3/2, 1, 3/2, 3/2, 1, 3/2)	2	direct binary scheme	App. B.2
C	(1, 4/3, 4/3, 4/3, 4/3, 4/3)	2	(4, 1) decomposition	App. B.2

Let $\mathcal{V}_{\widehat{N}}$ be the union of these five automorphism orbits. The constructions above and in Appendix B realize every point of $\mathcal{V}_{\widehat{N}}$.

8 The Exact Characteristic-Two Region of $\widehat{N}$

The lower bounds and the constructions now meet. Let $\mathcal{V}_{\widehat{N}}$ be the eleven constructed points from Table 7.1, and define the upward polyhedron

$$\mathcal{I}_{\widehat{N}} := \text{conv}(\mathcal{V}_{\widehat{N}}) + \mathbb{R}_{\geq 0}^6. \quad (8.1)$$

The constructions in Section 7 and Appendix B, together with direct sums and private padding, give $\mathcal{I}_{\widehat{N}} \subseteq \Sigma_{\text{lin}}^2(\widehat{N})$. The thirty inequalities below give the reverse inclusion. The six unit-share facets appear as two families because $\text{Aut}(\widehat{N})$ has participant orbits $\{1, 4\}$ and $\{2, 3, 5, 6\}$.

Table 8.1. The thirty irredundant facets of $\mathcal{I}_{\widehat{N}}$, in six automorphism orbits.

family	representative	size	proof mechanism
U_{line}	$c_1 \geq 1$	2	unit-share
U_{off}	$c_2 \geq 1$	4	unit-share
K_4	$c_3 + c_4 + c_5 + c_6 \geq 5$	8	star-kernel
K_d	$c_3 + c_4 + 2c_5 \geq 5$	8	star-kernel
T	$c_3 + 2c_5 + c_6 \geq 5$	4	nonstar tree
C_{comp}	$c_1 + c_4 + c_5 + c_6 \geq 5$	4	component-dual compression

Theorem 8.1 (Exact contribution region of $\widehat{N}$). *The characteristic-two linear contribution region of $\widehat{N}$ is exactly*

$$\Sigma_{\text{lin}}^2(\widehat{N}) = \mathcal{I}_{\widehat{N}}, \quad \mathcal{I}_{\widehat{N}} = \text{conv}(\mathcal{V}_{\widehat{N}}) + \mathbb{R}_{\geq 0}^6,$$

where $\mathcal{V}_{\widehat{N}}$ is the union of the five vertex orbits in Table 7.1. The region has exactly eleven vertices and thirty irredundant facets, with facet orbits in Table 8.1.

Proof. The constructions above give $\mathcal{I}_{\hat{N}} \subseteq \Sigma_{\text{lin}}^2(\hat{N})$. Conversely, the six unit-share inequalities follow from Lemma 2.1; the sixteen star-kernel inequalities are listed in Appendix A; the four tree inequalities are Proposition 3.3; and the four component-dual compression inequalities are Theorem 6.2. Exact rational H/V conversion of these thirty halfspaces is finite: solving the nonsingular systems of six active facet equalities and retaining the feasible solutions yields precisely the eleven vertices in Table 7.1; the nonnegative facet normals and the six unit inequalities give recession cone $\mathbb{R}_{\geq 0}^6$. Hence their intersection is exactly (8.1), and every characteristic-two linear contribution vector lies in $\mathcal{I}_{\hat{N}}$.

Corollary 8.2 (Exact maximum and average information ratios).

$$\sigma_{\max}^{(2)}(\hat{N}) = \sigma_{\text{av}}^{(2)}(\hat{N}) = \frac{5}{4}.$$

Proof. Let $M = \max_i c_i$. Every non-unit facet inequality in Table 8.1 has coefficient sum four and right-hand side five; the star inequality

$$c_3 + c_4 + c_5 + c_6 \geq 5 \text{ of Appendix A already suffices, and gives } 4M \geq 5.$$

The uniform construction (7.2) attains $M = 5/4$.

For the average ratio, Theorem 8.1 reduces the minimization of $\sum_i c_i$ to the eleven vertices in Table 7.1, because the recession cone is nonnegative. The sums of the five orbit representatives D_1, D_2, U, H, C are respectively 8, 9, 15/2, 8, 23/3. Thus the minimum is 15/2, attained by U , and division by six gives $\sigma_{\text{av}}^{(2)}(\hat{N}) = 5/4$.

9 Conclusion

The relaxed-line non-Fano port requires two different lower-bound mechanisms. The JK star comparison extends naturally to trees, but an argument based only on the ordinary one-edge/one-share edge-difference map has no positive rank surplus on a cycle. CDC supplies the coalition-indexed coordinate compatibility needed for the missing cyclic inequality. Together with matching constructions, these bounds determine the complete characteristic-two linear contribution region of $\hat{N}$ and give both information ratios 5/4.

There is also a natural direction beyond the present access structure. Peña-Macias [11], building on the JK access-structure method, used secret-sharing ideas to derive characteristic-dependent linear-rank inequalities. It would be interesting to determine whether the tree comparison or the additional block compatibilities supplied by CDC lead to new characteristic-dependent rank inequalities, and whether analogous cyclic constraints yield stronger lower bounds for larger access structures.

Acknowledgment of AI Assistance

During the development of this manuscript, the authors used AI tools, including ChatGPT (OpenAI), for mathematical discussion and editorial assistance. All mathematical claims, proofs, computations, and final formulations were reviewed and verified by the authors, who take full responsibility for the content.

References

1. Bamiloshin, M., Ben-Efraim, A., Farràs, O., Padró, C.: Common information, matroid representation, and secret sharing for matroid ports. *Designs, Codes and Cryptography* **89**(1), 143–166 (2021). <https://doi.org/10.1007/s10623-020-00811-1>
2. Beimel, A.: Secret-sharing schemes: A survey. In: *Coding and Cryptology*, LNCS 6639, pp. 11–46. Springer (2011). https://doi.org/10.1007/978-3-642-20901-7_2
3. Blakley, G.R.: Safeguarding cryptographic keys. In: *Proceedings of the 1979 AFIPS National Computer Conference*, pp. 313–318 (1979). <https://doi.org/10.1109/MARK.1979.8817296>
4. Brickell, E.F., Davenport, D.M.: On the classification of ideal secret sharing schemes. *Journal of Cryptology* **4**, 123–134 (1991). <https://doi.org/10.1007/BF00196772>
5. Csirmaz, L.: The size of a share must be large. *Journal of Cryptology* **10**(4), 223–231 (1997). <https://doi.org/10.1007/s001459900029>
6. Dougherty, R., Freiling, C., Zeger, K.: Characteristic-dependent linear rank inequalities with applications to network coding. *IEEE Transactions on Information Theory* **61**(5), 2510–2530 (2015). <https://doi.org/10.1109/TIT.2015.2403361>
7. Farràs, O., Kaced, T., Martín, S., Padró, C.: Improving the linear programming technique in the search for lower bounds in secret sharing. *IEEE Transactions on Information Theory* **66**(11), 7088–7100 (2020). <https://doi.org/10.1109/TIT.2020.3005706>
8. Jafari, A., Khazaei, S.: On abelian and homomorphic secret sharing schemes. *Journal of Cryptology* **34**(4), 43 (2021). <https://doi.org/10.1007/s00145-021-09410-2>
9. Martín, S., Padró, C., Yang, A.: Secret sharing, rank inequalities, and information inequalities. *IEEE Transactions on Information Theory* **62**(1), 599–609 (2016). <https://doi.org/10.1109/TIT.2015.2500232>
10. Padró, C., Vázquez, L., Yang, A.: Finding lower bounds on the complexity of secret sharing schemes by linear programming. *Discrete Applied Mathematics* **161**(7–8), 1072–1084 (2013). <https://doi.org/10.1016/j.dam.2012.10.020>
11. Peña-Macias, V.: Access structures for finding characteristic-dependent linear rank inequalities. *Kybernetika* **59**(2), 198–208 (2023). <https://doi.org/10.14736/kyb-2023-2-0198>
12. Peña-Macias, V., Sarria, H.: Characteristic-dependent linear rank inequalities via complementary vector spaces. *Journal of Information and Optimization Sciences* **42**(2), 345–369 (2021). <https://doi.org/10.1080/02522667.2019.1668157>
13. Simonis, J., Ashikhmin, A.: Almost affine codes. *Designs, Codes and Cryptography* **14**, 179–197 (1998). <https://doi.org/10.1023/A:1008244215660>
14. Shamir, A.: How to share a secret. *Communications of the ACM* **22**(11), 612–613 (1979). <https://doi.org/10.1145/359168.359176>
15. Stinson, D.R.: Decomposition constructions for secret-sharing schemes. *IEEE Transactions on Information Theory* **40**(1), 118–125 (1994). <https://doi.org/10.1109/18.272461>
16. van Dijk, M., Jackson, W.-A., Martin, K.M.: A general decomposition construction for incomplete secret sharing schemes. *Designs, Codes and Cryptography* **15**(3), 301–321 (1998). <https://doi.org/10.1023/A:1008381427667>
17. Seymour, P.D.: On secret-sharing matroids. *Journal of Combinatorial Theory, Series B* **56**(1), 69–73 (1992). [https://doi.org/10.1016/0095-8956\(92\)90007-K](https://doi.org/10.1016/0095-8956(92)90007-K)

A The Sixteen Star-Kernel Facets

All sixteen inequalities have right-hand side five:

$$\begin{array}{ll}
c_3 + c_4 + c_5 + c_6 \geq 5, & c_3 + c_4 + 2c_5 \geq 5, \\
2c_3 + c_4 + c_5 \geq 5, & c_2 + c_4 + 2c_6 \geq 5, \\
c_2 + c_4 + c_5 + c_6 \geq 5, & c_2 + c_3 + c_4 + c_6 \geq 5, \\
c_2 + c_3 + c_4 + c_5 \geq 5, & 2c_2 + c_4 + c_6 \geq 5, \\
c_1 + c_5 + 2c_6 \geq 5, & c_1 + 2c_5 + c_6 \geq 5, \\
c_1 + c_3 + c_5 + c_6 \geq 5, & c_1 + c_2 + c_5 + c_6 \geq 5, \\
c_1 + c_2 + c_3 + c_6 \geq 5, & c_1 + c_2 + c_3 + c_5 \geq 5, \\
c_1 + c_2 + 2c_3 \geq 5, & c_1 + 2c_2 + c_3 \geq 5.
\end{array}$$

They split into the K_4 and K_d orbits of Table 8.1; the two representatives displayed there, together with the automorphisms in (2.16), generate all sixteen inequalities.

B Construction Witnesses for $\widehat{N}$

This appendix gives the construction witnesses for the contribution-vector types not displayed in Section 7.

B.1 Scalar component schemes

Work over $\mathbb{F}_4 = \mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1)$. In each template, s is the scalar component secret and r_1, r_2 are fresh independent randomizers.

P_1	P_2	P_3	P_4	P_5	P_6
$A_0 \ r_1$	r_2	$s + r_1 + r_2$	$s + r_1$	$s + r_2$	$r_1 + r_2$
$A_1 \ s + r_1 + r_2$	r_1	r_2	$r_1 + \alpha r_2$	$s + r_1$	$s + r_2$
$A_2 \ s + r_1 + r_2$	$s + r_1$	$s + r_2$	$r_1 + \alpha r_2$	r_1	r_2
$A_3 \ r_1 + \alpha r_2$	r_1	$s + r_2$	$s + r_1 + r_2$	$s + r_1$	r_2
$A_4 \ r_1 + \alpha r_2$	$s + r_1$	r_2	$s + r_1 + r_2$	r_1	$s + r_2$

Their minimal qualified structures are respectively

$$F, \quad \widehat{N} + 456, \quad \widehat{N} + 234, \quad \widehat{N} + 135, \quad \widehat{N} + 126,$$

where $F := 14 + 25 + 36 + 123 + 156 + 246 + 345$. Exact rank calculation verifies each statement.

B.2 The remaining three contribution-vector types

For

$$D_2 = (1, 1, 2, 2, 2, 1),$$

use the two component structures $\widehat{N} + 126$ and $3 + 4 + 5$. The first is realized by template A_4 above. The second has the scalar ideal scheme that gives the secret s to participants 3, 4, 5 and no share to participants 1, 2, 6. Every qualified coalition of $\widehat{N}$ is qualified in both components, while every maximal unqualified coalition in (2.13) is qualified in at most one. Thus $(\lambda, \omega) = (2, 1)$ and (7.1) gives D_2 .

For

$$H = (3/2, 1, 3/2, 3/2, 1, 3/2),$$

take secret $(s_1, s_2) \in \mathbb{F}_2^2$ and independent uniform $r_1, \dots, r_6$ and give

participant share	
P_1	$r_1 + r_4, r_2 + r_5, r_3 + r_6$
P_2	$s_1 + r_3, r_2$
P_3	$s_2 + r_4, r_1 + r_5, r_6$
P_4	$s_1 + r_1, s_2 + r_2 + r_4, r_3 + r_5$
P_5	$s_2 + r_2, r_3$
P_6	$s_1 + r_6, r_4, r_5$

Using the rank criterion of Section 7, exact binary row reduction gives rank increment 0 on every minimal qualified coalition in (2.12) and increment 2 on every maximal unqualified coalition in (2.13); hence this is a perfect scheme for $\widehat{N}$.

Finally,

$$C = \left(1, \frac{4}{3}, \frac{4}{3}, \frac{4}{3}, \frac{4}{3}, \frac{4}{3}\right)$$

is obtained by a $(4, 1)$ decomposition of the four access structures

$$\begin{aligned} &F, \\ &\widehat{N} + 135, \\ &\widehat{N} + 126, \\ &23 + 24 + 25 + 34 + 36 + 45 + 46 + 56. \end{aligned}$$

Their contribution vectors are $c^{(1)} = c^{(2)} = c^{(3)} = (1, 1, 1, 1, 1, 1)$, supplied by the scalar $\mathbb{F}_4$ templates A_0, A_3, A_4 of Appendix B.1, and $c^{(4)} = (0, 1, 1, 1, 1, 1)$, supplied by the following binary two-dimensional ideal scheme: for secret (s_1, s_2) and randomness r_1, r_2 , give

participant share	
P_1	—
P_2	$s_1 + r_1, s_2 + r_2$
P_3	r_1, r_2
P_4	$s_2 + r_1 + r_2, s_1 + s_2 + r_1$
P_5	r_1, r_2
P_6	$s_1 + r_1, s_2 + r_2$

After scalar extension to $\mathbb{F}_4$, every qualified coalition of $\widehat{N}$ is qualified in all four components and every maximal unqualified coalition in at most one, so $(\lambda, \omega) = (4, 1)$. Formula (7.1) therefore gives $\frac{1}{3}(3, 4, 4, 4, 4, 4) = C$; realized with two-dimensional component secrets this is a scheme of secret dimension 6 and share dimensions $(6, 8, 8, 8, 8, 8)$.

C Completion of the Standard Non-Fano Port N

Jafari and Khazaei [8] left one unrealized characteristic-two orbit, represented by the vector

$$v_N = \left(\frac{5}{3}, 1, 1, \frac{4}{3}, \frac{4}{3}, \frac{4}{3} \right).$$

Here the standard non-Fano port is

$$N = 14 + 25 + 36 + 123 + 156 + 246 + 345 + 456.$$

The following binary scheme realizes v_N . For secret $(s_1, s_2, s_3) \in \mathbb{F}_2^3$ and independent uniform randomness $r_1, \dots, r_8$, the participant shares are:

P_1	P_2	P_3	P_4	P_5	P_6
$s_1 + r_1 + r_2 + r_3 + r_4 + r_5 + r_6 + r_7$	$s_2 + r_1$	$s_2 + s_3 + r_3 + r_6 + r_7 + r_8$	$s_1 + s_2 + r_1 + r_2 + r_3 + r_4 + r_5 + r_6 + r_7$	$s_3 + r_1$	$s_3 + r_3 + r_6 + r_7 + r_8$
$s_1 + s_2 + r_1 + r_6 + r_8$ $r_5 + r_8$	$s_2 + s_3 + r_2$ $s_1 + r_3$	$r_1 + r_2 + r_4 + r_5 + r_6$ $s_3 + r_1 + r_2 + r_3 + r_5 + r_7$	$s_1 + s_2 + s_3 + r_1 + r_6 + r_8$ $s_1 + s_2 + r_5 + r_8$	$s_1 + s_3 + r_2$ r_3	$s_3 + r_1 + r_2 + r_4 + r_5 + r_6$ $s_1 + r_1 + r_2 + r_3 + r_5 + r_7$
$r_1 + r_2 + r_5 + r_7 + r_8$	—	—	$s_2 + s_3 + r_1 + r_2 + r_3 + r_4 + r_5 + r_7$	$s_2 + s_3 + r_4$	$r_1 + r_2 + r_7$
$s_1 + s_3 + r_3 + r_7 + r_8$	—	—	—	—	—

The share dimensions are $(5, 3, 3, 4, 4, 4)$. Exact binary row reduction gives rank increment 0 after adjoining the secret space for each of the eight minimal qualified coalitions of N , and rank increment 3 for each maximal unqualified coalition 45, 46, 56, 126, 135, 234. Thus the scheme is perfect and realizes v_N . The automorphism group of N permutes participants 1, 2, 3 transitively, so the other two orbit points are obtained by moving the coordinate 5/3 to positions 2 and 3. Together with the JK lower bounds and their previously realized points, this completes the characteristic-two linear contribution region of N .