ON ENTROPIC AND ALMOST MULTILINEAR REPRESENTABILITY OF MATROIDS

LUKAS KÜHNE AND GEVA YASHFE

ABSTRACT. This article is concerned with two notions of generalized matroid representations motivated by information theory and computer science. The first involves representations by discrete random variables and the second approximate representations by subspace arrangements. In both cases we show that there is no algorithm that checks whether such a representation exists. As a consequence, the conditional independence implication problem is undecidable, which gives an independent answer to a question in information theory by Geiger and Pearl that was recently also answered by Cheuk Ting Li. These problems are closely related to problems of characterizing the achievable rates in certain network coding problems and of constructing secret sharing schemes. Our methods to approach these problems are mostly algebraic. Specifically, they involve reductions from the uniform word problem for finite groups and the word problem for sofic groups.

1. INTRODUCTION

1.1. Main results. A matroid is a combinatorial abstraction of linear independence in vector spaces and forests in graph. Classically, a matroid is said to be representable over a field if there exists a set of vectors in some vector space over that field such that the subsets of linearly independent vectors are exactly the independent subsets of the matroid. This article investigates two generalized notions of matroid representability.

1.1.1. Entropic matroids. The first are entropic representations:

Problem 1.1. The entropic matroid representation (EMR) problem asks the following:

Instance: A matroid $M$ on a finite ground set $E$ with rank function $r$.

Question: Does there exist a family of discrete random variables $\{X_e\}_{e \in E}$ and a positive scalar $\lambda \in \mathbb{R}_+$ such that the entropy of the joint distribution scaled by $\lambda$ agrees with the rank of the matroid, more precisely $r(A) = \lambda H(X_A)$ for all subsets $A \subseteq E$.

Matroids for which the EMR problem has a positive answer are called entropic. The class of entropic matroids contains the ones that are representable over a field (also called linear matroids) and multilinear matroids. Entropic matroids possibly go back to Fujishige [Fuj78] and these representations are equivalent to matroid representations by partitions [Mat99] and almost affine codes [SA98].

The first main result of this article is the following:

Theorem 1.2. The entropic matroid representation (EMR) problem is algorithmically undecidable.

In contrast, representability over some field can be decided using Gröbner bases [Oxl11, Thm. 6.8.9]. Generalized matrix representability over a division ring and multilinear representability are also undecidable [KPY20, KY19].
Entropic matroids are related to ideal secret sharing schemes: In the theory of secret sharing schemes one wants to distribute shares of a secret amongst a number of participants. The goal is that only certain authorized subsets of the participants can recover the secret by combining their shares, while other subsets of the participants can recover no information about the secret. See [Sti92] for a detailed explanation. The family of subsets of the participants that can jointly recover the secret is called the access structure.

A secret sharing scheme is ideal if the size of the share given to each participant equals the size of the secret. Brickell and Davenport observed that the access structure of an ideal secret sharing scheme is a matroid and called matroids arising in such a way secret sharing matroids [BD91]. These are the same as the entropic matroids [Mat99]. Martin extended this bijection to connected monotone access structures that potentially don’t admit an ideal secret sharing scheme [Mar91], and Seymour proved that the Vámós matroid is not a secret sharing matroid [Sey92].

Martin asked which connected monotone access structures admit an ideal secret sharing scheme [Mar91]. Theorem 1.2 show that this question is undecidable.

1.1.2. Almost multilinear matroids. The second theme of this paper are approximate representations by subspace arrangements.

Problem 1.3. The almost multilinear matroid representation (AMMR) problem asks the following:

Instance: A matroid $M$ on a finite ground set $E$ with rank function $r$ and a field $F$.

Question: Does there exist for every $\varepsilon > 0$ a vector space $V$ over $F$ together with a collection of subspaces $\{W_e\}_{e \in E}$ and a $c \in \mathbb{N}$ such that

$$\max_{S \subseteq E} \left| r(S) - \frac{1}{c} \dim \left( \sum_{e \in S} W_e \right) \right| < \varepsilon.$$ 

Matroids for which the AMMR problem has a positive answer are called almost multilinear. This class generalizes the class of linear and multilinear matroids and is defined analogously to the class of almost entropic matroids studied by Matúš [Mat07, Mat19]. Almost multilinear matroids are elements of the closure of the cone of realizable polymatroids defined by Kinser [Kin11]. Our second main result of the article is the following.

Theorem 1.4. The almost multilinear matroid representation (AMMR) problem is algorithmically undecidable.

Multilinear matroids found applications to network coding capacity: In [ESG10], El Rouayheb et al. constructed linear network capacity problems equivalent to multilinear matroid representability. Our previous result in [KY19] implies that the question whether an instance of the network coding problem has a linear vector coding solution is undecidable. Theorem 1.4 implies that it is also undecidable whether an instance of the network coding problem has an approximate linear vector coding solution.

A natural extension of both theorems is the question whether almost entropic representability is also undecidable. We believe the techniques of Theorem 1.4 should extend to prove this result, and we aim to accomplish this in a forthcoming article.

1.2. Related work. We attempt to give a concise summary of that part of the literature that is most relevant to this paper, and apologize for any omissions.

Very recently Cheuk Ting Li proved that the conditional independence implication problem is undecidable, as well as that the networking coding problem is undecidable [Li22]. His work became available very late in our writing. The methods used in both papers are related to each other, and also to the methods of [KY19]: all three papers reduce a representability
problem to the uniform word problem for finite groups. The similarity in methods seems to end there: the proof in [Li22] uses different (though related) combinatorial configurations of random variables, and is significantly shorter than ours. It does not cover approximate results like almost-multilinear representability, and we do not know whether it can be used to prove that entropic representability of matroids is undecidable (and thus be applied to show that it is undecidable whether an access structure admits an ideal secret scheme).

Multilinear representations of Dowling geometries were studied by Beimel, Ben-Efraim, Padró, and Tyomkin in [BBEPT14]. This work was extended by Ben-Efraim and Matúš to entropic matroids [MBE20] building on Matúš’ earlier work on these matroids in [Mat99]. We previously used generalized Dowling geometries to prove that the representability problem of multilinear matroids is undecidable [KY19] and, with Rudi Pendavingh, we used more general von Staudt constructions to compare the multilinear matroid representations with representations over division rings [KPY20]. Almost entropic matroids featured prominently in Matúš’ recent article where he proved that algebraic matroids are almost entropic [Mat19].

1.3. Conditional independence implications. Given a finite ground set \( E \), a conditional independence (CI) statement is a triple \((A \perp B \mid C)\) of subsets \( A, B, C \subseteq E \) which encodes the statement “\( A \) is independent from \( B \) given \( C \)”. We say that a family of discrete random variables \( \{X_e\}_{e \in E} \) realizes a CI statement \((A \perp B \mid C)\) if the joint distribution of \( X_A \) and \( X_B \) are probabilistically independent given \( X_C \).

**Problem 1.5.** The conditional independence implication problem (CII) is:

**Instance:** A set \( A \) of CI statements on a finite ground set \( E \) and a CI statement \( c \).

**Question:** Does 

\[
\bigwedge_{A \in A} A \Rightarrow c
\]

hold for every family \( \{X_e\}_{e \in E} \) of discrete random variables? In other words, is it true that whenever a family \( \{X_e\}_{e \in E} \) of discrete random variables realizes all CI statements in \( A \) it also realizes the CI statement \( c \).

In the literature, the sets appearing in CI statements are sometimes defined to be pairwise disjoint. In this paper, we do not make this assumption but note that both formulations are equivalent as shown by Cheuk Ting Li [Li21].

In the 1980s, Pearl and Paz conjectured that there exists a finite set of axioms characterizing all valid CI implication statements [PP86]. This conjecture was later refuted by Studený [Stu90]. Subsequently, Geiger and Pearl proved that the CII problem is decidable under certain conditions on the CI statements and asked whether it is undecidable in general [GP93]. Partial results concerning the CII problem were obtained in [NGSVG13, Li21] and it was shown in [KKNS20] that the CII problem is co-recursively enumerable. Very recently Cheuk Ting Li showed that the CII problem is undecidable [Li22].

An oracle to decide the CII problem can also decide the EMR problem. Therefore we obtain a second independent solution of the long-standing CII problem.

**Corollary 1.6.** The conditional independence implication (CII) problem is algorithmically undecidable.

1.4. Methods and structure of the article. Our results rely on the following ingredients:

(a) We start by recalling the definitions of entropy functions, matroids and their representations, the uniform word problem for finite groups, and sofic groups in Section 2. We collect elementary lemmas from representation theory and field theory in Section 2.8.
(b) Given a finite group, one can define an associated matroid, the so-called Dowling geometry, whose representations are closely related to the representation theoretic properties of the group [Dow73]. We work with a generalization of this construction to finitely presented groups which we present in Section 3. We call the resulting matroids generalized Dowling geometries (GDG). We first used them in [KY19, KPY20]. They are special cases of frame matroids as studied by Zaslavsky in [Zas03]. The idea is to encode group presentations via the von Staudt constructions.

(c) After defining entropic matroids in Section 4, we prove in Section 4.1 that (roughly speaking) the existence of an entropic representation of the GDG of a finitely presented group \([S | R]\) implies the existence of a group homomorphism of \([S | R]\) into a finite group such that images of some elements are nontrivial. Similarly, in Section 9 we show that an almost-multilinear representation corresponds to a homomorphism of \([S | R]\) into a group such that the images of some elements are nontrivial.

(d) This enables us to reduce certain word problems to matroid theoretic representability problems of GDGs. Specifically we use Slobodskoi’s theorem concerning the universal word problem for finite groups for entropic matroids in Section 7 and the word problem for sofic groups for almost multilinear matroids in Section 9.1. We prove the corollary pertaining to the conditional independence implication problem in Section 8.

(e) The main technical difficulty in making this idea work is that the correspondence between GDG representations and group homomorphisms is delicate, and depends on certain additional properties of the presentation and the homomorphism. In Section 6 we perform a procedure we call scrambling on a given group presentation to bring it into a suitable form. This ensures that the scrambled matroids are multilinear which is a notion we recall in Section 5.

(f) As a technical tool we introduce probability space and vector space representations of matroids. In Appendices A and B we show that these notions essentially coincide with entropic and multilinear matroids, respectively. Lastly, we construct (metric) ultraproducts of categories in Appendix C, which we use to investigate almost multilinear matroids.

ACKNOWLEDGMENTS

We would like to thank Tobias Boege, Michael Dobbins, Zlil Sela, and Thomas Zaslavsky for inspiring discussions. We are grateful to Karim Adiprasito for introducing us to the topic of almost multilinear matroids.

2. Preliminaries

2.1. Notation for probability spaces and random variables. An indexed collection of random variables on a probability space \((\Omega, \mathcal{F}, P)\) consists of a set \(E\), a collection of measurable spaces \(\{(\Omega_e, \mathcal{F}_e)\}_{e \in E}\), and a collection of measurable functions \(\{X_e : \Omega \to \Omega_e\}_{e \in E}\).

For convenience, we often write “let \(\{X_e\}_{e \in E}\) be a collection of random variables on \((\Omega, \mathcal{F}, P)\),” and use the notation \(\{(\Omega_e, \mathcal{F}_e)\}_{e \in E}\) for the codomains of the random variables without explicitly naming them. We also denote by \(\{P_e\}_{e \in E}\) the probability measures defined by \(P_e = (X_e)_\ast P\). By definition this implies that each of the transformations

\[
X_e : (\Omega, \mathcal{F}, P) \to (\Omega_e, \mathcal{F}_e, P_e)
\]

is measure-preserving.

Given a collection of random variables \(\{X_e\}_{e \in E}\) on \(\Omega\) as above and a tuple \(S = (s_1, \ldots, s_n)\) with elements in \(E\), we define a measurable space \((\Omega_S, \mathcal{F}_S)\) by \(\Omega_S = \prod_{i=1}^n \Omega_{s_i}\) and \(\mathcal{F}_S = \)
The base of the logarithm is irrelevant for this article, for consistency we work with the natural logarithm throughout. W e set

\[ X_S (\omega) = (X_{s_i} (\omega))_{i=1}^n. \]

On \((\Omega_S, \mathcal{F}_S)\) we define the probability measure \(P_S = (X_S)_* P\) as the pushforward of \(P\).

### 2.2. Entropy functions of discrete random variables.

Let \(\{X_e\}_{e \in E}\) be a collection of discrete random variables on \((\Omega, \mathcal{F}, P)\). The (Shannon) entropy \(H(X_S)\) of the joint distribution of random variable for \(S \subseteq E\) is defined as

\[ H(X_S) := - \sum_{\omega \in \Omega_S} P_S(\omega) \log P_S(\omega). \]

The base of the logarithm is irrelevant for this article, for consistency we work with the natural logarithm throughout. We set \(H(X_S) := \infty\) if the sum in (1) does not converge.

### 2.3. Matroids.

We frequently use standard matroid terminology as for instance explained in Oxley’s text book [Oxl11]. For the reader’s convenience we briefly recall the definition of a matroid.

**Definition 2.1.** A matroid \(M = (E, r)\) is a pair consisting of a finite ground set \(E\) together with a rank function \(r : \mathcal{P}(E) \to \mathbb{N}\) such that

(a) \(r(A) \leq |A|\) for all \(A \subseteq E\),

(b) \(r(A) \leq r(B)\) for all \(A \subseteq B \subseteq E\) (\(r\) is monotone), and

(c) \(r(A \cup B) + r(A \cap B) \leq r(A) + r(B)\) for all \(A, B \subseteq E\) (\(r\) is submodular).

A rank function \(r : \mathcal{P}(E) \to \mathbb{R}_+\) satisfying (b) and (c) is called a polymatroid.

Given a matroid \(M = (E, r)\) we use the following terms:

**Independent sets:** A set \(A \subseteq E\) is called independent if \(r(A) = |A|\) and dependent otherwise.

**Bases:** An independent set of maximal cardinality is called a basis. They are all of the same size and this size is called the rank of the matroid.

**Circuits:** A circuit \(C\) is a minimally dependent subset of \(E\), that is \(C\) is dependent and every proper subset of \(C\) is independent.

**Flats:** A subset \(F \subseteq E\) is called a flat if \(r(F) < r(F \cup \{e\})\) for all \(e \in E \setminus F\).

**Loops:** An element \(e \in E\) is a loop if the set \(\{e\}\) is dependent.

**Simple:** A matroid is simple if every pair \(\{e, e'\} \subseteq E\) is contained in a basis.

**Connected:** A matroid is connected if every pair \(\{e, e'\} \subseteq E\) is contained in a circuit.

### 2.4. Matroid representations.

A main motivation to define matroids stems from linear algebra. Classically, a matroid \(M = (E, r)\) is representable over a field \(\mathbb{F}\) if there exists a family of vectors \(\{v_e\}_{e \in E}\) in a vector space over \(\mathbb{F}\) such that \(r(A) = \dim(\text{span}(\{v_e\}_{e \in A}))\) for all \(A \in E\). The matroid \(M\) is called linear over \(\mathbb{F}\) in this case. Using Gröbner bases one can decide whether a matroid is linear over some field [Oxl11, Theorem 6.8.9].

In this subsection we define various notions of generalized matroid representations that are studied throughout the article.

**Definition 2.2 ([SA98]).** A matroid \(M = (E, r)\) is multilinear over a field \(\mathbb{F}\) if there exist an integer \(c\) and a vector space \(V\) over \(\mathbb{F}\) with subspaces \(\{W_e\}_{e \in E}\) such that for each \(S \subseteq E\)

\[ r(S) = \frac{1}{c} \dim \left( \sum_{e \in S} W_e \right). \]
In this case the vector space $V$ and the indexed family of subspaces $\{W_e\}_{e \in E}$ are called a multilinear representation of $M$, or a representation of $M$ as a c-arrangement. Observe that if we add the constraint $c = 1$ we recover the definition of linear representability.

Given a collection $\{X_e\}_{e \in E}$ of discrete random variables, Fujishige observed that the assignment $H : \mathcal{P}(E) \to \mathbb{R}_+$ given by the entropy function $H(X_S)$ of the joint distribution for $S \subseteq E$ is a polymatroid [Fuj78]. This motivates the following definition:

**Definition 2.3** ([Fuj78]). A matroid $M = (E, r)$ is *entropic* if there exists a family $\{X_e\}_{e \in E}$ of random variables on a discrete probability space $(\Omega, \mathcal{F}, P)$ and a constant $\lambda \in \mathbb{R}_+$ such that for all subsets $A \subseteq E$

$$r(A) = \lambda H(X_A).$$

We now introduce approximate notions of multilinear and entropic matroids.

**Definition 2.4.** A polymatroid $(E, r)$ is *linear* over a field $\mathbb{F}$ if there exists a vector space $V$ together with subspaces $\{W_e\}_{e \in E}$ of $V$ satisfying

$$r(S) = \dim \left( \sum_{e \in S} W_e \right),$$

for all $S \subseteq E$.

A matroid $M = (E, r)$ is *almost multilinear* if for every $\varepsilon > 0$ there exists a linear polymatroid $\left( \tilde{E}, \tilde{r} \right)$ and a $c \in \mathbb{N}$ such that

$$\left\| r - \frac{1}{c} \tilde{r} \right\|_{\infty} = \max_{S \subseteq E} \left| r(S) - \frac{1}{c} \tilde{r}(S) \right| < \varepsilon.$$

Note that we may always assume the ambient vector space $V$ of a linear polymatroid $(E, r)$ is finite dimensional: if the representation is given by the subspaces $\{W_e\}_{e \in E}$ of $V$, we may replace $V$ by $\sum_{e \in E} W_e$, which has dimension $r(E)$.

**Definition 2.5** ([Mat07]). A matroid $(E, r)$ is *almost entropic* if for every $\varepsilon$ there exists a collection of discrete random variables $\{X_e\}_{e \in E}$ and a constant $\lambda \in \mathbb{R}_+$ such that

$$\max_{S \subseteq E} |r(S) - \lambda H(X_S)| < \varepsilon.$$ 

2.5. Metrics.

**Definition 2.6.** Let $n \in \mathbb{N}$. The *normalized Hamming distance* $d_{\text{hamm}}$ is the metric on the symmetric group $S_n$ defined by

$$d_{\text{hamm}}(\sigma, \tau) = \frac{1}{n} |\{i \in [n] \mid \sigma(i) \neq \tau(i)\}|$$

for all $\sigma, \tau \in S_n$.

The normalized Hamming distance satisfies that if $\sigma, \sigma', \tau \in S_n$ then

$$d_{\text{hamm}}(\sigma, \sigma') = d_{\text{hamm}}(\sigma \circ \tau, \sigma' \circ \tau), \quad \text{and similarly} \quad d_{\text{hamm}}(\sigma, \sigma') = d_{\text{hamm}}(\tau \circ \sigma, \tau \circ \sigma').$$

**Definition 2.7.** Let $A, B \in M_n(\mathbb{F})$ be matrices. Their *normalized rank distance* is

$$d_{\text{rk}}(A, B) := \frac{1}{n} \text{rk}(A - B).$$

Similarly, if $f, g \in \text{End}(W)$, where $W$ is a finite dimensional vector space over a field, define

$$d_{\text{rk}}(f, g) = \frac{1}{\dim(W)} \text{rk}(f - g)$$
(where the rank of an endomorphism is the dimension of its image).

It is clear that any result on the metric $d_{rk}$ defined on $M_n(\mathbb{F})$ extends to $\text{End}(W)$ for any finite dimension vector space $W$ over $\mathbb{F}$.

**Proposition 2.8.** The function $d_{rk}$ is a metric on $M_n(\mathbb{F})$.

**Proof.** Symmetry and positivity are obvious. Let us prove the triangle inequality: for $A, B, C \in M_n(\mathbb{F})$, we want to show

$$d_{rk}(A, C) \leq d_{rk}(A, B) + d_{rk}(B, C).$$

This is equivalent to

$$\text{rk}(A - C) \leq \text{rk}(A - B) + \text{rk}(B - C).$$

Now, for any vector subspaces $W_1, W_2$ of $\mathbb{F}^n$ we have $\dim(W_1 + W_2) \leq \dim(W_1) + \dim(W_2)$. Therefore:

$$\dim \text{im}(A - B) + \dim \text{im}(B - C) \geq \dim(\text{im}(A - B) + \text{im}(B - C)),$$

and the space $\text{im}(A - B) + \text{im}(B - C)$ contains $\text{im}(A - C)$, since $(A - C)v$ equals $(A - B)v + (B - C)v$ for each $v \in \mathbb{F}^n$. \qed

**Remark 2.9.** Note that $d_{rk}$ is left- and right-invariant under multiplication by invertible matrices, and that if $d_{rk}(A, B) < \varepsilon$ then $d_{rk}(CA, CB) \leq \varepsilon$ for any $C \in M_n(\mathbb{F})$. For the latter statement, observe that $\text{rk}(CA - CB) = \text{rk}(C(A - B)) \leq \text{rk}(A - B)$.

### 2.6. Uniform word problem for finite groups.

The uniform word problem for finite groups (UWPG) is the following decision problem.

**Instance:** A finite presentation $\langle S \mid R \rangle$ of a group and an element $w \in S$.

**Task:** Decide whether there exists a finite group $G$ and a homomorphism $\varphi : G_{S,R} \to G$ such that $w \notin \ker(\varphi)$.

Our undecidability result relies on the following consequence of Slobodskoi’s work [Slo81].

**Theorem 2.10.** The uniform word problem for finite groups is undecidable.

Slobodskoi’s result is stronger: it shows that in fact the word problem for finite groups is undecidable for some specific $\langle S \mid R \rangle$ (in the notation above, it is only the word $w$ that is not fixed).

### 2.7. Sofic groups.

For an introduction to sofic groups see the survey by Pestov [Pes08].

The following is one of several equivalent definitions of sofic groups (see for instance [ES06]). To see the equivalence to the characterization in [Pes08, Theorem 3.5], one uses the amplification trick described in the proof of the same theorem.

**Definition 2.11.** A group $G$ is sofic if for every finite $F \subseteq G$ and for each $\varepsilon > 0$ there exist an $n \in \mathbb{N}$ and a mapping $\theta : F \to S_n$ such that

- (a) If $g, h, gh \in F$ then $d_{\text{hamm}}(\theta(g)\theta(h), \theta(gh)) < \varepsilon$,
- (b) If the neutral element $e \in F$ then $d_{\text{hamm}}(\theta(e), \text{id}) < \varepsilon$, and
- (c) For all distinct $x, y \in F$, $d_{\text{hamm}}(\theta(x), \theta(y)) \geq 1 - \varepsilon$.

Our proof that the existence of almost multilinear matroid representations is undecidable rests on the following theorem. It follows from the standard result that a solvable group is sofic together with the theorem of Kharlampovich [Kha81] that there exists a finitely presented solvable group with undecidable word problem.

**Theorem 2.12.** There exists a finitely presented sofic group with an algorithmically undecidable word problem.
2.8. **Algebraic lemmas.** We collect some results and prove a few lemmas for later use. All of them are either elementary or well known, but we include proofs for all but Mal’cev’s theorem, which can be found (for example) in [LS77].

Recall that a group $G$ is residually finite if for any $x \in G$ such that $x \neq e_G$ there exists a finite group $H$ and a homomorphism $\varphi : G \to H$ such that $\varphi(x) \neq e_H$.

**Theorem 2.13** (Malcev’s theorem). Let $\mathbb{F}$ be a field. A finitely generated subgroup of $\text{GL}_n(\mathbb{F})$ is residually finite.

**Lemma 2.14.** Let $\mathbb{F}$ be a field, $G$ a finitely generated group, $g \in G$ an element, and let $\rho : G \to \text{GL}_n(\mathbb{F})$ be a representation such that $\rho(g) \neq I_n$. Then there exists $n' \in \mathbb{N}$ and a representation $\rho' : G \to \text{GL}_{n'}(\mathbb{F})$ such that for every $x \in G$ the matrix $\rho'(x)$ is either $I_{n'}$ or the permutation matrix of a derangement, and $\rho'(g) \neq I_{n'}$.

**Proof.** The image $\rho(G)$ is a finitely generated subgroup of $\text{GL}_n(\mathbb{F})$, so it is residually finite by Mal’cev’s theorem. Let $H$ be a finite group and let $\varphi : \rho(G) \to H$ be a homomorphism such that $\varphi(\rho(g)) \neq e_H$. The left-action of $H$ on itself defines a permutation representation of $H$, and thus of $\rho(G)$ and of $G$, on a set of $n' = |H|$ elements, such that any element that acts nontrivially acts by a derangement. Choosing a bijection between $H$ and the set $\{1, \ldots, n'\}$ we produce a homomorphism $G \to S_{n'}$ which maps each $x \in G$ to the identity or to a derangement (and $g$ to a derangement). There is a homomorphism $S_{n'} \to \text{GL}_{n'}(\mathbb{F})$ which maps each permutation to its permutation matrix. Taking $\rho'$ to be the composition of these homomorphisms $G \to S_{n'} \to \text{GL}_{n'}(\mathbb{F})$ we obtain the result. □

**Lemma 2.15.** Let $\mathbb{F}$ be an algebraically closed field of characteristic either 0 or larger than $n$ and let $A \in \text{GL}_n(\mathbb{F})$ be the permutation matrix of a derangement. Then $A$ is conjugate to a diagonal block matrix in which every $k \times k$ nonzero block is a diagonal matrix of the form

$$
\begin{bmatrix}
\omega^0 & & \\
\omega^1 & & \\
& \ddots & \\
& & \omega^{k-1}
\end{bmatrix} \in \text{GL}_k(\mathbb{F})
$$

for $\omega$ a $k$-th root of unity.

**Proof.** Suppose $A$ is the permutation matrix of a derangement $\sigma \in S_n$. Let the cycle decomposition of $\sigma$ be

$$(i_1i_2\ldots i_{k_1})(i_{k_1+1}i_{k_1+2}\ldots i_{k_2})\ldots(i_{k_{r-1}+1}i_{k_{r-1}+2}\ldots i_n)$$

Then if $P$ is the permutation matrix of the permutation that takes $j$ to $i_j$ for all $1 \leq j \leq n$, it is clear that $PAP^{-1}$ is a diagonal block matrix which blocks of size $k_1, k_2-k_1, k_3-k_2, \ldots, k_r-k_{r-1}$, in which each nonzero $k \times k$ block is the permutation matrix of a cyclic permutation, i.e. is of the form

$$
B = \begin{bmatrix}
0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & \ddots & 0 & 0 \\
0 & 0 & 0 & 1 & 0
\end{bmatrix} \in \text{GL}_k(\mathbb{F}).
$$

Such a matrix defines a representation of $\mathbb{Z}/k\mathbb{Z}$ (in which the generator $1 \in \mathbb{Z}/k\mathbb{Z}$ maps to $B$). Its character vanishes on every $x \in \mathbb{Z}/k\mathbb{Z}$ except the identity, on which it achieves the value $k$. Since this is precisely the sum of the irreducible characters of $\mathbb{Z}/k\mathbb{Z}$ the result follows.
More concretely, if $\omega$ is a primitive $k$-th root of unity in $\mathbb{F}$ then for the Vandermonde matrix $Q = (\omega^{-(i-1)(j-1)})_{1 \leq i,j \leq k}$ we have

$$QBQ^{-1} = \begin{bmatrix} \omega^0 & \omega^1 & \cdots & \omega^{k-1} \\ \omega^1 & \omega^0 & \cdots & \omega^{k-2} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{k-1} & \omega^{k-2} & \cdots & \omega^0 \end{bmatrix}. \quad \square$$

We need a basic property of transcendental field extensions.

**Lemma 2.16.** Let $\mathbb{F}$ be a field. Let $p \in \mathbb{F}[x_1, \ldots, x_n]$ and let $L = \mathbb{F}(z_1, \ldots, z_n)$. If $p \neq 0$ then $p(z_1, \ldots, z_n) \neq 0$.

*Proof.* By induction on $n$. For $n = 1$: It suffices to prove the claim in the larger field $L' = \overline{\mathbb{F}}(z_1)$ (where $\overline{\mathbb{F}}$ denotes the algebraic closure). If $p \neq 0$ then $p$ has $\deg p$ roots in $\overline{\mathbb{F}}$, and these are all its roots in $L' \supseteq \overline{\mathbb{F}}$, because a nonzero polynomial has at most as many roots as its degree. Since $z_1 \in L' \setminus \overline{\mathbb{F}}$, it is not a root of $p$.

If the claim is established for some $n$ and $p \in \mathbb{F}[x_1, \ldots, x_{n+1}]$ is nonzero, gather together like powers of $x_{n+1}$ and write

$$p = \sum_{i=0}^{r} q_i x_{n+1}^i$$

for polynomials $q_0, \ldots, q_r \in \mathbb{F}[x_1, \ldots, x_n]$. Then $q_j \neq 0$ for some $0 \leq j \leq r$ (else $p = 0$).

Denote $\mathbb{F}' = \mathbb{F}(z_1, \ldots, z_n)$. Then $\tilde{p}(x_{n+1}) = p(z_1, \ldots, z_n, x_{n+1}) \in \mathbb{F}'[x_{n+1}]$ satisfies

$$\tilde{p}(x_{n+1}) = \sum_{i=0}^{r} q_i (z_1, \ldots, z_n) x_{n+1}^i \neq 0$$

because (by induction) the coefficient of $x_{n+1}^j$ is nonzero. It follows from the base case (over the field $\mathbb{F}'$) that for $L = \mathbb{F}'(z_{n+1}) = \mathbb{F}'(z_1, \ldots, z_{n+1})$ we have $\tilde{p}(z_{n+1}) = p(z_1, \ldots, z_{n+1}) \neq 0$. \quad \square

We apply this lemma in the following form:

**Corollary 2.17.** Let $\mathbb{F}$ be a field and let $L = \mathbb{F}(z_{k,i,j})_{1 \leq k \leq r, 1 \leq i,j \leq n}$. For each $1 \leq k \leq r$ denote by $A_k \in M_n(\mathbb{L})$ the matrix given by

$$A_k = (z_{k,i,j})_{1 \leq i,j \leq n}.$$  

Let $w$ an element of the free algebra over $\mathbb{F}$ with generators $b_1, \ldots, b_r, b_1^{-1}, \ldots, b_r^{-1}$ and $c_1, \ldots, c_s, c_1^{-1}, \ldots, c_s^{-1}$ (note that formally $b_i$ and $b_i^{-1}$ as well as $c_i$ and $c_i^{-1}$ are unrelated generators, and not inverses in this algebra). For invertible matrices $B_1, \ldots, B_r, C_1, \ldots, C_s \in M_n(\mathbb{L})$, denote by $w(B_1, \ldots, B_r, C_1, \ldots, C_s) \in M_n(\mathbb{L})$ the matrix obtained by substituting $B_1$ and $B_1^{-1}$ for $b_1$ and $b_1^{-1}$ and $C_1$ and $C_1^{-1}$ for $c_1$ and $c_1^{-1}$ in the expression $w$.

If there exist invertible matrices $B_1, \ldots, B_r, C_1, \ldots, C_s \in M_n(\mathbb{L})$ such that the matrix $w(B_1, \ldots, B_r, C_1, \ldots, C_s)$ is invertible then $w(A_1, \ldots, A_r, C_1, \ldots, C_s)$ is invertible too.

*Proof.* Using Cramer’s formula, consider $p = \det (w(A_1, \ldots, A_r, C_1, \ldots, C_s))$ as a rational function over $\mathbb{F}$ in variables the entries $\{z_{k,i,j}\}_{1 \leq k \leq r, 1 \leq i,j \leq n}$ of $A_1, \ldots, A_r$. Represent it as a reduced fraction of polynomials $\frac{f}{g}$ in the variables. Then

$$\det (w(B_1, \ldots, B_r, C_1, \ldots, C_s))$$

is the value of this rational function when the entries of $B_1, \ldots, B_r$ are substituted for the variables. In particular, $f$ and $g$ are nonzero (because they give nonzero values with this substitution). Thus also $p \neq 0$ by an application of Lemma 2.16 to $f$ and to $g$. \quad \square
Corollary 2.18. Let $\mathbb{F}$ be a field, let $L = \mathbb{F}(z)$, and let $A, B \in M_n(\mathbb{F})$ be invertible matrices. Then $\det(zA + B) \neq 0$.

Proof. It suffices to prove $zA + B = A(zI + A^{-1}B)$ is invertible. Denoting $C = A^{-1}B$, it therefore suffices to prove $zI + C$ is invertible. Consider $\det(zI + C)$ as a polynomial in $z$. If this polynomial is 0 then for every $\alpha \in \mathbb{F}$ we have $\det((-\alpha)I + C) = \det(C - \alpha I) = 0$, so $\alpha$ is an eigenvalue of $C$. But $C$ cannot have more than $n$ eigenvalues whereas $\mathbb{F}$ is infinite. □

3. Generalized Dowling Groupoids and Geometries

We find it useful to think of generalized Dowling geometries (see the overview in Section 1) as matroidal encodings of certain groupoids, which we call Dowling groupoids. In this section we introduce the Dowling groupoid of a finitely presented group, explain how representations of these groupoids are related to representations of the associated groups, and define the generalized Dowling geometries.

To define the generalized Dowling groupoids and geometries we use group presentations of a specific form. The relators in our presentations are not necessarily reduced.

Definition 3.1. We call a group presentation $\langle S \mid R \rangle$ symmetric triangular if it satisfies the following conditions.

(a) $S$ and $R$ are finite and the neutral element $e$ is a generator in $S$.
(b) The generators $S$ are symmetric. That is, for $e \neq s \in S$ also $s^{-1} \in S$. Further, $ss^{-1}e$ is a relator in $R$.
(c) All relators in $R$ are of length three.
(d) The relators in $R$ are cyclically symmetric. That is, if $abc \in R$ is a relator for $a, b, c \in S$ then also $bca$ and $cab$ are relators in $R$.
(e) If $abc \in R$ is a relator then also $c^{-1}b^{-1}a^{-1}$ is a relator.
(f) $eee$ is a relator.

While algebraically some of these requirements are artificial, they make the combinatorics that follows more convenient.

Any finitely presented group has a symmetric triangular presentation. To obtain one from a given presentation $\langle S \mid R \rangle$, first add the neutral element $e$ to $S$ if necessary. Then symmetrize the generators (by adding a formal inverse $s^{-1}$ for each $s \in S \setminus \{e\}$ which does not already have one, together with the relation $s^{-1}se = e$). Then “break up” long relators into short ones as follows: given a relator $s_1s_2\ldots s_n$ in $R$, add generators $x_2, x_3$, and so on up to $x_{n-2}$, and symmetrize the generating set (to add inverses for the new generators). Then add the relations

\[ s_1s_2x_1^{-1} = e, \]
\[ x_1s_3x_2^{-1} = e, \]
\[ \vdots \]
\[ x_{n-2}s_{n-1}s_n = e, \]

and delete $s_1s_2\ldots s_n$ from $R$. Finally, symmetrize the set of relations by adding the cyclic shifts and their inverses for every relator, and add the relator $eee$.

Definition 3.2. Let $G$ be a group given by a symmetric triangular presentation $\langle S \mid R \rangle$. The Dowling groupoid associated to $\langle S \mid R \rangle$ is the finitely presented groupoid $G$ with the following presentation:

(a) The objects are $\{b_1, b_2, b_3\}$,
(b) Generators for the morphisms are given by
\[ \{ g_{s,ij} : b_i \to b_j \mid s \in S, \text{ and } i, j \in \{1, 2, 3\} \text{ with } i \neq j \}. \]

(c) For each \( s \in S \) and each pair of distinct indices \( i, j \in \{1, 2, 3\} \) we impose the relation \( g_{s,ij} \circ g_{s,ij} = id_{b_i} \). For each cyclic shift \((i, j, k)\) of \((1, 2, 3)\) and for each relation \(s's's = e\) in \(R\), we impose the relation
\[ g_{s''k,ij} \circ g_{s',jk} \circ g_{s,ij} = id_{b_i}. \]

**Remark 3.3.** It is useful to note that since \( \langle S \mid R \rangle \) is symmetric triangular, the following relations hold in \(G\):

(a) For each permutation \((i, j, k)\) of \((1, 2, 3)\) and for each \( s \in S \), the relation
\[ g_{e,ijk} \circ g_{s,ijk} = g_{s,ijk} \circ g_{e,ijk}. \]

(b) For each permutation \((i, j, k)\) of \((1, 2, 3)\), the relation \( g_{e,ijk} \circ g_{e,ijk} \circ g_{e,ijk} = id_{b_i} \).

Each relation of type (a) can be deduced from the relation
\[ g_{s^{-1},ijk} \circ g_{e,ijk} \circ g_{s,ijk} = id_{b_i} \]
which can themselves be deduced from the defining relations of \(G\) and the fact that \( s^{-1}es = e \) is a relation of \(\langle S \mid R \rangle\), because the presentation is symmetric triangular.

Similarly, the six relations of type (b) follow from the fact that \( eee = e \) is a relation in \(R\) (and from the defining relations of \(G\)). Note that for \((i, j, k)\) an odd permutation of \((1, 2, 3)\) (which is not a cyclic shift) the relation \( g_{e,ijk} \circ g_{e,ijk} \circ g_{e,ijk} = id_{b_i} \) is the inverse of \( g_{e,ijk} \circ g_{e,ijk} \circ g_{e,ijk} = id_{b_i} \), where \((i, j, k)\) is a cyclic shift of \((1, 2, 3)\).

### 3.1. Representations of \(G\) and of \(G\).

Let \(G\) be a finitely presented group as in the definition above. The Dowling groupoid \(G\) does not interest us in itself; it is a sort of intermediate object between \(G\) and the matroids constructed further below. The point is that from a representation of \(G\) (i.e. a functor \(F : G \to C\) into some category) one can obtain a representation of \(G\) in \(C\) and vice versa. Here \(G\) is considered as a groupoid with one object \(*.\) This is shown in several lemmas below. The proofs are rather obvious and readers may wish to skip them (the raison d’être for this section is the verification that the relations defining \(G\) have been chosen correctly).

**Lemma 3.4.** For each representation \(F : G \to C\) of \(G\) in a category \(C\) there is an isomorphic representation \(F' : G \to C\) which satisfies:

(a) \(F'(b_1) = F'(b_2) = F'(b_3),\)
(b) \(F'(g_{e,ijk}) = id_{F'(b_i)}\) for all \(i, j,\)
(c) \(F'(g_{s,12}) = F'(g_{s,23}) = F'(g_{s,31})\) for each \(s \in S,\) and
(d) \(F'(g_{s,12}) = F'(g_{s,23}) = F'(g_{s,31}) = F'(g_{s,12})^{-1}.\)

That \(F'\) is an isomorphic representation of \(G\) means that there is a natural isomorphism \(F \to F'\).

**Proof.** Define \(F'\) on objects by setting \(F'(b_i) := F(b_i)\) for all \(1 \leq i \leq 3\). Further define it on the generating morphisms \(f : b_i \to b_j\) as follows:

\[ F'(f) := \begin{cases} F(g_{e,1} \circ f \circ g_{e,1,i}) & \text{if } i \neq 1 \text{ and } j \neq 1, \\ F(g_{e,1} \circ f) & \text{if } i = 1, \\ F(f \circ g_{e,1,i}) & \text{if } j = 1. \end{cases} \]

For each object \(b_i\) of \(G\) we define an isomorphism \(\eta_{b_i} : F(b_i) \to F'(b_i)\) by setting \(\eta_1 := id_{F(b_1)}\) and \(\eta_i = F(g_{e,1,i})\) for \(i = 2, 3\). By definition of \(F'\) this yields for each
generating morphism \( f : b_i \to b_j \) of \( \mathcal{G} \) the commutative diagram:

\[
\begin{array}{c}
F(b_i) \\ \downarrow F(f) \\
F(b_j) \\
\end{array}
\quad \xrightarrow{\eta_{b_i}} \quad
\begin{array}{c}
F'(b_i) \\ \downarrow F'(f) \\
F'(b_j) \\
\end{array}
\]

For general morphisms of \( \mathcal{G} \) the same diagrams commute, because they can be written as compositions of generating morphisms. Thus \( F' \) is a functor, i.e. it respects composition: if \( f_2 \circ f_1 = f_3 \) in \( \mathcal{G} \) for some \( f_1 : b_i \to b_j, f_2 : b_j \to b_k, \) and \( f_3 : b_1 \to b_k \) then the diagram

\[
\begin{array}{c}
F(b_i) \\ \downarrow F(f_1) \\
F(b_j) \\ \downarrow F(f_2) \\
F(b_k) \\
\end{array}
\quad \xrightarrow{\eta_{b_i}} \quad
\begin{array}{c}
F'(b_i) \\ \downarrow F'(f_1) \\
F'(b_j) \\ \downarrow F'(f_2) \\
F'(b_k) \\
\end{array}
\]

commutes, implying that

\[
F'(f_2) \circ F'(f_1) = \eta_{b_k} \circ F(f_2) \circ (F(f_1))
\]

and thus that \( F'(f_2) \circ F'(f_1) = \eta_{b_k} \circ F(f_2) \circ (F(f_1)) = \eta_{b_k} \circ F(f_3) \circ \eta_{b_i}^{-1} \). But by definition we have \( F'(f_3) = \eta_{b_k} \circ F(f_3) \circ \eta_{b_i}^{-1} \), which shows

\[
F'(f_3) = F'(f_2 \circ f_1)
\]

as desired. By definition the maps \( \{ \eta_{b_i} \}_{b_i \in \mathrm{ob}(\mathcal{G})} \) define a natural isomorphism \( F \to F' \).

We now prove each of the claimed properties of \( F' \) in turn:

Property (a) is satisfied by definition, and property (b) follows from the following computations, in which we use the relations of \( \mathcal{G} \):

\[
F'(g_{e,1,2}) = F(g_{e,2,1} \circ g_{e,1,2}) = F(id_{b_1}) = id_{F'(b_1)}
\]

\[
F'(g_{e,2,3}) = F(g_{e,3,1} \circ g_{e,2,3} \circ g_{e,1,2}) = F(id_{b_1}) = id_{F'(b_1)}
\]

\[
F'(g_{e,3,1}) = F(g_{e,3,1} \circ g_{e,1,3}) = F(id_{b_1}) = id_{F'(b_1)}.
\]

We now prove property (c). To this end observe that \( F'(g_{s,1,2}) = F(g_{e,2,1} \circ g_{s,1,2}) \) and furthermore \( F'(g_{s,2,3}) = F(g_{e,3,1} \circ g_{s,2,3} \circ g_{e,1,2}) \). The relations of \( \mathcal{G} \) imply that

\[
F'(g_{s,1,2}) = F(g_{e,2,1} \circ g_{s,1,2}) \overset{1}{=} F(g_{e,3,1} \circ g_{e,2,3} \circ g_{s,1,2}) \overset{2}{=} F(g_{e,3,1} \circ g_{s,2,3} \circ g_{e,1,2}) = F'(g_{s,2,3}).
\]

where (1) is obtained by precomposing the identity \( g_{e,2,1} \circ g_{e,1,2} = id_{b_1} = g_{e,3,1} \circ g_{e,2,3} \circ g_{e,1,2} \) with \( g_{e,1,2} \) and (2) follows from the relation \( g_{e,2,3} \circ g_{s,1,2} = g_{s,2,3} \circ g_{e,1,2} \). The identity \( F'(g_{s,2,3}) = F'(g_{s,3,1}) \) follows similarly: we have

\[
F'(g_{s,3,1}) = F(g_{s,3,1} \circ g_{e,1,3}) = F(g_{s,3,1} \circ g_{e,2,3} \circ g_{e,1,2}) = F(g_{s,2,3}).
\]

For property (d), using the fact that \( g_{s,2,1} = g_{s,1,2}^{-1} \) in \( \mathcal{G} \) we see that \( F'(g_{s,2,1}) = F'(g_{s,1,2})^{-1} \). Similarly we have \( g_{s,3,2} = g_{s,2,3}^{-1} \) and \( g_{s,1,3} = g_{s,3,1}^{-1} \). It follows that

\[
F'(g_{s,2,1}) = F'(g_{s,3,2}) = F'(g_{s,1,3}).
\]

**Lemma 3.5.** Consider \( G \) as a groupoid with one object \(*\) and morphisms the elements of the group \( G \). Let \( F : \mathcal{G} \to C \) be a representation satisfying properties (a)-(d) of Lemma 3.4.
Then there is a functor

\[ F' : G \rightarrow C \]

defined by \( F'(*) = F(b_1) \) and on the generating morphisms by \( F'(s) = F(g_{s,1,2}) \).

**Proof.** We only have to verify that \( F'(s''s') \circ F'(s') \circ F'(s) = \text{id}_{F'(s)} \) for any relation \( s''s' = e \) in \( R \). We compute

\[
\begin{align*}
F'(s''s') \circ F'(s') \circ F'(s) &= F(g_{s'',1,2}) \circ F(g_{s',1,2}) \circ F(g_{s,1,2}) \\
&= F(g_{s'',3,1}) \circ F(g_{s',2,3}) \circ F(g_{s,1,2}) = F(g_{s'',3,1} \circ g_{s',2,3} \circ g_{s,1,2}) = F(\text{id}_{b_1}) \\
&= \text{id}_{F(b_1)} = \text{id}_{F'(s)}.
\end{align*}
\]

□

**Lemma 3.6.** Consider \( G \) as a groupoid with one object \(*\). Let \( F : G \rightarrow C \) be a representation of \( G \). Then there is a functor

\[ F' : \mathcal{G} \rightarrow C \]

defined on objects by \( F'(b_i) = F(*) \) and on the generating morphisms by:

\[
\begin{align*}
F'(g_{s,1,2}) &= F'(g_{s,2,3}) = F'(g_{s,3,1}) = F(s) \quad \text{and} \\
F'(g_{s,2,1}) &= F'(g_{s,3,2}) = F'(g_{s,1,3}) = F(s)^{-1}
\end{align*}
\]

for each \( s \in S \). This functor satisfies properties (a)-(d) of Lemma 3.4.

**Proof.** Once we prove \( F' \) is a functor, properties (a)-(d) follow directly from the definition. Thus we only need to check that each relation between morphisms in \( G \) is respected by \( F' \).

Observe that if \( s \in S \) and \( i, j \in \{1, 2, 3\} \) are distinct then \( F'(g_{s,j,i}) \circ F'(g_{s,i,j}) \) equals either \( F(s) \circ F(s)^{-1} \) or \( F(s)^{-1} \circ F(s) \), depending on whether the pair \((i, j)\) is one of \( \{(1, 2), (2, 3), (3, 1)\} \), and in either case the composition maps to the identity. Since \( F'(g_{s,j,i}) = F(e) = \text{id}_{F(s)} \), it is clear that

\[
F'(g_{e,k,i}) \circ F'(g_{e,j,k}) \circ F'(g_{e,i,j}) = \text{id}_{F(b_i)}
\]

whenever \( i, j, k \) are distinct indices. Similarly,

\[
F'(g_{s,j,k}) \circ F'(g_{e,i,j}) = F'(s)^{\text{sgn}(j,k)} = F'(s)^{\text{sgn}(i,j,k)} = F'(g_{e,j,k}) \circ F'(g_{s,i,j}).
\]

If \( s''s' = e \) is a relation in \( R \) and \((i, j, k)\) is a cyclic shift of \( (1, 2, 3) \) then we have \( F'(g_{s,i,j}) = F(s) \), \( F'(g_{e,j,k}) = F(s') \), and \( F'(g_{s'',k,i}) = F(s'') \), so that

\[
\begin{align*}
F'(g_{s'',k,i}) \circ F'(g_{s',j,k}) \circ F'(g_{s,i,j}) &= F(s'') \circ F(s') \circ F(s) \\
&= F(s''s'') \circ F(e) = \text{id}_{F(b_i)}.
\end{align*}
\]

□

### 3.2. Generalized Dowling geometries

We define a class of matroids closely related to the Dowling geometries. The relation to the Dowling groupoids defined above should be clear.

**Definition 3.7.** Let \( G = \langle S \mid R \rangle \) be a group together with a symmetric triangular presentation. The **generalized Dowling geometry** associated to the presentation \( \langle S \mid R \rangle \) is the rank 3 matroid \( M \) on the ground set

\[ E := \{b_1, b_2, b_3\} \cup \{s_i \mid s \in S, 1 \leq i \leq 3\} \]

(i.e., three elements \( b_1, b_2, b_3 \) and three indexed copies of each element \( s \in S \)) and with the following flats of rank 2 (which are called lines, in analogy with affine geometry):

- For each \( s \in S \), we place the element \( s_1 \) on the line spanned by \( \{b_1, b_2\} \), and similarly \( s_2 \) and \( s_3 \) are on the lines spanned by \( \{b_2, b_3\} \) and \( \{b_3, b_1\} \) respectively. This means that each of the sets

\[
\{b_1, b_2\} \cup \{s_1\}_{s \in S}, \quad \{b_2, b_3\} \cup \{s_2\}_{s \in S}, \quad \{b_3, b_1\} \cup \{s_3\}_{s \in S}
\]

is a flat.
• For each relation $s^n s' s = e$ in $R$ and any cyclic shift $(i, j, k)$ of the indices $(1, 2, 3)$, we take $\{s_i, s'_j, s_k^n\}$ to be a flat. We assume that the trivial relations $s s^{-1} e = e$ and $e e e = e$ are in $R$, so that $\{e_1, e_2, e_3\}$ and (for example) $\{s_1, e, s_3^{-1}\}$ are flats for each $s \in S$.

**Proposition 3.8.** This is a matroid with basis $B = \{b_1, b_2, b_3\}$.

*Proof.* Any two of the rank-2 flats defined above intersect in at most one element, and $B$ is not contained in any of these flats. The result thus follows from [Ox11, Prop. 1.5.6]. □

**Definition 3.9.** Let $G = \langle S \mid R \rangle$ be a group with a symmetric triangular presentation. We define a set $\mathcal{M}_{S, R}$ of generalized Dowling geometries, which we call the set of generalized Dowling geometries subordinate to $\langle S \mid R \rangle$.

Denote by $T$ the set of all words $s^n s' s$, where $s, s', s^n \in S$ are three generators (not necessarily distinct). For each $X \subseteq T$ symmetrize the relations of $\langle S \mid R \cup X \rangle$ and denote by $M_X$ the generalized Dowling geometry associated to the resulting group presentation. Then

$$
\mathcal{M}_{S, R} = \{M_X \mid X \subseteq T\}.
$$

**Remark 3.10.** Each generalized Dowling geometry in $\mathcal{M}_{S, R}$ is the geometry associated to $\langle S \mid R \cup X \rangle$ for some $X$, and there is a quotient map $\langle S \mid R \rangle \to \langle S \mid R \cup X \rangle$ which is the identity on the generators.

The family $\mathcal{M}_{S, R}$ can also be described as a collection of certain weak images of the generalized Dowling geometry associated to $\langle S \mid R \rangle$, but we will not use this.

4. **Probability space representations of matroids**

An entropic representation of a matroid is given by a collection of random variables on a discrete probability space. We introduce some new language to handle these more conveniently: we avoid working directly with the entropy function, but rather with the independence and determination properties of the variables. We package everything we need into the definition of a “probability space representation” and the accompanying notation. The discussion is essentially equivalent to the probabilistic representations introduced by Matůš in [Mat93].

**Definition 4.1.** Let $\langle \Omega, \mathcal{F}, P \rangle$ be a probability space and let $\{X_e\}_{e \in E}$ be a finite collection of random variables on $\langle \Omega, \mathcal{F}, P \rangle$, that is measurable functions $X_e : \Omega \to \Omega$.

(a) The variables $\{X_e\}_{e \in E}$ are independent if for any $(A_e)_{e \in E} \in \prod_{e \in E} \mathcal{F}_e$,

$$
P\left(\bigcap_{e \in E} X_e^{-1}(A_e)\right) = \prod_{e \in E} P\left(X_e^{-1}(A_e)\right).
$$

(This is the same notion as independence of random variables.)

(b) Fix $c \in C \subseteq E$. The function $X_c$ is determined by $\{X_e\}_{e \in C \setminus \{c\}}$ if there exists a measurable function

$$
f : \prod_{e \in C \setminus \{c\}} \Omega_e \to \Omega_c
$$

such that $f \circ (X_e)_{e \in C \setminus \{c\}} = X_c$. Such a function $f$ is called a determination function for $X_c$ given $\{X_e\}_{e \in C \setminus \{c\}}$, or just a determination function for short.

**Definition 4.2.** Let $M$ be a matroid on a finite set $E$. A probability space representation of $M$ consists of a discrete probability space $\langle \Omega, \mathcal{F}, P \rangle$ and an indexed collection of random variables $\{X_e\}_{e \in E}$ on $\Omega$ such that the following conditions hold:

(a) (Independence.) If $A \subseteq E$ is independent, the functions $\{X_e\}_{e \in A}$ are independent.
(b) (Determination.) If \( C \subseteq E \) is a circuit and \( e \in C \), then \( X_e \) is determined by \( \{X_f\}_{f\in C \setminus \{e\}} \).

c) (Non-triviality.) If \( e \in E \) is not a loop, there are disjoint measurable \( S, T \subseteq \Omega_e \) such that \( X_e^{-1}(S) \) and \( X_e^{-1}(T) \) have nonzero probability.

**Remark 4.3.** The non-triviality condition implies, for instance, that \( \Omega_e \) is not a singleton. Together with the independence condition, it also ensures that if \( e \in A \subseteq E \) where \( A \) is independent then \( X_e \) is not determined by \( \{X_f\}_{f\in A \setminus \{e\}} \).

Note that since the probability space is discrete, it is harmless to assume that all singletons have positive probability. With this additional assumption we have that \( X_A \) is surjective for each independent \( A \subseteq E \).

Whenever we work with just one matroid on a ground set \( E \) and one probability space representation in \( (\Omega, \mathcal{F}, P) \), we will denote the measurable spaces and functions associated to each element \( e \in E \) by \( (\Omega_e, \mathcal{F}_e) \) and \( X_e : \Omega \to \Omega_e \) respectively, without further explicit mention of the notation.

**Theorem 4.4.** Let \( M \) be a connected matroid of rank at least two. Then \( M \) is entropic if and only if it has a probability space representation in a discrete probability space in which each singleton has nonzero probability. In this case, each of the random variables \( \{X_e\}_{e \in E} \) are uniformly distributed and the underlying probability space can be chosen to be finite.

The first part of the theorem relies on standard facts concerning entropy functions and the second part of the theorem is a trivial generalization of a result by Matúš in [Mat93, p.190-191]. We defer the proof to Appendix A.

### 4.1. Entropic representations of generalized Dowling Geometries

The main theorem of this section is concerned with entropic representations of generalized Dowling geometries.

**Theorem 4.5.** Let \( G \) be a group with a symmetric triangular presentation \( (S \mid R) \) and let \( M \) be the associated generalized Dowling geometry. If \( M \) is entropic then there exists \( n \in \mathbb{N} \) such that there exists a group homomorphism \( \rho : G \to S_n \) with \( \rho(s) \neq \rho(s') \) for distinct \( s, s' \in S \).

This is deduced from the following more technical result.

**Theorem 4.6.** Let \( (S \mid R) \) be a group with a symmetric triangular presentation. Let \( M = (E, C) \) be the associated generalized Dowling geometry, and let \( G \) be the corresponding groupoid. Suppose \( M \) has a probability space representation in a discrete probability space \( (\Omega, \mathcal{F}, P) \), with each \( e \in E \) assigned the measurable space \( (\Omega_e, \mathcal{F}_e) \) and the measurable function \( X_e : \Omega \to \Omega_e \). For \( s \in S \) and each circuit \( C \in C \) of the form \( \{b_i, b_j, s_i\} \) (with \( i, j \) distinct) let

\[
f_{s,i,j} : \Omega_{b_i} \times \Omega_s \to \Omega_{b_j} \quad \text{and} \quad f_{s,j,i} : \Omega_{b_j} \times \Omega_s \to \Omega_{b_i}
\]

be the two corresponding determination functions of the circuit.

Further define

\[
\varphi_{s,i,j} : \Omega_{b_i} \times \Omega \to \Omega_{b_j} \times \Omega = (f_{s,i,j} (\omega_i, X_{s_i}(\omega)), \omega)
\]

and similarly

\[
\varphi_{s,j,i} : \Omega_{b_j} \times \Omega \to \Omega_{b_i} \times \Omega = (f_{s,j,i} (\omega_j, X_{s_i}(\omega)), \omega).
\]
Then there is a functor $F : \mathcal{G} \to \text{FinSet}$ defined on objects by $F(b_i) = \Omega_{b_i} \times \Omega$ and on the
generators of the morphisms by $F(g_{s,i,j}) = \varphi_{s,i,j}$. This functor is faithful (that is, it maps
distinct generating morphisms to distinct morphisms.) More explicitly:

(a) The functions $\varphi_{s,i,j}$ and $\varphi_{s',i,j}$ are mutually inverse.
(b) If $(i, j, k)$ is an even permutation of $(1, 2, 3)$ and $s' s' s = e$ is a relation in $R$ then
$$
\varphi_{s'',i,k} \circ \varphi_{s',j,k} \circ \varphi_{s,i,j} = \text{id}_{\Omega_{b_i} \times \Omega}.
$$

(c) If $s, s' \in S$ are distinct elements and $i, j \in \{1, 2, 3\}$ are distinct then $\varphi_{s,i,j} \neq \varphi_{s',i,j}.

Proof. We assume, as we may by Theorem 4.4, that $\Omega$ (together with all probability spaces $\Omega_{b}$ for $b \in E$) is finite. Thus if $F$ defines a functor its values are in $\text{FinSet}$ (rather than just $\text{Set}$.) To show $F$ is a functor it suffices to prove the three statements above.

(a) Let $(\omega_i, \omega) \in \Omega_{b_i} \times \Omega$, and assume without loss of generality that $i$ precedes $j$ in the cyclic ordering of the indices. Denote $\omega_s = X_{s_i}(\omega)$. Then there exists $\omega' \in \Omega$
such that $X_{b_i}(\omega') = \omega_i$ and $X_{s_i}(\omega') = \omega_s$, since $X_{\{b_i,s_i\}}$ is surjective. Denote
$\omega_j = X_j(\omega')$. Then
$$
f_{s,i,j}(\omega_i, \omega_s) = f_{s,i,j} \circ X_{\{b_i,s_i\}}(\omega') = X_{b_j}(\omega'),
$$
and similarly $f_{s,j,i}(\omega_i, \omega_s) = f_{s,j,i} \circ X_{\{b_j,s_i\}}(\omega') = X_{b_i}(\omega')$. It follows that
$$
\varphi_{s,i,j}(\omega_i, \omega) = (\omega_j, \omega) \quad \text{and} \quad \varphi_{s,j,i}(\omega_j, \omega) = (\omega_i, \omega).
$$

(b) Let $(\omega_i, \omega) \in \Omega_{b_i} \times \Omega$, and denote $\omega_s = X_{s_i}(\omega)$, $\omega_{s'} = X_{s'_j}(\omega)$. Since $\{b_i, s_i, s'_j\}$ is an independent set, there exists $\omega' \in \Omega$
such that $X_{b_i}(\omega') = \omega_i$, $X_{s_i}(\omega') = \omega_s$, and $X_{s'_j}(\omega') = \omega_{s'}$
Since $\{s_i, s'_j, s''_k\} \in \mathcal{C}$, the variable $X_{s''_k}$ is determined by the values of $X_{s_i}$ and $X_{s'_j}$,
and we have
$$
X_{s''_k}(\omega') = X_{s''_k}(\omega)
$$
because the same equalities hold for $X_{s_i}$ and $X_{s'_j}$. Using this, we compute:
$$
\varphi_{s,i,j}(\omega_i, \omega) = (f_{s,i,j}(\omega_i, \omega_s), \omega) = (X_{b_j}(\omega'), \omega)
$$
where the last equality holds because $X_{b_i}(\omega') = \omega_i$ and $X_{s_i}(\omega') = \omega_s$. In precisely
the same way,
$$
\varphi_{s',j,k}(X_{b_j}(\omega'), \omega) = (f_{s',j,k}(X_{b_j}(\omega'), \omega_{s'}), \omega) = (X_{b_k}(\omega'), \omega)
$$
and
$$
\varphi_{s'',k,i}(X_{b_k}(\omega'), \omega) = (f_{s'',k,i}(X_{b_k}(\omega'), X_{s''_k}(\omega')), \omega) = (\omega_i, \omega)
$$
so that $\varphi_{s'',k,i} \circ \varphi_{s',j,k} \circ \varphi_{s,i,j}(\omega_i, \omega) = (\omega_i, \omega)$ where $(\omega_i, \omega) \in \Omega_{b_i} \times \Omega$ is an arbitrary element.

(c) Assume without loss of generality that $i$ precedes $j$ in the cyclic ordering, and con-
cider the circuits $C'_1 = \{b_j, b_j, s_i\}$ and $C'_2 = \{b_i, b_j, s'_j\}$ in $M$. Since $\{s_i, s'_j\}$ is an
independent subset, there exist elements $\omega, \omega' \in \Omega$ such that $X_{s'_j}(\omega) = X_{s'_j}(\omega')$ but
$X_{s_i}(\omega) \neq X_{s_i}(\omega')$ (here we used the non-triviality condition of probability space
representations of matroids).

Fix $\omega_i \in \Omega_{b_i}$. Then by definition
$$
\varphi_{s',i,j}(\omega_i, \omega) = f_{s',i,j}(\omega_i, X_{s'_i}(\omega)) = f_{s',i,j}(\omega_i, X_{s'_i}(\omega')) = \varphi_{s',i,j}(\omega_i, \omega').
$$
Suppose for a contradiction that $\omega_i := \varphi_{s,i,j}(\omega_i, \omega) = \varphi_{s,i,j}(\omega_i, \omega')$ also. Since
$\{b_i, s_i\}$ are independent we can find $\bar{\omega}, \bar{\omega}' \in \Omega$ such that $(X_{b_i}, X_{s_i})(\bar{\omega}) = (\omega_i, X_{s_i}(\omega))$
and $(X_{b_i}, X_{s_i})(\bar{\omega}') = (\omega_i, X_{s_i}(\omega'))$. Using the fact that $X_{b_j}$ is determined by $X_{b_i}$,
and \( X_{s_i} \) we obtain the equalities
\[
(X_{b_i}, X_{s_i}, X_{b_j}) (\tilde{\omega}) = (\omega_i, X_{s_i} (\omega), \omega_j) \quad \text{and} \quad
(X_{b_i}, X_{s_i}, X_{b_j}) (\tilde{\omega}') = (\omega_i, X_{s_i} (\omega'), \omega_j).
\]
In particular \( (X_{s_i}, X_{b_j}) (\tilde{\omega}) = (\omega_i, \omega_j) = (X_{b_i}, X_{b_j}) (\tilde{\omega}') \). But \( X_{s_i} \) is determined by \( X_{b_i} \) and \( X_{b_j} \), so
\[
X_{s_i} (\omega) = X_{s_i} (\tilde{\omega}) = X_{s_i} (\tilde{\omega}') = X_{s_i} (\omega'),
\]
a contradiction. \( \Box \)

5. MULTILINEAR REPRESENTATIONS OF MATROIDS

Multilinear matroids are entropic [Mat99], so the results of Section 4.1 are valid for them as well: a multilinear representation of a generalized Dowling geometry gives rise, by the correspondences described above, to a representation of the associated groupoid. We prove a partial converse to this result, which states that under certain conditions a matrix representation of a group \( \langle S \mid R \rangle \) implies that the corresponding generalized Dowling geometry is multilinear. But first we digress and discuss multilinear matroid representations on their own terms: We introduce an equivalent definition of multilinear representability which is directly analogous to probability space representations. We feel this definition helps clarify what is going on.

5.1. Notation for vector spaces and linear maps. We introduce some notation in close analogy with the notation for probability spaces and random variables introduced in Section 2.1.

Let \( \mathbb{F} \) be a field. An indexed collection of linear maps on a vector space \( V \) over \( \mathbb{F} \) consists of an index set \( E \), a collection of vector spaces \( \{W_e\}_{e \in E} \), and a collection of linear maps \( \{T_e : V \to W_e\}_{e \in E} \). As in Section 2.1, we sometimes write “let \( \{T_e\}_{e \in E} \) be a collection of linear maps on \( V \), and refer to the codomain of each \( T_e \) by \( W_e \) (without naming \( W_e \) explicitly).

Given a tuple \( S = (s_1, \ldots, s_n) \) of elements of \( E \), we denote \( W_S = \bigoplus_{i=1}^n W_{s_i} \) and define a linear map \( T_S : V \to W_S \) by
\[
T_S(v) = (T_{s_i}(v))_{i=1}^n.
\]
If the order is inessential, the same notation can be used if \( S \) is a set.

5.2. Vector space representations. The following terminology is nonstandard, but useful because of the close analogy with random variables, probability spaces, and probability space representations of matroids. All vector spaces in this section are over a fixed field \( \mathbb{F} \) and assumed to be finite dimensional.

**Definition 5.1.** Let \( V \) be a vector space, let \( E \) be a finite set, and let \( \{T_e\}_{e \in E} \) be a collection of linear maps on \( V \).

(a) The maps \( \{T_e\}_{e \in E} \) are independent if \( \text{rk}(T_E) = \sum_{e \in E} \text{dim} W_e \).
(b) Fix \( x \in E \). The map \( T_x \) is determined by \( \{T_e\}_{e \in E \setminus \{x\}} \) if there exists a linear map \( S : W_{E \setminus \{x\}} \to W_x \) such that
\[
T_x = S \circ T_{E \setminus \{x\}}.
\]

**Definition 5.2.** Let \( M \) be a matroid on \( E \). A **vector space representation** of \( M \) consists of \( c \in \mathbb{N} \), a vector space \( V \), a collection of vector spaces \( \{W_e\}_{e \in E} \) with \( \text{dim} W_e = c \) for all \( e \in E \), and a collection of linear maps \( \{T_e : V \to W_e\}_{e \in E} \). These are required to satisfy:

(a) If \( A \subseteq E \) is independent, the maps \( \{T_e\}_{e \in A} \) are independent.
(b) If \( c \in C \subseteq E \) is a circuit then \( T_c \) is determined by \( \{T_e\}_{e \in C \setminus \{c\}} \).
We hope the proliferation of similar names (linear and multilinear representations of matroids, vector space representations) does not cause confusion.

Vector space representability for matroids is equivalent to multilinear representability for each connected component:

**Theorem 5.3.** A simple matroid has a vector space representation if and only if it is multilinear.

This is a special case of the more general Theorem 9.5 which is proved in Appendix B.

Given a representation of a finitely presented group we can construct a vector space representation of the associated generalized Dowling geometry under certain conditions.

**Theorem 5.4.** Let $G = \langle S \mid R \rangle$ be a group with a symmetric triangular presentation, and let $\rho : G \to \text{GL}(W)$ be a linear representation of $G$ in a vector space $W$. Suppose that
(a) If $s, s' \in S$ are distinct then $\rho(s) - \rho(s')$ is invertible,
(b) Whenever $s, s', s'' \in S$ (not necessarily distinct) satisfy $\rho(s^*)^{-1} \neq \rho(s's)$ the linear transformation $\rho(s'')^{-1} - \rho(s's) \in \text{End}(W)$ is invertible, and
(c) For $s, s', s'' \in S$ satisfying $\rho(ss's'') = e$, the equation $ss's'' = e$ is a relation in $R$.

Then the generalized Dowling geometry corresponding to the presentation $\langle S \mid R \rangle$ is multilinear.

Moreover, if the representation $\rho$ just satisfies the assumptions (a) and (b) then some matroid of the generalized Dowling geometries $\mathcal{M}_{S,R}$ subordinate to $\langle S \mid R \rangle$ is multilinear.

**Proof.** The first statement is the special case $\varepsilon = 0$ of the more general Theorem 9.8 proved below.

The second statement follows from the first after adding relations to $ss's'' = e$ to $R$ whenever $\rho(ss's'') = e$ holds. Note that by definition of the subordinate generalized Dowling geometries the matroid of this new presentation is a member of $\mathcal{M}_{S,R}$. $\square$

6. **GROUP SCRAMBLING**

We introduce a two-step construction to modify finitely presented groups. Its goal is to facilitate the encoding of word problems in representation problems for generalized Dowling geometries.

In this section we are working in a vector space over a field that contains $\mathbb{C}$ throughout to ensure the existence of primitive roots of unity which we use in the proofs. To show that a matroid is entropic it suffices to show that it is multilinear over some field. Therefore, this assumption doesn’t result in limitations of the main theorems of this section.

The first step, which we call *scrambling*, takes as input a symmetric triangular presentation $\langle S \mid R \rangle$ of a group $G$, and outputs a presentation $\langle S' \mid R' \rangle$ of $(G * F_R) \times \mathbb{Z}^n$ where $F_R$ is the free group on the generators $f_r$ for $r \in R$ and $*$ is the free product of groups. The new presentation has matrix representations satisfying the conditions of Theorem 5.4. The second step, which we call *augmentation*, takes as input the result of the first step together with the original presentation $\langle S \mid R \rangle$ and a generator $s \in S$. It outputs a presentation of $(G * F_R * F_4) \times \mathbb{Z}^n$ (where $F_4 = \langle z_1, \ldots, z_4 \rangle$ is the free group on four generators). The resulting presentation has $z_1$ and $sz_1s$ as two of its generators; it has a matrix representation satisfying the conditions of Theorem 5.4 if and only if there is a matrix representation $\rho$ of $G$ such that $\rho(s) \neq \rho(e)$. The “only if” direction follows from the fact that $z_1 \neq sz_1s$ only if $s \neq e$. The “if” follows from a direct construction of a representation, which is rather lengthy and forms a significant part of what follows.

6.1. **Sufficiently generic elements.** In the rest of this section we face the following sort of problem several times: given some finitely presented group $G = \langle S \mid R \rangle$, a free group $F$ on
some finite set of generators, and a linear representation \( \rho : G \ast F \to \text{GL}_n(\mathbb{C}) \), show that \( \rho(g) - I_n \) is invertible or zero.

We have some control over \( \rho \). In particular, we are able to ensure that for each \( g \in G \) the matrix \( \rho(g) \) is either \( I_n \) or the permutation matrix of a derangement. This motivates the next definition.

**Definition 6.1.** Let \( G \) be a group and \( F_T \) a free group on the set of generators \( T \). An element of \( x \in G \ast F_T \) is sufficiently generic if the following holds. Let \( \rho : G \ast F_T \to \text{GL}_n(\mathbb{C}) \) be any linear representation satisfying

(a) For each \( g \in G \), \( \rho(g) \) is either \( I_n \) or the permutation matrix of a derangement.
(b) The indexed collection of entries of the matrices \( \{\rho(t)\}_{t \in T} \) is algebraically independent over \( \mathbb{C} \).

Then \( \rho(x) - I_n \) is either invertible or 0.

We prove that various elements of \( G \ast F_T \) are sufficiently generic.

**Lemma 6.2.** Let \( g, g' \in G \) and let \( t \in T \). The following elements of \( G \ast F_T \) are sufficiently generic:

(i) The element \( gtgt^{-1} \),
(ii) the commutator \([g, t] \) and
(iii) the commutator \([g, tg'] \).

**Proof.** Let \( \rho : G \ast F_T \to \text{GL}_n(\mathbb{C}) \) be a representation satisfying the assumptions (a) and (b) of Definition 6.1. So in particular \( \rho(g) \) is the permutation matrix of a derangement and \( \rho(t) \) is a matrix with algebraically independent entries.

By Lemma 2.15 each of the matrices \( \rho(g) \) and \( \rho(g^{-1}) \) is conjugate to a diagonal block matrix in which there is no \( 1 \times 1 \) block, and each \( m \times m \) block is a diagonal matrix of the form

\[
\begin{bmatrix}
\omega^0 \\
\vdots \\
\omega^{m-1}
\end{bmatrix}
\]

for \( \omega \) an \( m \)-th root of unity. Let \( C \) be a matrix conjugating \( \rho(g) \) into such a form (and thus also \( \rho(g^{-1}) \), with \( \omega \) replaced by \( \omega^{-1} \)). If \( w \) is any word in \( g \) and \( t \), \( A := I - \rho(w) \) is invertible if and only if \( CAC^{-1} = I - C\rho(w)C^{-1} \) is invertible; this amounts to checking invertibility in a basis in which \( \rho(g^{\pm 1}) \) has the block diagonal form above. If an appropriate matrix is substituted for \( \rho(t) \), \( CAC^{-1} \) is again a block diagonal matrix, and by Corollary 2.17 to check that \( CAC^{-1} \) is invertible it suffices to check that each diagonal block is invertible.

(i) To show \( \rho(gtgt^{-1}) - I_n \) is invertible it suffices to show \( \rho(t) - \rho(gtg) \) is invertible.

In a basis in which \( \rho(g) \) has the form above, substitute a block diagonal matrix for \( \rho(t) \) in which each block is of the form

\[
\begin{bmatrix}
0 & 0 & 1 \\
0 & \ddots & 0 \\
1 & 0 & 0
\end{bmatrix}
\]
In this basis, each block of $\rho(t) - \rho(gtg)$ is of the form
\[
\begin{bmatrix}
0 & 0 & 1 \\
0 & \ddots & 0 \\
1 & 0 & 0
\end{bmatrix}
- \begin{bmatrix}
\omega^0 & & \\
& \ddots & \\
& & \omega^{m-1}
\end{bmatrix}
\begin{bmatrix}
0 & 0 & 1 \\
0 & \ddots & 0 \\
1 & 0 & 0
\end{bmatrix}
= \begin{bmatrix}
0 & 0 & 1 \\
0 & \ddots & 0 \\
1 & 0 & 0
\end{bmatrix}
- \begin{bmatrix}
0 & 0 & \omega^{m-1} \\
0 & \ddots & 0 \\
\omega^{m-1} & 0 & 0
\end{bmatrix}
= (1 - \omega^{m-1}) \begin{bmatrix}
0 & 0 & 1 \\
0 & \ddots & 0 \\
1 & 0 & 0
\end{bmatrix},
\]
which has rank $m$, so each block is invertible as desired. Thus by Corollary 2.17 the matrix $\rho(gtg^{-1}) - I_n$ is invertible.

(ii) Using again Corollary 2.17 it suffices to show that $[A, \rho(g)] - I_n$ is invertible for some invertible matrix $A$. Again, working in a basis in which $\rho(g)$ has the diagonal block form described above and taking an $A$ with the same diagonal block structure, it suffices to show this on each block separately. Note that for invertible matrices $A, B$, the matrix $[A, B] - I_n$ is invertible if and only if $AB - BA$ is invertible. To see this, note that
\[
(AB - BA) (BA)^{-1} = ABA^{-1}B^{-1} - I_n.
\]
Thus for each integer $m \geq 2$ and each primitive $m$-th root of unity $\omega$ we need to find an $m \times m$ matrix $A$ such that
\[
A \begin{bmatrix}
\omega^0 & & \\
& \ddots & \\
& & \omega^{m-1}
\end{bmatrix}
- \begin{bmatrix}
\omega^0 & & \\
& \ddots & \\
& & \omega^{m-1}
\end{bmatrix}
A
\]
is invertible. Take the matrix $A$ that acts on the standard basis $e_1, \ldots, e_n$ of the column space $\mathbb{C}^n$ by $Ae_i = e_{i+1}$ for $i < n$, and $Ae_n = e_1$. Thus
\[
A = \begin{bmatrix}
0 & & 1 \\
1 & 0 & \\
& \ddots & \\
& & 1
\end{bmatrix}
\]
where the unfilled entries are zero. Hence
\[
A \begin{bmatrix}
\omega^0 & & \\
& \ddots & \\
& & \omega^{m-1}
\end{bmatrix}
- \begin{bmatrix}
\omega^0 & & \\
& \ddots & \\
& & \omega^{m-1}
\end{bmatrix}
A
= \begin{bmatrix}
\omega^0 & 0 & \omega^{m-1} \\
0 & \ddots & 0 \\
\omega^{m-2} & 0 & \omega^{m-1}
\end{bmatrix}
- \begin{bmatrix}
0 & 0 & \omega^0 \\
0 & \ddots & 0 \\
\omega^1 & 0 & \omega^{m-1}
\end{bmatrix}
= (1 - \omega) A \begin{bmatrix}
\omega^0 & & \\
& \ddots & \\
& & \omega^{m-1}
\end{bmatrix}
\]
which is invertible, as a product of an invertible scalar and two invertible matrices.

(iii) As $\rho(g')$ is by assumption also a permutation matrix $\rho(tg')$ is also a matrix with algebraically independent entries. Thus this case follows from the previous one. \(\square\)

Now we show that the conjugation of a sufficiently generic element is sufficiently generic.

**Lemma 6.3.** In the notation of Definition 6.1, let $g, h \in G \ast F_T$ be two elements and assume $g$ is sufficiently generic. The element $hgh^{-1}$ is then sufficiently generic as well.
Proof. We have

\[ \rho(g) - I_n = \rho(h)^{-1}(\rho(hgh^{-1}) - I_n)\rho(h). \]

By assumption the matrix \( \rho(g) - I_n \) is either invertible or zero. Thus, also the matrix \( \rho(hgh^{-1}) - I_n \) is either invertible or zero. \( \square \)

6.2. Scrambled groups and their representations. We encode the properties our scrambling construction satisfies into a definition, and work with it axiomatically to defer the discussion of the implementation. The actual construction is postponed to Section 6.4.

Definition 6.4. Let \( G \) be a group given by a symmetric triangular presentation \( \langle S \mid R \rangle \). We call a finitely presented group \( G' = \langle S' \mid R' \rangle \) a scrambling of \( \langle S \mid R \rangle \) if it satisfies the following properties:

(PS1) \( \langle S' \mid R' \rangle \) is a symmetric triangular presentation.
(PS2) There is an isomorphism \( \mu : G' \to (G * F_R) \times \mathbb{Z}^N \) for some \( N \geq 0 \) where \( F_R \) is the free group on the letters \( f_r \) for \( r \in R \). We denote the projections onto the factors by

\[ \pi_G : (G * F_R) \times \mathbb{Z}^N \to G, \]

\[ \pi_Z : (G * F_R) \times \mathbb{Z}^N \to \mathbb{Z}^N, \]

\[ \pi_{ab}^{F_R} : (G * F_R) \times \mathbb{Z}^N \to \mathbb{Z}^{\lvert R \rvert} \times \mathbb{Z}^N, \]

where \( \pi_{ab}^{F_R} \) is the composition of the projection to \( F_R \times \mathbb{Z}^N \) with the abelianization homomorphism of \( F_R \). Slightly abusing notation we identify \( G' \) with \( (G * F_R) \times \mathbb{Z}^N \) via \( \mu \).

(PS3) If \( s, s' \in S' \) are distinct then \( \pi_{ab}^{F_R}(s) \neq \pi_{ab}^{F_R}(s') \).

(PS4) For any \( s, s', s'' \in S' \) (not necessarily distinct) either

(i) \( \pi_{ab}^{F_R}(s's's') \neq 0 \),
(ii) \( s's's' = e \) in \( G' \), or
(iii) \( s's's' \) is a sufficiently generic element in \( G * F_R \).

(PS5) There is a function \( i : S \to S' \) such that \( \pi_G \circ i = \text{id}_G \mid S \).

(PS6) There is a basis \( B = \{ b_1, \ldots, b_N \} \) of \( \mathbb{Z}^N \) and a function \( j : B \to S' \) such that \( \mu \circ j(b_i) = (e_{G * F_R}, b_i) \) for each \( 1 \leq i \leq N \).

(The functions \( i \) and \( j \) are to be given explicitly.)

(PS7) For each \( s \in S \) we have \( \mu(i(s)) \in (G * \{ e_F \}) \times \mathbb{Z}^N \leq (G * F_R) \times \mathbb{Z}^N \). Further, there is a \( 1 \leq k \leq N \) such that \( \pi_Z(i(s)) = \sum_{m=1}^{N} c_m b_m \) with \( c_k \geq 5 \), and such that for each \( s' \in S' \), the absolute value of the \( b_k \)-coefficient of \( \pi_Z(s') \) is at most \( c_k + 1 \).

In the subsequent we will frequently use the following immediate consequence of the definition of a group scrambling.

Proposition 6.5. In the notation of Definition 6.4 consider the equation

\[ \pi_{ab}^{F_R}(xx'x'') = 0 \]

where \( x, x', x'' \in G' \). If we fix \( x = g \) and \( x'' = g'' \) for some generators \( g, g'' \in S' \) then there is at most one \( x' \in S' \) that satisfies this equation.

Proof. Since the group \( \mathbb{Z}^{\lvert R \rvert} \times \mathbb{Z}^N \) is abelian the equation \( \pi_{ab}^{F_R}(xx'x'') = 0 \) is equivalent to \( \pi_{ab}^{F_R}(x') = -\pi_{ab}^{F_R}(gg'') \) assuming \( x = g \) and \( x'' = g'' \). Therefore by property (PS3) if there exists a generator \( g' \) such that \( x' = g' \) fulfills the equation this generator must be unique. \( \square \)

Let \( G = \langle S \mid R \rangle \) be a group with a given symmetric triangular presentation. We prove that certain matrix representations of \( G \) extend to nice representations of scramblings of \( G \).

Proposition 6.6. Let \( \langle S' \mid R' \rangle \) be a scrambling of \( G = \langle S \mid R \rangle \), so that \( \langle S' \mid R' \rangle \simeq (G * F_R) \times \mathbb{Z}^N \). Let \( \rho : G \to \text{GL}_n \mathbb{C} \) be a representation satisfying that for each \( g \in G \) the matrix \( \rho(g) \) is either the permutation matrix of a derangement or the identity matrix. Then
there exists a field extension $\mathbb{C} \subseteq \mathbb{L}$ and a representation

$$\tilde{\rho} : (G \ast F_R) \times \mathbb{Z}^N \rightarrow \text{GL}_n \mathbb{L}$$

which satisfies:

(a) If $s, s' \in S'$ are distinct then $\tilde{\rho}(s) - \tilde{\rho}(s')$ is invertible,
(b) For $s, s', s'' \in S'$ (not necessarily distinct) the matrix $\tilde{\rho}(s'')^{-1} - \tilde{\rho}(s's)$ is either invertible or zero, and
(c) $\tilde{\rho}(g) = \rho(g)$ for each $g \in G$ (where $\text{GL}_n \mathbb{C}$ is identified with its image in $\text{GL}_n \mathbb{L}$).

Proof. Let $\mathbb{L} = \mathbb{C} \left( \{ y_{r,i,j} \}_{r \in R, 1 \leq i,j \leq n} \cup \{ z_1, \ldots, z_N \} \right)$ be the field of rational functions in $|R|^n + N$ variables over $\mathbb{C}$.

The free group $F_R$ has generators $f_r$ for $r \in R$. For each such generator $f_r$ we define

$$\tilde{\rho}(f_r) = (y_{r,i,j})_{1 \leq i,j \leq n}.$$ 

For $g \in G$ define $\tilde{\rho}(g) = \rho(g)$. This extends to a representation $\tilde{\rho} : G \ast F_R \rightarrow \text{GL}_n(\mathbb{L})$ because $G \ast F_R$ is a free product, and $F_R$ is free. Thus $\langle S \cup \{ f_r \}_{r \in R} \mid R \rangle$ is a presentation of $G \ast F_R$, and it is clear that $\tilde{\rho}$ maps all words that represents relators to the identity matrix.

This representation extends further to a representation of $(G \ast F_R) \times \mathbb{Z}^N$ as follows. For $v = (v_1, \ldots, v_N) \in \mathbb{Z}^N$ define

$$\tilde{\rho}(v) = \left( \prod_{i=1}^N z_i^{v_i} \right) \cdot I_n.$$ 

If $g \in G \ast F_R$ and $v \in \mathbb{Z}^N$, define $\tilde{\rho}(gv) = \tilde{\rho}(g) \tilde{\rho}(v)$. Any element of $(G \ast F_R) \times \mathbb{Z}^N$ can be written in exactly one way in the form $gv$, so $\tilde{\rho}$ is well defined. It is a homomorphism essentially because if $v \in \mathbb{Z}^N$ then $\tilde{\rho}(v)$ is a scalar matrix, and hence commutes with the image of $\tilde{\rho}$. More explicitly, we have

$$\tilde{\rho}(g_1 v_1 \cdot g_2 v_2) = \tilde{\rho}((g_1 g_2) (v_1 v_2)) = (\tilde{\rho}(g_1) \tilde{\rho}(g_2)) (\tilde{\rho}(v_1) \tilde{\rho}(v_2))$$

$$= \tilde{\rho}(g_1) \tilde{\rho}(v_1) \tilde{\rho}(g_2) \tilde{\rho}(v_2) = \tilde{\rho}(g_1 v_1) \tilde{\rho}(g_2 v_2),$$

for $g_1, g_2 \in G \ast F_R$ and $v_1, v_2 \in Z^N$. Observe that if $v \in \mathbb{Z}^n$ is nonzero then $\tilde{\rho}(v)$ is of the form $\lambda I_n$ where $\lambda$ is transcendental over $\mathbb{C}$. It is convenient and harmless to abuse the notation by identifying scalar matrices $\lambda I_n$ with the scalar $\lambda$.

We now prove the three claimed properties. It is convenient to define an auxiliary representation $\tilde{\rho}^{ab} : (G \ast F_R) \times \mathbb{Z}^N$ which is equal to $\tilde{\rho}$ on the generators except that $\tilde{\rho}^{ab}(f_r) = y_{r,1,1}$ for all $r \in R$.

(a) Let $s, s' \in S'$ be distinct elements. Denote $v = \pi^{ab}_{F_R,Z}(s)$ and $v' = \pi^{ab}_{F_R,Z}(s')$, as well as $z = \tilde{\rho}^{ab}(v)$ and $z' = \tilde{\rho}^{ab}(v')$. By property (PS3) of scramblings $v \neq v'$, so $z^{-1} z'$ is transcendental over $\mathbb{C}$. Denote $g = \pi_G(s)$ and $g' = \pi_G(s')$. Corollary 2.17 applied to the expression $b_1 - b_2$ yields that it suffices to prove that the matrix $\rho(g) z - \rho(g') z'$ is invertible.

Since $z^{-1} z'$ is transcendental over $\mathbb{C}$, Corollary 2.18 implies that

$$\det (\rho(g) z - \rho(g') z') \neq 0.$$ 

Hence also $\det (\rho(g) z - \rho(g') z') \neq 0$.

(b) Let $s, s', s'' \in S'$ be not necessarily distinct generators. Then by property (PS4) of scramblings exactly one of the following three cases hold:
Case 1: Suppose $\pi_{F,Z}^{ab}(s''s') \neq 0$. Denote $z'' = \tilde{\rho}^{ab}(\pi_{F,Z}^{ab}(s''))$ and $z = \tilde{\rho}^{ab}(\pi_{F,Z}^{ab}(s's'))$, as well as $g'' = \pi_G(s'')$ and $g = \pi_G(s's')$. Then

$$(z'')^{-1} \rho(g'')^{-1} - z \rho(g) = (z'')^{-1} \left(\rho(g'')^{-1} - z'' z \rho(g)\right).$$

By Corollary 2.18 $\det(\rho(g'')^{-1} - z'' z \rho(g))$ is nonzero as $z'' z = \tilde{\rho}^{ab}(\pi_{F,Z}^{ab}(s''s'))$ is transcendental over $\mathbb{C}$ because $\pi_{F,Z}^{ab}(s''s') \neq 0$. Therefore by Corollary 2.17 also the matrix $\tilde{\rho}(s'')^{-1} - \tilde{\rho}(s's')$ is invertible.

Case 2: If $s''s' = \varepsilon$ then $\tilde{\rho}(s''s') = I_n$ which yields $\tilde{\rho}(s'')^{-1} - \tilde{\rho}(s's') = 0$.

Case 3: Suppose $s''s'$ is sufficiently generic. By construction of $\tilde{\rho}$ the representation matrices of elements of $G$ are either the identity matrix or permutation matrices of derangements and the entries of the representation matrices of the free generators of $F_R$ are completely transcendental elements over the prime field. So by definition of sufficiently generic elements the matrix $\tilde{\rho}(s''s') - I_n$ is invertible. Thus, also the matrix $\tilde{\rho}(s'')^{-1} - \tilde{\rho}(s's')$ is invertible.

(c) This is immediate from the construction of $\tilde{\rho}$.

6.3. The augmentation construction. We construct and prove the necessary properties of augmentations of scrambled presentations. See the beginning of Section 6 for the necessary definitions. Essentially, the goal is to obtain a presentation of $(G * F_R * \langle z_1, \ldots, z_4 \rangle) \times \mathbb{Z}^N$ with certain combinatorial properties. We recommend looking at the statements of Propositions 6.9 and 6.10 before reading the construction in detail.

Construction 6.7. Let $\langle S' \mid R' \rangle$ be a scrambling of the group $G = \langle S \mid R \rangle$ given by a symmetric triangular presentation, and let $s \in S$ be a given generator. We use the same notation as in Definition 6.4: $G' = \langle S' \mid R' \rangle$ is isomorphic to $(G * F_R) \times \mathbb{Z}^N$ for some given $N \in \mathbb{N}$, $B = \{b_1, \ldots, b_N\}$ is a basis of $\mathbb{Z}^N$, and $\mu, \pi_Z, \pi_{F,Z}, i, j$ are the same maps as in that definition.

In what follows we construct a new finitely presented group $G'' = \langle S'' \mid R'' \rangle$ by iteratively adding generators and relations to $S'$ and $R'$.

(C1) Add four generators $z_1, \ldots, z_4$ to $S'$. For each $1 \leq i \leq N$ and each $1 \leq k \leq 4$ we add the following generators and relations in order to ensure that $j(b_i)$ commutes with $z_k$ in $G''$:

(a) Add a generator $u_{z_1,i}$ and its inverse $u_{z_1,i}^{-1}$.

(b) Add the relations $u_{z_1,i} u_{z_k,i}^{-1} e = e, j(b_i) z_k u_{z_k,i}^{-1} = e, \text{ and } u_{z_1,i} j(b_i) u_{z_k,i}^{-1} z_k^{-1} = e$.

Remark 6.8. Note that the first of these relations ensures that $u_{z_1,i}$ and $u_{z_k,i}^{-1}$ are actually inverses in $G''$; the second is equivalent to $u_{z_1,i} = j(b_i) z_k$; and substituting the second relation into the third, we obtain $j(b_i) z_k j(b_i) u_{z_k,i}^{-1} z_k^{-1} = e$. We “break up” relations in this way in the rest of this construction and in Construction 6.12.

(C2) Add a new generator $t$ to $S'$. The following ensures that $t = s z_1 s$ in $G''$: Denote $s' = \varepsilon(s)$, and express $-2 \cdot \pi_{F,Z}^{ab}(s') \in \mathbb{Z}^N$ as a minimal-length sum

$$\varepsilon_1 b_{k_1} + \varepsilon_2 b_{k_2} + \ldots + \varepsilon_r b_{k_r}$$

of elements of $B$, where $\varepsilon_1, \ldots, \varepsilon_r \in \{-1, 1\}$. Recall that $\pi_{F,Z}^{ab}(s')$ is generated by elements in $B$ by property (PS7). We add generators and relations to “break up” the relation

$$t = z_4^{-1} \left( z_4 \left( z_3^{-1} ((z_3 s') (z_1 s')) \right) z_2 b_{k_1}^{e_1} z_2 b_{k_2}^{e_2} z_2 \ldots b_{k_{r-1}}^{e_{r-1}} z_2 b_{k_r}^{e_r} \right) \frac{z_2^{-1} \ldots z_2^{-1}}{r \text{ times}}.$$
(a) Add generators \( v_1, \ldots, v_4 \), one for each of the words

\[
z_3s', (z_3s')z_1, (z_3s')z_1s', (z_3^{-1}((z_3s')z_1s')) = s'z_1s'.
\]

Then add their inverses, together with relations

\[
v_1v_1^{-1}e = e, \ldots, v_4v_4^{-1}e = e
\]

and the relations

\[
z_3s'v_1^{-1} = e, \quad v_1z_1v_2^{-1} = e, \quad v_2s'v_3^{-1} = e, \quad z_3^{-1}v_3v_4^{-1} = e.
\]

These relations ensure that \( v_1 = z_3s' \), \( v_2 = (z_3s')z_1 \), \( v_3 = (z_3s')z_1s' \), and \( v_4 = s'z_1s' \) in the resulting group.

(b) Add further generators \( v_5 = v_{4+1} \) up to \( v_{4+2r} \), one for each of the words

\[
(z_3^{-1}((z_3s')z_1s'))z_2, \ldots, (z_3^{-1}((z_3s')z_1s'))z_2b_{k_1}b_{k_2}z_2 \ldots b_{k_{r-1}}z_2b_{k_r}.
\]

Add the inverses of these generators, together with the appropriate relations (in a manner analogous to the above).

(c) Add generators \( v_{5+2r} \) up to \( v_{5+3r} \), for each of the words

\[
z_4v_{4+2r}, z_4v_{4+2r}z_2^{-1}, \ldots, z_4v_{4+2r}z_2^{-1} \overbrace{\ldots z_2^{-1}}^{r \text{ times}}.
\]

Add inverses for these generators, and add the appropriate relations (again, in a manner precisely analogous to the above).

(d) Add a generator \( t \), together with its inverse and the relation \( tt^{-1}e = e \), and add the relation \( z_4^{-1}v_{5+3r}t^{-1} = e \), to ensure \( t = s'z_1s \) in \( G'' \).

(C3) Symmetrize the set of relations.

We abuse notation slightly and denote by \( b_i \) (for \( 1 \leq i \leq N \)) the element \( j (b_i) \) in \( G'' \). In such situations we use multiplicative notation. Thus for \( \epsilon \in \{-1, 1\} \), \( b_i^\epsilon \) denotes an element of \( G'' \), but \( \epsilon b_i \) denotes an element of \( \mathbb{Z}^N \).

**Proposition 6.9.** In the notation of the construction, \( G'' = \langle S'' \mid R'' \rangle \) is isomorphic to \((G * F_{R} * \langle z_1, \ldots, z_4 \rangle) \times \mathbb{Z}^N \) by an isomorphism which maps each element of \( S'' \subset S'' \) to the corresponding element of \((G * F_{R}) \times \mathbb{Z}^N \leq (G * F_{R} * \langle z_1, \ldots, z_4 \rangle) \times \mathbb{Z}^n \), and which maps \( z_1, \ldots, z_4 \) to the elements of the same name in \((G * \langle z_1, \ldots, z_4 \rangle) \times \mathbb{Z}^N \).

This isomorphism maps \( t \in S'' \) to \((sz_1s, 0) \in (G * F_{R} * \langle z_1, \ldots, z_4 \rangle) \times \mathbb{Z}^N \).

**Proof.** The proposition defines a map \( G'' \rightarrow (G * F_{R} * \langle z_1, \ldots, z_4 \rangle)\times \mathbb{Z}^N \), and this is clearly surjective. It is injective: first note that step (C1) of the construction ensures that every element of \( G'' \) commutes with each \( j (b_k) \). Consider a relation added during step (C2), skipping over all relations of the form \( yy^{-1}e = e \) for \( y \) a new generator. Each such relation is of the form \( x_1 \ldots x_n y^{-1} = e \), for \( y \) one of the new generators which does not appear in any of the previous relations (except \( yy^{-1}e = e \)). Thus, traversing this list in reverse, we may apply Tietze transformations to remove each relation along with the generator \( y \). The same procedure can be applied to the relations \( u_{2k,i}u_{2k,i}^{-1}e = e \) and \( j (b_i) z_ku_{2k,i}^{-1} = e \) and the generators \( u_{2k,i} \) (for all \( 1 \leq k \leq 4 \) and \( 1 \leq i \leq N \)), thus eliminating all new generators in \( S'' \) except for \( z_1, \ldots, z_4 \) and their inverses. It is easy to see that when this process is finished we end up with the group presentation

\[
\left\langle S' \cup \{z_1, \ldots, z_4\} \mid R' \cup \{j (b_i) z_k, j(b_i)^{-1}z_k^{-1}\} \right\rangle_{1 \leq i \leq N, 1 \leq k \leq 4},
\]

which is isomorphic to \((G * F_{R} * \langle z_1, \ldots, z_4 \rangle) \times \mathbb{Z}^N \) in the desired manner.

Observe that \( t = s'z_1s'z_2b_{k_1}z_2b_{k_2}z_2 \ldots b_{k_{r-1}}z_2b_{k_r}z_2^{-r} \) in \( G'' \), where \( s' \in S' \) maps to \((s, \pi \langle s' \rangle) \in (G * \langle z_1, \ldots, z_4 \rangle) \times \mathbb{Z}^N \) (this is its image in \( G * F_{R} \times \mathbb{Z}^N \) under \( \mu \)). \( \square \)
This proposition allows us to identify $G''$ with $(G * F_R * \langle z_1, \ldots, z_4 \rangle) \times \mathbb{Z}^N$.

**Proposition 6.10.** Let $G = \langle S \mid R \rangle$ be a group given by a symmetric triangular presentation and let $G' = \langle S' \mid R' \rangle$ be a scrambling. Let $s \in S$ and let $G'' = \langle S'' \mid R'' \rangle \simeq (G * F_R * \langle z_1, \ldots, z_4 \rangle) \times \mathbb{Z}^N$ be the associated augmentation. Then the following two conditions are equivalent:

(i) There exists a field $\mathbb{F} \supset \mathbb{C}$, an $n \in \mathbb{N}$, and a representation $\rho : G \to \text{GL}_n\mathbb{F}$ such that $\rho(s) \neq \rho(e)$.

(ii) There exists a field $\mathbb{F} \supset \mathbb{C}$, an $n \in \mathbb{N}$, and a representation

$$\tilde{\rho} : G'' \to \text{GL}_n\mathbb{F}$$

which satisfies:

(a) If $x, x' \in S''$ are distinct then $\tilde{\rho}(x) - \tilde{\rho}(x')$ is invertible,

(b) For $x, x', x'' \in S''$ a not necessarily distinct triple of generators $\tilde{\rho}(x'')^{-1} - \tilde{\rho}(x'x)$ is invertible or 0.

**Proof.** Assume (ii) holds. Identifying $G''$ with $(G * F_R * \langle z_1, \ldots, z_4 \rangle) \times \mathbb{Z}^N$ using Proposition 6.9 we observe that the generator $t \in S''$ (see Construction 6.7) is mapped to $sz_1s$, and that $z_1 \in S''$. Since $z_1, t$ are distinct generators, $\tilde{\rho}(z_1) - \tilde{\rho}(t)$ is invertible, and in particular $\tilde{\rho}(t) = \tilde{\rho}(sz_1s) \neq \tilde{\rho}(z_1)$. Thus $\tilde{\rho}(s) \neq \tilde{\rho}(e)$. Restricting $\tilde{\rho}$ to $G' \simeq (G * F_R * \langle z_1, \ldots, z_4 \rangle) \times \mathbb{Z}^N$ we obtain (i).

Assuming (i) holds, let $\rho : G \to \text{GL}_n\mathbb{F}$ be a representation such that $\rho(s) \neq \rho(e)$. By applying Lemma 2.14, changing $n$ as necessary, we obtain a new representation $\rho'$ of $G$ with the property that every $\rho(x)$ for $x \in S$ is the permutation matrix of a derangement or the identity matrix and $\rho(s) \neq I_n$. By Proposition 6.6, $\rho$ extends to a representation $\rho'$ of $G' \simeq G * F_R \times \mathbb{Z}^N$ over $\mathbb{F}(\xi_1, \ldots, \xi_n)$ satisfying conditions analogous to (a) and (b).

Define

$$\mathbb{L} = \mathbb{L} \left( \{ \xi_{k,i,j} \}^{1 \leq k \leq 4, \atop 1 \leq i, j \leq n} \right),$$

and extend $\rho'$ to $\tilde{\rho}' : G'' \to \text{GL}_n\mathbb{K}$ by defining (on generators) $\tilde{\rho}'(z_k) = (\xi_{k,i,j})^{1 \leq i, j \leq n} \in \text{GL}_n\mathbb{K}$ for each $1 \leq k \leq 4$. This defines a representation $\tilde{\rho}' : (G * F_R * \langle z_1, \ldots, z_4 \rangle) \times \mathbb{Z}^N \simeq G'' \to \text{GL}_n\mathbb{K}$ because elements of the $\mathbb{Z}^N$-factor map to scalar matrices, which commute with all matrices in $\text{GL}_n\mathbb{K}$, and because any representation of $G * F_R$ extends to a representation of $G * F_R * \langle z_1, \ldots, z_4 \rangle$ once the images of $z_1, \ldots, z_4$ are chosen (there is no constraint on these images because there are no nontrivial relations involving any of $z_1, \ldots, z_4$).

We verify that conditions (a) and (b) hold for this representation by considering the various pairs and triples of generators in $S''$. To organize the case enumeration, for each $x \in G''$ define $\deg_{z_i}(x)$ to be the degree of $x$ in $z_i$ for each $1 \leq i \leq 4$ (these degrees are well defined). Further define

$$\deg_z : G'' \to \mathbb{Z}^4,$$

$$\deg_z(x) = \left( \deg_{z_1}(x) \right)^4_{i=1}.$$

This is a homomorphism. Table 1 contains, for each pair of mutually inverse generators $x, x^{-1}$ of $S''$, a representative with nonnegative degrees in $z_1, \ldots, z_4$. Observe that if $\deg_z(x''x') \neq 0$ then $\tilde{\rho}(x'')^{-1} - \tilde{\rho}(x'x)$ is invertible. Indeed, $\deg_{z_i}(x'x) \neq \deg_{z_i}(x''^{-1})$ for some $i$. Considering

$$\det \left( \tilde{\rho}(x'')^{-1} - \tilde{\rho}(x'x) \right)$$
as a polynomial in the entries of $\tilde{\rho}(z_i)$ we see that the determinant doesn’t vanish, because it doesn’t vanish if we substitute a transcendental multiple of the identity matrix by Corollary 2.18. We also get invertibility if $\pi_{F,Z}(x''x') \neq 0$, by the same argument.

Therefore to verify the conditions it suffices to check pairs of generators $x, x'$ which have equal values under $\deg_z$ and $\pi_{F,Z}$ and triples $x'', x', x$ of generators which satisfy $\deg_z(x''x') = \pi_{F,Z}(x''x') = 0$ (the order of the generators in the product doesn’t matter because both the range of both maps is abelian). Considering the rows $R_1, \ldots, R_15$ of the table as vectors in $\mathbb{Z}^4$, we are thus looking for dependencies of the form $\pm R_i \pm R_j \pm R_k = 0$. Since all rows in the table have nonnegative degrees (and no row is 0 except the last, which corresponds to generators in $S'$, at least one of the coefficients in such a dependence must be negative and at least one must be positive. Thus we may assume (by permuting the indices if necessary) that it has the form $R_i + R_j = R_k$. Note that $e \in S'$, so this covers both conditions (a) and (b).

Given a dependence $R_i + R_j = R_k$ among the rows, let $x, x'$, and $x''^{-1}$ be the generators corresponding to $R_i, R_j,$ and $R_k$ respectively. If $\pi_{F,Z}(x''x') = e$, we must check that several elements are trivial or sufficiently generic, that is certain matrices are zero or invertible, corresponding to condition (b) for the permutations of $(x'', x', x)$ (and of $(x''^{-1}, x'^{-1}, x^{-1})$).

It suffices to consider the elements $xx'x''^{-1}$ and $x'xx''^{-1}$ Indeed, any even permutation of $(x'', x', x)$ is cyclic, and therefore the product over such a permutation is a cyclic shift of the product $x''x'x$ and hence conjugate to it (for instance $x'xx'' = x''^{-1}(x''x')x''$). Similarly an odd permutation of $(x'', x', x)$ is an even permutation of $(x', x'', x)$. And by Lemma 6.3 conjugations of sufficiently generic elements are again sufficiently generic. This also covers cases where one of the generators (say $x'$) is $e$, so it also suffices for condition (a).

| Generator $x$          | $\deg_z(x)$          |
|------------------------|-----------------------|
| $z_4$                  | $(0, 0, 0, 1)$        |
| $u_{z_4,i} = j(b_1)z_4$| $(0, 0, 0, 1)$        |
| $z_3$                  | $(0, 0, 1, 0)$        |
| $u_{z_3,i} = j(b_1)z_3$| $(0, 0, 1, 0)$        |
| $z_2$                  | $(0, 1, 0, 0)$        |
| $u_{z_2,i} = j(b_1)z_2$| $(0, 1, 0, 0)$        |
| $z_1$                  | $(1, 0, 0, 0)$        |
| $u_{z_1,i} = j(b_1)z_1$| $(1, 0, 0, 0)$        |
| $z_3s'z$               | $(0, 0, 1, 0)$        |
| $z_3s'z_1$             | $(1, 0, 1, 0)$        |
| $z_3s'z_1s'$           | $(1, 0, 1, 0)$        |
| $s'z_1s'$              | $(1, 0, 0, 0)$        |
| $s'z_1s'z_2 \ldots b_{k_i}^{1} \ldots z_2$ for $1 \leq i \leq r$ | $(1, i, 0, 0)$        |
| $s'z_1s'z_2 b_{k_i}^{1} \ldots z_2b_{k_i}^{i}$ for $1 \leq i \leq r$ | $(1, i, 0, 0)$        |
| $z_1s'z_2s' z_2b_{k_i}^{1} \ldots z_1b_{k_i}^{i} z_2^{i}$ for $0 \leq i \leq r$ | $(1, r-i, 0, 1)$      |
| $sz_1s$                | $(1, 0, 0, 0)$        |
| any $x \in S'$         | $(0, 0, 0, 0)$        |

Table 1. The generators of $S''$ together with their degrees $\deg_z$. 
We now enumerate the necessary cases by going over the possible types of $R_k \in \mathbb{Z}^4$. In all that follows, $[x, y]$ (for $x, y$ either elements of $G''$ or invertible matrices) is notation for the group-theoretic commutator $xyx^{-1}y^{-1}$.

**Case 1:** Suppose $R_k = (0, 0, 1, 0)$. Then without loss of generality $R_i = (0, 0, 1, 0)$ and $R_j = (0, 0, 0, 0)$. In this case $x''-1$ and $x$ are among $z_3$, $j(b_i)z_3$ (for some $1 \leq i \leq N$), and $z_3s'$, while $x' \in S'$. It follows that
\[
\pi_{F,Z}^{ab}(x''x) \in \{0, \pm b_i, \pm \pi_Z(s'), \pm b_i \pm \pi_Z(s')\}.
\]

**Case 1.1:** If $\pi_{F,Z}^{ab}(x''x) = 0$ it follows that $x'' = x^{-1}$, and in order that $\pi_Z(x''x'x) = 0$ we must have $x' = e$ by Proposition 6.5. Thus the product of any permutation of $(x'', x', x)$ is $e$.

**Case 1.2:** If $\pi_{F,Z}^{ab}(x''x) = \pm b_i$ we may assume $x''-1 = z_3$ and $x = j(b_i)z_3$. Proposition 6.5, $x' = j(b_i)-1$. Since $j(b_i)$ commutes with $z_3$, the possible products of permutations of $(x'', x', x)$ are then all equal to $e$.

**Case 1.3:** If $\pi_{F,Z}^{ab}(x''x) = \pm \pi_{F,Z}^{ab}(s')$ we may assume $x''-1 = z_3$ and $x = z_3s'$. Thus $\pi_{F,Z}^{ab}(x') = -\pi_{F,Z}^{ab}(s')$, and by Proposition 6.5 we must have $x' = s^{-1}$. The possible products of permutations of $(x'', x', x)$ are then all conjugate to either
\[
z_3^{-1}s^{-1}z_3s = [z_3, s^{-1}] \quad \text{or} \quad s^{-1}z_3^{-1}z_3s' = e.
\]

We deal with the case $[z_3, s^{-1}]$ in Lemma 6.11.

**Case 1.4:** If $\pi_{F,Z}^{ab}(x''x) = \pm b_i \pm \pi_{F,Z}^{ab}(s')$, we may assume $x''-1 = j(b_i)z_3$ and $x = z_3s'$. Thus $\pi_{F,Z}^{ab}(x') = b_i - \pi_Z(s')$, and by Proposition 6.5 we must have $x' = j(b_i)s'^{-1}$. In this case the elements $x'', x', x$ differ by the elements of the previous case by $j(b_i)^{\pm 1}$. Since $j(b_i)$ commutes with all other generators and cancels from any product of the triple $(x'', x', x)$, the computation is the same as in the previous case.

**Case 2:** Suppose $R_k = (0, 1, 0, 0)$ or $R_k = (0, 0, 0, 1)$. Then without loss of generality $R_i = R_k$ and $R_j = (0, 0, 0, 0)$. Each possibility in this case was checked in the $R_k = (0, 0, 1, 0)$-case with $z_3$ in place of $z_2$ or $z_4$.

**Case 3:** Suppose $R_k = (1, 0, 0, 0)$. Then without loss of generality $R_i = (1, 0, 0, 0)$ and $R_j = (0, 0, 0, 0)$.

In this case $x''-1$ and $x$ are among $z_1$, $j(b_i)z_1$ (for some $1 \leq i \leq N$), $s'z_1s'$, and $sz_1s$, while $x' \in S'$. It follows that
\[
\pi_{F,Z}^{ab}(x''x) \in \{0, \pm b_i, \pm 2\pi_Z(s'), \pm (2\pi_Z(s') - b_i)\}.
\]

There is no $x' \in S'$ with $\pi_{F,Z}^{ab}(x') \in \{\pm 2\pi_Z(s'), \pm (2\pi_Z(s') - b_i)\}$ by property (PS7) of scramblings, so either $x'' = x^{-1}$ (in which case $x' = e$ and any conjugate of any product of the triple is $e$) or one the following cases occurs:

**Case 3.1:** $\{x''-1, x\} = \{z_1, j(b_i)z_1\}$: this case was considered in the $R_k = (0, 0, 1, 0)$-case, with $z_3$ in place of $z_1$.

**Case 3.2:** $\{x''-1, x\} = \{z_1, s'z_1s\}$. In this case $x' = e$ and any product of a permutation of the triple is conjugate to $sz_1s^{-1}$. We consider this case in Lemma 6.11.

**Case 3.3:** $\{x''-1, x\} = \{j(b_i)z_1, s'z_1s\}$. In this case $x' = j(b_i)^{\pm 1}$, and since $j(b_i)$ commutes with all other generators the resulting products are just those of the previous case.

**Case 4:** Suppose $R_k = (1, 0, 1, 0)$. Then $x''-1$ is either $z_3s'z_1$ or $z_3s'z_1s'$. There are two cases to consider:

**Case 4.1:** $R_i = (1, 0, 0, 0)$ and $R_j = (0, 0, 1, 0)$.

In this case $x'$ is either $z_4$ or $j(b_i)z_3$ for some $1 \leq i \leq N$, and $x$ is one of $z_1$, $j(b_k)z_1$ (for some $1 \leq k \leq N$), $s'z_1s'$, and $sz_1s$. We consider the possibilities for $x''-1$:
Case 4.1.1: $x''^{-1} = z_3s'z$: Since $\pi_{FZ}^{ab}(s')$ is not of the form $\pm b_i \pm b_i \pm b_i$, or $\pm 2\pi (s') \pm b_i$ by property (PS7) of scramblings, it is impossible to obtain $\pi_{FZ}^{ab}(x''x'x) = 0$ in this case.

Case 4.1.2: $x''^{-1} = z_3s'z_1s'$: As in the previous case, to obtain $\pi_{FZ}^{ab}(x''x') = 0$ we must have $x' = z_3$ and $x = s'z_1s'$. The possible products of permutations of $(x'', x', x)$ are all conjugate to either

$$(z_3s'z_1s')^{-1} z_3 (s'z_1s') = e \quad \text{or} \quad z_3 (z_3s'z_1s')^{-1} (s'z_1s') = \left[ z_3, (s'z_1s')^{-1} \right].$$

We deal with the case $\left[ z_3, (s'z_1s')^{-1} \right]$ in Lemma 6.11.

Case 4.2: Suppose $R_i = (1, 0, 1, 0)$ and $R_j = (0, 0, 0, 0)$. In this case $x$ is either $z_3s'z_1$ or $z_3s'z_1s'$ and $x' \in S'$. We consider the possibilities for $x''^{-1}$:

Case 4.2.1: $x''^{-1} = z_3s'z_1$: If $x = z_3s'z_1$ then $\pi_{FZ}^{ab}(x''x) = 0$, and by Proposition 6.5 we must have $x' = e$. In this case any product of a permutation of $(x'', x', x)$ is $e$. If $x = z_3s'z_1s'$ then $\pi_{FZ}^{ab}(x''x) = \pi_{FZ}^{ab}(s')$, and again by Proposition 6.5 we must have $x' = s'^{-1}$. Any product of a permutation of $(x'', x', x)$ is then conjugate to one of

$$(z_3s'z_1)^{-1} s'^{-1} (z_3s'z_1s') = \left[ (z_3s'z_1)^{-1}, s'^{-1} \right] \quad \text{and} \quad s'^{-1} (z_3s'z_1s') = e.$$

The case $\left[ (z_3s'z_1)^{-1}, s'^{-1} \right]$ is dealt with in Lemma 6.11.

Case 4.2.2: $x''^{-1} = z_3s'z_1s'$: If $x = z_3s'z_1s'$ then by exchanging the roles of $x$ and $x''$ (and inverting all three generators) we reduce to the previous case. If $x = z_3s'z_1s'$ then $\pi_{FZ}^{ab}(x''x) = 0$, and by Proposition 6.5 we must have $x' = e$. In this case any product of a permutation of $(x'', x', x)$ is $e$.

Case 5: Suppose $R_k = (1, i, 0, 0)$ for $1 \leq i \leq r$. There are two cases to consider in this case:

Case 5.1: $R_k = (1, i, 0, 0)$ and $R_j = (0, 1, 0, 0)$.

In this case $x''^{-1}$ is either $s'z_1s'z_2\ldots b_{k_i-1}^{-1}b_2$ or $s'z_1s'z_2\ldots z_2b_i$. If $i > 1$, $x$ is either $s'z_1s'z_2\ldots z_2b_{k_i-1}^{-1}b_2$ or $s'z_1s'z_2\ldots z_2$, and thus $\pi_{FZ}^{ab}(x''x)$ is either $0$, $-\varepsilon b_{k_i}$, $-\varepsilon b_{k_i-1}$, or $-\varepsilon_{i-1} b_{k_i-1} - \varepsilon b_{k_i}$. The generator $x'$ must be either $z_2$ or $j(b_k)z_2$ for some $1 \leq k \leq N$, so in the case $\pi_{FZ}^{ab}(x''x) = -\varepsilon_{i-1} b_{k_i-1} - \varepsilon b_{k_i}$ there is nothing to check (because it implies $\pi_{FZ}^{ab}(x''x') \neq 0$). In each of the other cases, all elements $b_i$ and $j(b_k)$ vanish from the product (because they commute with all other generators, and cancel out). So the product of any permutation of $(x'', x', x)$ is conjugate to one of

$$(s'z_1s'z_2)^{-1} z_2 (s'z_1s'z_2^{-1}) = \left[ (s'z_1s'z_2)^{-1}, z_2 \right] \quad \text{and} \quad z_2 (s'z_1s'z_2)^{-1} (s'z_1s'z_2^{-1}) = e.$$

The case $\left[ (s'z_1s'z_2)^{-1}, z_2 \right]$ is dealt with in Lemma 6.11.

If $i = 1$ we have that $\pi_{FZ}^{ab}(x'')$ equals either $-2\pi_{FZ}^{ab}(s)$ or $2\pi_{FZ}^{ab}(s)$ or $-\varepsilon b_{k_i}$. Then $z_1s$ and $s_1z$ (the other possible values for $x$ have been dealt with in the case $i > 1$). Thus $\pi_{FZ}^{ab}(x)$ is one of $0$, $b_k$ (for some $1 \leq k \leq N$), and $2\pi_{FZ}^{ab}(s')$. By property (PS7) of scramblings, if $\pi_{FZ}^{ab}(x) \neq 2\pi_{FZ}^{ab}(s')$ then $\pi_{FZ}^{ab}(x''x') \neq 0$ (note that $x'$ is either $z_2$ or its product with some $j(b_k)$), and thus $\pi_{FZ}^{ab}(x')$ is either $0$ or some basis element). Therefore we need only consider the case where $x = s'z_1s'$. Since all basis elements of $\mathbb{Z}^N$ cancel in the product, it suffices to compute the products of permutations of $(x'', x', x)$ for $x''^{-1} =$
Suppose Case 6.1: \(x' = x \neq z_2\). Each such product is conjugate to one of
\[
(s', z_1s')^{-1} z_2 (s', z_1s') = [z_2^{-1}, s', z_1s'] \quad \text{and}
\]
\[
z_2 (s', z_1s')^{-1} (s', z_1s') = e.
\]
The case \([z_2^{-1}, s', z_1s']\) is dealt with in Lemma 6.11.

**Case 5.2:** \(R_i = (1, i, 0, 0)\) and \(R_j = (0, 0, 0, 0)\).

In this case, \(x' \in S'\) while \(x\) and \(x''\) are equal to one of \(s'z_1s'z_2 \ldots b_{k_i}^{ε_i-1}z_2\) and \(s'z_1s'z_2 \ldots z_2 b_{k_i}^{ε_i}\). It follows that \(π_{F,Z}^ab (x''x) \in \{±ε_i b_{k_i}, 0\}\) and therefore by Proposition 6.5 \(x' = e\) or \(x' = b_{k_i}^±\). In any case, any product of a permutation of \((x'', x', x)\) is \(e\).

**Case 6:** Suppose \(R_k = (1, i, 0, 1)\) for \(0 ≤ i ≤ r\). There are three cases to consider in this case.

In all of them we must have \(x'' = z_4 s'z_1s'z_2 b_{k_i}^{ε_i} \ldots z_2 b_{k_i}^{ε_i} z_{i-1} = z_4 s z_1 s z_2\).

**Case 6.1:** \(R_i = (1, i - 1, 0, 1)\) and \(R_j = (0, 1, 0, 0)\) (if \(i ≠ 0\)).

In this case \(x = z_4 s'z_1s'z_2 b_{k_i}^{ε_i} \ldots z_2 b_{k_i}^{ε_i} z_{i-1} = z_4 s z_1 s z_2\). Since \(π_{F,Z}^ab (x''x) = 0\) we must also have \(π_{F,Z}^ab (x') = 0\). Thus \(x' = z_2\). The product of any permutation of \((x'', x', x)\) is then conjugate to either
\[
(z_4 s z_1 s z_2)^{-1} z_2 (z_4 s z_1 s z_2)^{-1} = [z_4 s z_1 s z_2]^{-1}, z_2\]
or
\[
z_2 (z_4 s z_1 s z_2)^{-1} (z_4 s z_1 s z_2)^{-1} = e.
\]
The case \([z_4 s z_1 s z_2]^{-1}, z_2\) is dealt with in Lemma 6.11.

**Case 6.2:** \(R_i = (1, i, 0, 0)\) and \(R_j = (0, 0, 0, 1)\).

Suppose first \(i ≠ 0\). Then \(x\) is one of \(s'z_1s'z_2 \ldots b_{k_i}^{ε_i-1}z_2\) and \(s'z_1s'z_2 \ldots b_{k_i}^{ε_i-1}z_2 b_{k_i}^{ε_i}\), while \(x'\) is either \(z_4\) or \(j (b_k) z_4\) for some \(1 ≤ k ≤ N\). Supposing \(π_{F,Z}^ab (x''x') = 0\), we may ignore any basis element of \(Z^N\) in any product of a permutation of \((x'', x', x)\) (these basis elements commute with all other generators and cancel each other). Modulo the \(Z^N\) factor, \(x\) is equivalent to \(s z_1 s\) and \(x'\) is equivalent to \(z_4\). Thus any product of a permutation of \((x'', x', x)\) is conjugate to either
\[
(z_4 s z_1 s z_2)^{-1} z_4 (s z_1 s) = e \quad \text{or}
\]
\[
z_4 (z_4 s z_1 s)^{-1} (s z_1 z) = [z_4, (s z_1 s)^{-1}].
\]
The latter case is dealt with in Lemma 6.11.

If \(i = 0\) there are more possibilities for \(x\): it may additionally be one of \(z_1\), \(j (b_k') z_1\) (for some \(1 ≤ k' ≤ N\)), \(s'z_1s\), and \(s z_1 s\). The possibilities for \(x'\) remain the same. Again, assuming \(π_{F,Z}^ab (x''x') = 0\), we may work modulo the \(Z^N\) factor; thus the last two possibilities for \(x\) are both equivalent to \(s z_1 s\), which has already been considered. The first two possibilities for \(x\) are equivalent to \(z_1\). Thus the possible products of permutations of \((x'', x', x)\) are all equivalent to one of \(e, [z_4, (s z_1 s)^{-1}]\),
\[
(z_4 s z_1 s)^{-1} z_4 z_1 = s^{-1} z_1^{-1} s^{-1} z_1 \quad \text{and}
\]
\[
z_4 (z_4 s z_1 s)^{-1} z_1 = z_4 (s^{-1} z_1^{-1} s^{-1}) z_4^{-1} z_1.
\]
The case \(s^{-1} z_1^{-1} s^{-1} z_1\) is dealt with in Lemma 6.11. The case \(z_4 (s^{-1} z_1^{-1} s^{-1}) z_4^{-1} z_1\) reduces to this case: we need to show
\[
I - \hat{ρ} (z_4 (s^{-1} z_1^{-1} s^{-1}) z_4^{-1} z_1)
\]
is invertible. Considering the determinant of this matrix as a polynomial in the entries of \(\hat{ρ} (z_4)\) and \(\hat{ρ} (z_1)\), it is enough to prove this when an identity matrix is substituted for \(\hat{ρ} (z_4)\).
Case 6.3: $R_i = (1,i,0,1)$ and $R_j = (0,0,0,0)$.

In this case $x' = e$ and $x'' = x$. Thus the product of any permutation of $(x'',x',x)$ is $e$.

Case 7: Suppose $R_k = (0,0,0,0)$. Then also $R_i = R_j = (0,0,0,0)$. Since all three generators are then in $S'$, there is nothing to check: condition (b) holds by Proposition 6.6. \qed

Lemma 6.11. In the notation of Proposition 6.10, the following elements are sufficiently generic:

$$\left\{ [z_3, s'^{-1}], sz_1 s z_1^{-1}, \left[z_3, (s' z_1 s')^{-1}\right], \left[(z_3 s' z_1)^{-1}, s'^{-1}\right], \left[(s' z_1 z_2)^{-1}, z_2\right] \right\}.$$  

Proof. Observe that for all of these the value under $\pi_Z$ is 0. Therefore, all occurrence of $s'$ can be replaced with $s$ without changing the words’ value in the group $G''$.

We split these elements into several subsets:

1. $sz_1 s z_1^{-1}$ and $s^{-1} z_1^{-1} s^{-1} z_1$. The inverse of the second is conjugate to the first, so only one needs to be checked by Lemma 6.3. This commutator is sufficiently generic by Lemma 6.2 (i).

2. The commutators $[z_3, s'^{-1}] = [z_3, s^{-1}]$ and $[(z_3 s' z_1)^{-1}, s'^{-1}] = [(z_3 s z_1)^{-1}, s^{-1}]$. By substituting an appropriate matrix for $\tilde{\rho}(z_3)$, the image of each under $\tilde{\rho}$ can be brought to the form $[A, \tilde{\rho}(s^{-1})]$ for any chosen invertible matrix $A$: for the first commutator we can just set $\tilde{\rho}(z_3) = A$; for the second, we want to arrange $\tilde{\rho}((z_3 s z_1)^{-1}) = A$, and we can take $\tilde{\rho}(z_3) = A^{-1} \tilde{\rho}((s z_1)^{-1})$. Therefore these elements are sufficiently generic by Lemma 6.2 (ii).

3. The other commutators:

$$\left\{ \left[z_3, (s z_1 s)^{-1}\right], \left[(s z_1 s z_2)^{-1}, z_2\right], \left[z_3^{-1}, s z_1 s\right], \left[(s z_1 s z_2)^{-1}, z_2\right], \text{ and } \left[z_4, (s z_1 s)^{-1}\right] \right\}.$$  

Let $w$ be any of these commutators and consider $\tilde{\rho}(w)$ as a matrix entry which are polynomials in the entries of the matrices $\{\tilde{\rho}(z_i)\}_{i=1}^4$. It is clear that for any pair of invertible matrices $A, B$ we can arrange for $\tilde{\rho}(w)$ to equal $[A, B]$ by choosing the entries of $\{\tilde{\rho}(z_i)\}_{i=1}^4$ appropriately. For example, for $\left[(z_4 s z_1 s z_2)^{-1}, z_2\right]$ we can set $\tilde{\rho}(z_3) = B, \tilde{\rho}(z_1) = I$, and take $\tilde{\rho}(z_4)$ to be the unique matrix such that $\tilde{\rho}((z_3 s z_1 s z_2)^{-1}) = A$. Similarly, for $\left[z_3, (s z_1 s)^{-1}\right]$ we can set $\tilde{\rho}(z_3) = A$ and take $\tilde{\rho}(z_1)$ to be the unique matrix such that $\tilde{\rho}((s z_1 s)^{-1}) = B$. By setting $B = \tilde{\rho}(s^{-1})$ this reduces all of these commutators to the commutators of (2). \qed

6.4. The scrambling construction. We describe a construction fulfilling the axioms for group scramblings (see Definition 6.4).

Construction 6.12. Let $G = \langle S \mid R \rangle$ be a group given by a symmetric triangular presentation. We construct a finitely presented group $G' = \langle S' \mid R' \rangle$ together with an isomorphism $\varphi : G' \to G \times \mathbb{Z}^{S|R}$ in a sequence of steps. In each step (except the first preprocessing step) a group $G_i = \langle S_i \mid R_i \rangle$ and a homomorphism $\varphi_i : G_i \to G \times \mathbb{Z}^{S|R}$ is constructed. It is always the case that $S_i \subset S_{i+1}, R_i \subset R_{i+1}$, and $\varphi_{i+1} | S_i = \varphi_i | S_i$. We take $G'$ and $\varphi$ to be the group presentation and homomorphism of the last step.

In what follows we denote by $B = \{b_s\}_{s \in S} \cup \{b_r\}_{r \in R}$ a basis for $\mathbb{Z}^{S|R}$.

(CSI) (A preprocessing step.) We modify $\langle S \mid R \rangle$ to arrange that no relation $abc = e$ in $R$ contains the same generator twice (though it may contain a generator and its inverse) as follows. If some $s \in S$ appears twice or three times in some relation in $R$, add new elements $s$ and $s''$ to $S$, and add the relations $ss'e = e$ and $ss''e = e$ to $R$. Then, in
In this step we add generators for the formal inverse of \( x_s \). We call \( x_s^{-1} \) the formal inverse of \( x_s \). We consider mutually inverse generators \( s, s^{-1} \) in \( S \) as distinct for this purpose. In particular, for any such pair there are four symbols: \( x_s, x_{s-1}, x_s^{-1}, \) and \( x_{s-1}^{-1} \). Furthermore, define symbols \( w_r, w_r^{-1} \) for each \( r \in R \). Set \( S_0 = \{ x_s, x_s^{-1} \}_{s \in S} \cup \{ w_r, w_r^{-1} \}_{r \in R} \cup \{ e \} \), \( R_0 = \{ x_s x_s^{-1} e = e \}_{s \in S} \cup \{ w_s w_s^{-1} e = e \}_{r \in R} \), and \( G_0 = \langle S_0 \mid R_0 \rangle \), so that \( G_0 \) is a free group on \( |S| \) generators (note: \( x_s \) and \( x_{s-1} \) are not inverses in \( G_0 \) for any pair \( s, s^{-1} \in S \)). Then define \( \varphi_0 : G_0 \to (G * F_R) \times \mathbb{Z}^{S \cup R} \) where \( F_R \) is the free group with generators \( f_r \) for \( r \in R \) by setting \( \varphi_0 (x_s) = (s, 5b_s) \quad \varphi_0 (w_r) = (f_r, 0) \) for each generator \( x_s \) and \( w_r \), and extending to \( G_0 \).

In this step we add generators for the \( \mathbb{Z}^{S \cup R} \) part together with the appropriate commutators as relations to ensure they commute with all other generators.

(a) For each \( s \in S \) define symbols \( t_s \) and \( t_s^{-1} \), and for each \( r \in R \) define symbols \( t_r \) and \( t_r^{-1} \) (again, mutually inverse generators \( s, s^{-1} \) in \( S \) are distinct for this purpose). Define \( T^+ = \{ t_s \}_{s \in S} \cup \{ t_r \}_{r \in R} \) let \( T^- = \{ t_s^{-1} \}_{s \in S} \cup \{ t_r^{-1} \}_{r \in R} \) be the formal inverses of those symbols in \( T^+ \), and define \( T = T^+ \cup T^- \).

Choose a linear ordering \( \prec \) on \( T^+ \).

(b) For each \( s \in S \) and \( t \in T^+ \) define new symbols \( u_{s,t} \) and \( u_{s,t}^{-1} \). Similarly for each \( r \in R \) and \( t \in T^+ \) define new symbols \( u_{r,t} \) and \( u_{r,t}^{-1} \). Lastly for distinct \( t_1, t_2 \in T^+ \) with \( t_1 \prec t_2 \) define the new symbols \( u_{t_1,t_2} \) and \( u_{t_1,t_2}^{-1} \). Denote the set of all these symbols by \( U \), and define \( S_1 = S_0 \cup T \cup U \).

If \( t_1 \prec t_2 \) are elements of \( T^+ \), define the additional notation \( u_{t_1,t_2} \) for \( u_{t_2,t_1} \) (it is not a distinct symbol). Similarly let \( u_{t_1,t_2}^{-1} \) denote \( u_{t_2,t_1}^{-1} \).

(c) Write the following relations: for each pair of mutually inverse symbols \( y, y^{-1} \) in \( T \cup U \), write the relation \( yy^{-1} e = e \). For each \( s \in S \) and \( t \in T^+ \), write the relations \( x_s t u_{s,t}^{-1} e = e \) and \( u_{s,t} x_s^{-1} t^{-1} e = e \) (here \( t^{-1} \in T^- \) is the formal inverse of \( t \in T^+ \)). Similarly for each \( r \in R \) and \( t \in T^+ \), write the relations \( w_r t u_{r,t}^{-1} e = e \) and \( u_{r,t} w_r^{-1} t^{-1} e = e \). Denote the set of all these relations by \( R_T \). Define \( R_1 = R_0 \cup R_T \).

Define \( G_1 = \langle S_1 \mid R_1 \rangle \), and define \( \varphi_1 : G_1 \to (G * F_R) \times \mathbb{Z}^{S \cup R} \) by setting \( \varphi_1 (t_s) = b_s \) for each \( s \in S \), \( \varphi_1 (t_r) = b_r \) for each \( r \in R \), \( \varphi_1 (x_s) = \varphi_0 (x_s) \), and extending to all other generators and elements as the relations dictate (for example, if \( t \in T^+ \) and \( s \in S \) then \( \varphi_1 (u_{s,t}) = \varphi_0 (x_s) \cdot \varphi_1 (t) \)).

Note that \( \varphi_1 \) is surjective: \( (e, b_r) \) and \( (e, b_s) \) are in the image for each \( r \in R \) and each \( s \in S \). Similarly \( (s, 5b_s) \) is in the image for each \( s \in S \).
(CS4) Order $R$ arbitrarily, and denote the relations by $r_1, \ldots, r_n$. For each relation $r = r_j$, in order, for $j = 1, \ldots, n$: 

(a) Write $r$ as $abc = e$ for $a, b, c \in S$ (by step (1) these are distinct).

(b) Define generators and relations to “break up” the relation

$$w_r^{-1}(w_r x_a t_r^5 x_b t_r^5 x_c (t_a^{-1} t_r^{-1} t_b^{-1} t_c^{-1})^5) = e$$

from left to right. Explicitly, write out the word on the left hand side of the relation without the $w_r^{-1}$:

$$w_r x_a t_r \ldots t_r x_b t_r \ldots t_r x_c t_a^{-1} t_r^{-1} t_b^{-1} t_c^{-1} \ldots t_a^{-1} t_r^{-1} t_b^{-1} t_c^{-1}$$

Then define symbols $y_{r,1}, \ldots, y_{r,36}$ (together with formal inverses $y_{r,1}^{-1}, \ldots, y_{r,36}^{-1}$), one for each prefix of this word, omitting the empty prefix, the first prefix $w_r$ and the final three prefixes (the entire word, and the entire word with the last or the two last letters omitted). Denote the set of all these symbols by $Y_r$. Write the following relations:

$$w_r x_a y_{r,1} = e, \quad y_{r,1} t_r y_{r,2}^{-1} = e, \quad \ldots, \quad y_{r,35} t_b^{-1} y_{r,36} = e.$$  

(Multiplying by the symbols $y_{r,i}$ from the right and substituting the previous relation into each relation in turn, these read $y_{r,1} = w_r x_a$, $y_{r,2} = w_r x_a t_r$, and so on up to $y_{r,36} = w_r x_a t_r \ldots t_b^{-1}$, which equals the entire word without the final two letters $t_r^{-1} t_c^{-1}$.) Finally, write the relation

$$w_r^{-1} y_{r,36} u_{t_c, t_r} = e.$$  

Also, for each $y_{r,i}$ write the relation $y_{r,i} y_{r,i}^{-1} e = e$.

Denote the set of all these relations by $R_r$. Then define $S_{j+1} = S_j \cup Y_r$ and $R_{j+1} = R_j \cup R_r$, $G_{1+j} = \langle S_{1+j} \mid R_{1+j} \rangle$, and extend $\varphi_j : G_j \to (G * F_R) \times \mathbb{Z}^{S \cup R}$ to

$$\varphi_{j+1} : G_{j+1} \to (G * F_R) \times \mathbb{Z}^{S \cup R}$$

in the manner dictated by the relations (this is possible because every generator $y \in S_{1+j} \setminus S_j$ satisfies a relation which defines it in terms of previous generators.) Observe that $\varphi_{1+j}$ is a homomorphism: it maps every relator of $R_{1+j}$ to the identity.

For “trivial” relators of the form $yy^{-1}e = e$ this is obvious, and similarly for the 36 relations

$$w_r x_a y_{r,1}^{-1}, \quad y_{r,1} t_r y_{r,2}^{-1}, \quad \ldots, \quad y_{r,35} t_b^{-1} y_{r,36},$$

since they define $y_{r,1}, \ldots, y_{r,36}$ in terms of the previous generators. For the relator $w_r^{-1} y_{r,36} u_{t_c, t_r}$, note that $u_{t_c, t_r} = t_c t_r$, and when we substitute previous relations into it we obtain

$$w_r^{-1} w_r x_a t_r^5 x_b t_r^5 x_c (t_a^{-1} t_r^{-1} t_b^{-1} t_c^{-1})^5 = e.$$  

When the left hand side is evaluated under $\varphi_j$ we obtain precisely $abc$, but this product is the identity in $G$, as desired.

(CS5) (Postprocessing.) Let $G_{n+1} = \langle S_{n+1} \mid R_{n+1} \rangle$ be the presentation of the last step and $\varphi_{n+1} : G_{n+1} \to (G * F_R) \times \mathbb{Z}^{S \cup R}$ the corresponding homomorphism. Symmetrize the set of relations. For any relation $abc = e$ in $R_{n+1}$ in which $a = e$ or $a \in T$, add the relations $bac = e$ and $bca = e$. Then symmetrize the set of relations again. This does not change the group: each generator in $T$ commutes with all other generators.

Remark 6.13. It is obvious from the construction that it is computable. The presentation $\langle S' \mid R' \rangle$ can be computed from $\langle S \mid R \rangle$, and the homomorphism $\varphi$ can be computed in the sense that we can explicitly write the image of each generator in $S'$ (as a tuple consisting of a word in the generators $S$ and an explicitly-given element of $\mathbb{Z}^{S \cup R}$).
Theorem 6.14. Let $G = \langle S \mid R \rangle$ be a group given by symmetric triangular presentation. Let $G' = \langle S' \mid R' \rangle$ and $\varphi : G' \to G \times \mathbb{Z}^{\text{SL}R}$ be the output of Construction 6.12 applied to $\langle S \mid R \rangle$. Then $\langle S' \mid R' \rangle$ is a group scrambling of $\langle S \mid R \rangle$ in the sense of Definition 6.4.

Proof of Theorem 6.14. Properties (PS3) and (PS4) require some case enumeration and are therefore split up into the Lemmas 6.15 and 6.16.

(PS1): The generating set $S'$ is symmetric by construction, and similarly all relations in $R'$ have length three. The relations are cyclically symmetric as we symmetrized the relations in the last step of the construction.

(PS2): Denote $N = |S \sqcup R|$. We prove that $\mu = \varphi : G' \to (G * F_{R'}) \times \mathbb{Z}^{\text{SL}R} \simeq (G * F_{R}) \times \mathbb{Z}^N$ is an isomorphism:

1. It is a homomorphism, as explained in the construction.
2. It is surjective because $\varphi_1 : G_1 = \langle S_1 \mid R_1 \rangle \to (G * F_{R'}) \times \mathbb{Z}^{\text{SL}R}$ is surjective, where $S_1 \subset S'$ and $\varphi(s) = \varphi_1(s)$ for each $s \in S_1$.
3. It is injective: just like in the proof of Proposition 6.9, all generators except for $\{x_s \in \mathcal{S} \cup \{t_r\} \in \mathcal{R} : 1 \leq r \leq 5\}$ can be eliminated using Tietze transformations. The relations then simplify to:
   1. $t_s, x = e$ for each generator $x \neq t_s$.
   2. $t_r, x = e$ for each generator $x \neq t_r$.
   3. For each mutually inverse pair $s, s^{-1} \in S'$, the relation $x_{s^{-1}}x_s = e$.
   4. For each relation $abc = e$ in $\langle S \mid R \rangle$, the relation $w^{-1}_r w_x x_a t_a t_b t_c (t_a t_b t_c)^{-1} = e$.

Since $\{t_s \in \mathcal{S} \cup \{t_r\} \in \mathcal{R} \}$ commute with all generators, the relation of the form $w^{-1}_r w_x x_a t_a t_b t_c (t_a t_b t_c)^{-1} = e$ can be replaced by $x_a t_a t_b t_c = e$. Using further Tietze transformations, introduce for each $s \in S$ a new generator $\tilde{x}_s$ and the relation $\tilde{x}_s = x_s t_s^{-5}$. Since each generator $x_s$ can be expressed as $\tilde{x}_s t_s^5$, the generators $\{x_s \in \mathcal{S} \}$ can be eliminated (again by Tietze transformations). This yields a presentation with generators $\{\tilde{x}_s \in \mathcal{S} \cup \{w_r \} \in \mathcal{R} : 1 \leq r \leq 5\}$, with relations similar to the above: the relations of type (a) and (b) are the same, relations of type (c) are replaced by $\tilde{x}_s \tilde{x}_s^{-1} = e$, and each relation of type (d) is replaced by $\tilde{x}_a \tilde{x}_b \tilde{x}_c = e$ for each relation $abc = e$ in $R$. It is clear that the resulting group is isomorphic to $(G * F_{R'}) \times \mathbb{Z}^{\text{SL}R}$ with $\mu$ mapping each $\tilde{x}_s$ to the corresponding $s \in S$, each $w_r$ to the free generator $f_r$, and each element of $\{t_s \in \mathcal{S} \cup \{t_r\} \in \mathcal{R} \}$ to the corresponding basis element of $\mathbb{Z}^{\text{SL}R}$.

(PS5): Define $i : S \to S'$ by $i(s) = x_s$. Then $\pi_G(i(s)) = s$.

(PS6): Denote $B = \{b_s \} \in \mathcal{S} \cup \{b_r \} : 1 \leq r \leq 5\}$. This is a basis of $\mathbb{Z}^{\text{SL}R} \simeq \mathbb{Z}^N$. Define $j : B \to S'$ by $j(b_s) = t_s$ (for all $s \in S \cup R$). Then $\mu(j(b_s)) = (e, b_s)$.

(PS7): Let $s \in S$. Then $\pi_Z(i(s)) = \pi_Z(x_s) = 5b_s$, so (expressed in the basis $B = \{b_s \} \in \mathcal{S} \cup \{b_r \} : 1 \leq r \leq 5\}$ the $b_s$-coefficient of $\pi_Z(i(s))$ is at least 5. We verify that the $b_s$-coefficient of $\pi_Z(s')$ (expressed in $B$) is at most 6 for each $s' \in S'$:

1. If $x$ is one of the generators added in step (1) then $\pi_Z(x) = \pm 5b$ for some $b \in B$, and its $b_s$-coefficient is clearly at most 6 in absolute value.
2. If $x$ is one of the generators $w_r$ and $w_r^{-1}$ it is zero under the projection $\pi_Z$.
3. Similarly, any of the generators $t_s$ or $t_r$ added in step (2) have $b_s$-coefficient at most 1 in absolute value.
4. The generators $u_{s,t}$ added in step (3) have $b_s$-coefficient at most 6 in absolute value; the generators $u_{t_1,t_2}$ have $b_s$-coefficient at most 1 in absolute value.
(5) If $x$ is one of the generators added in step (4), there is a relation $abc = e$ in $R$ such that $x$ is a proper prefix of

$$w_1 t_a^{-1} t_b^{-1} t_c^{-1} t_a^{-1} t_b^{-1} t_c^{-1} \ldots t_a^{-1} t_b^{-1} t_c^{-1}.$$

If $s \notin \{a, b, c\}$ then $\pi_Z(x)$ has $b_s$-coefficient 0. If $s \in \{a, b, c\}$, then since $a, b, c$ are distinct it is easy to see that $\pi_Z(x)$ has $b_s$-coefficient nonnegative and at most 5.

**Lemma 6.15.** Properties (PS3) and (PS4) hold for the generators added in the steps (CS1)-(CS3) of Construction 6.12.

**Proof.** Table 2 contains the generators defined in steps (1-3) of the construction (one representative from each mutually inverse pair) together with their values under $\pi_{F,Z}^{ab}$. (We slightly abuse notation: if $t \in T^+ = \{t_s\}_{s \in S} \cup \{t_r\}_{r \in R}$ then $b_t$ refers to $b_s$ or $b_r$ according to the value of $t$. Further, we denote by $f_r$ both the generators of the free group $F_R$ and its abelianization $\mathbb{Z}[R]$.)

| Generator $x$ | $\pi_{F,Z}^{ab}(x)$ |
|---------------|-----------------|
| $e$           | 0               |
| $x_s$ for each $s \in S$ | $5b_s$         |
| $w_r$ for each $r \in R$ | $f_r$         |
| $t_s$ for each $s \in S$ | $b_s$         |
| $t_r$ for each $r \in R$ | $b_r$         |
| $u_{s,t}$ for $s \in S$, $t \in T^+$ | $5b_s + b_t$ |
| $u_{r,t}$ for $r \in R$, $t \in T^+$ | $f_r + b_t$ |
| $u_{t_1,t_2}$ for distinct $t_1, t_2 \in T^+$ | $b_{t_1} + b_{t_2}$ |

**Table 2.** The generators added in the steps (CS1)-(CS3) of the scrambling construction.

For Property (PS3) it suffices to verify that the values of any two of the generators in the table under $\pi_{F,Z}^{ab}$ are distinct, and that the value of any generator under $\pi_{F,Z}^{ab}$ is different than the value of the inverse of another generator. This is clear by inspection of the rows of the table.

We now verify Property (PS4) by checking that if generators $x, x', x''$ from Table 2 satisfy $\pi_{F,Z}^{ab}(xx'x'') = 0$ then the word $xx'x''$ is trivial in $G'$ or sufficiently generic. So assume these generators satisfy $\pi_{F,Z}^{ab}(xx'x'') = 0$. This means we have $\pi_{F,Z}^{ab}(x) + \pi_{F,Z}^{ab}(x') + \pi_{F,Z}^{ab}(x'') = 0$. But the $\pi_{F,Z}^{ab}$-values in Table 2 are positive linear combinations of the elements of the basis of $\mathbb{Z}[R] \times \mathbb{Z}^N$, so at least one of the generators $x, x', x''$ is the inverse of a generator listed in this table. By negating the equation if necessary, we may assume without loss of generality that exactly one is the inverse of a generator listed in Table 2, and after replacing $x''$ by $x''^{-1}$ and renaming the generators if necessary we obtain the equation

$$\pi_{F,Z}^{ab}(x) + \pi_{F,Z}^{ab}(x') = \pi_{F,Z}^{ab}(x'').$$

Subsequently we need to show that for generators $x, x', x''$ that satisfy this equation the elements $xx', x''^{-1}, x'x''^{-1}, x''^{-1}xx', x'xx''^{-1}, x''^{-1}x', x''^{-1}x'x$ are all trivial or sufficiently generic. Note that the cyclic shifts of these words arise by conjugating with $x^{-1}$ or $x'$.
As conjugation preserves the set of sufficiently generic words by Lemma 6.3 it suffices to consider the elements $xx'x''^{-1}$ and $x'xx''^{-1}$ in the following.

So we now look for all generators $x, x', x''$ in Table 2 satisfying Equation $(\pi_{F,Z}^{ab})$ and check if the elements $xx'x''^{-1}$ and $x'xx''^{-1}$ are trivial in $G'$ or sufficiently generic. We split the argument into cases based on the value of $x''$. We can exclude the cases $x = e$ or $x' = e$ as this would imply $\pi_{F,Z}^{ab}(xx''^{-1}) = e_F$ or $\pi_{F,Z}^{ab}(x'x''^{-1}) = e_F$ respectively, and there exist no nontrivial solution to these equations by property (PS3) which we already verified above.

If $g_1, g_2, g_3$ are generators in Table 2 we don’t distinguish between the solutions $x = g_1$, $x' = g_2$, $x'' = g_3$ and $x = g_2$, $x' = g_1$, $x'' = g_3$ as we analyze the words $xx'x''^{-1}$ and $x'xx''^{-1}$ for each such solution in both cases.

**Case 1:** Suppose $x'' = e$. Then $x = w_r$, $x' = w_r^{-1}$ for some $r \in R$. Both words $xx'x''^{-1}$ and $x'xx''^{-1}$ are trivial in $G'$ in this case.

**Case 2:** Suppose $x'' = x_s$ for some $s \in S$. There is no solution in this case.

**Case 3:** Suppose $x'' = w_r$ for some $r \in R$. There is no solution in this case.

**Case 4:** Suppose $x'' = t_s$ for some $s \in S$. There is no solution in this case.

**Case 5:** Suppose $x'' = t_r$ for some $r \in R$. Then $x = w_r^{-1}$, $x' = u_{r,t}$, and both associated words are trivial in $G'$.

**Case 6:** Suppose $x'' = u_{s,1}$ for $s \in S$ and $t \in T^+$. The unique solution is $x = x_s$ and $x' = t$.

In this case $x''^{-1}x'x = u_{s,1}^{-1}x_s = e$ is a relator in $R'$, as is $u_{s,1}^{-1}tx = e$.

**Case 7:** Suppose $x'' = u_{r,t}$ for $r \in R$ and $t \in T^+$. The unique solution is $x = w_r$ and $x' = t$. The resulting words are again trivial in $G'$.

**Case 8:** Suppose $x'' = u_{1,t_1}t_2$ for $t_1, t_2 \in T^+$. The unique solution is $x = t_1$ and $x' = t_2$. In this case $x''^{-1}x'x = u_{1,t_1}^{-1}t_1t_2 = e$ is a relation in $R'$.

□

**Lemma 6.16.** Properties (PS3) and (PS4) hold for all generators added in the scrambling construction.

**Proof.** We inductively verify that these properties still hold when further generators are added for each relation in $R$ in step (CS4) of Construction 6.12. To this end, order the relations in $R$ arbitrarily and denote them (in order) $r_1, \ldots, r_n$. By induction on $1 \leq j \leq n$ we show that:

(i) For each $j = 1, \ldots, n$, the generators $\left\{ y_{r_j,i}^{\pm 1} \right\}_{i=1}^{36}$ all satisfy that their value under $\pi_{F,Z}^{ab}$ involves $b_{r_j}$ or $f_{r_j}$ and no other element of $\{b_r, f_r\}_{r \in R}$.

(ii) The generators added in steps (CS1)-(CS3) of the construction, together with $\bigcup_{k \leq j} \left\{ y_{r_k,i}^{\pm 1} \right\}_{i=1}^{36}$ satisfy conditions (PS3) and (PS4).

Let the $j$-th relation $r_j$ be $abc = e$. Table 3 lists one generators from each mutually inverse pair $\left\{ y_{r_j,i}, y_{r_j,i}^{-1} \right\}$ added in step (CS4) for this relation.

Part (i) is clear: the new generators all satisfy that their value under $\pi_{F,Z}^{ab}$ involves $b_{r_j}$ or $f_{r_j}$ and no other element of $\{b_r, f_r\}_{r \in R}$. We need to verify (ii), i.e. conditions (PS3) and (PS4).

For condition (PS3) it suffices to check that any two of the new generators have distinct values under $\pi_{F,Z}^{ab}$, and that their values under $\pi_{F,Z}^{ab}$ are distinct from those of the generators added in steps (CS1)-(CS3) of the construction. Note that the values of $\pi_{F,Z}$ in Table 3 are all distinct, so it suffices to compare these generators with the ones added in steps (CS1)-(CS3). These all have a $b_{r_j}$-coefficient at most one. We list all generators which after applying $\pi_{F,Z}^{ab}$ have $b_{r_j}$-coefficient one or involve the generator $f_{r_j}$ in Table 4. Apparently, any two of these have different values under $\pi_{F,Z}^{ab}$. and it is not possible that $\pi_{F,Z}^{ab}(x) = \pi_{F,Z}^{ab}(x') = -\pi_{F,Z}^{ab}(x')$. 

we proceed similarly as above, namely we consider generator \( \pi_3 \) of the scrambling construction.

\[
\text{Case 1:}\quad \pi_3(x) = f_r + 5b_a + (i-1)b_r
\]

\[
\text{Case 2:}\quad \pi_3(x) = f_r + 5b_a + 5b_b + (i-2)b_r
\]

\[
\pi_3(x) = f_r + 5b_a + 5b_b + 10b_r
\]

\[
\text{Tables 3 and 4. The generators of the relation } r_j \text{ in step (CS4) of the scrambling construction.}
\]

| Generator \( x \) | \( \pi_{F,Z}^{ab}(x) \) |
|-------------------|----------------------|
| \( y_{r,j,i} \) for \( 1 \leq i \leq 6 \) | \( f_r + 5b_a + (i-1)b_r \) |
| \( y_{r,j,i} \) for \( 7 \leq i \leq 12 \) | \( f_r + 5b_a + 5b_b + (i-2)b_r \) |
| \( y_{r,j,13} \) | \( f_r + 5b_a + 5b_b + 10b_r \) |
| \( y_{r,j,13+5k} \) for \( 1 \leq k \leq 4 \) | \( f_r + (5-k)b_a + (5-k)b_b + (5-k)b_c + (10-2k)b_r \) |
| \( y_{r,j,14+5k} \) for \( 0 \leq k \leq 4 \) | \( f_r + (4-k)b_a + (5-k)b_b + (5-k)b_c + (10-2k)b_r \) |
| \( y_{r,j,15+5k} \) for \( 0 \leq k \leq 4 \) | \( f_r + (4-k)b_a + (5-k)b_b + (5-k)b_c + (9-2k)b_r \) |
| \( y_{r,j,16+5k} \) for \( 0 \leq k \leq 4 \) | \( f_r + (4-k)b_a + (4-k)b_b + (5-k)b_c + (9-2k)b_r \) |
| \( y_{r,j,17+5k} \) for \( 0 \leq k \leq 3 \) | \( f_r + (4-k)b_a + (4-k)b_b + (5-k)b_c + (8-2k)b_r \) |

For condition (PS4) we proceed similarly as above, namely we consider generators \( x, x', x'' \) in the Tables 2 and 3 that satisfy Equation (\( \pi_{F,Z}^{ab} \)). We verify that for these generators the words \( xx'x''-1 \) and \( xx'xx''-1 \) are trivial in \( G' \) or sufficiently generic.

By the above discussion we may exclude those cases in which \( x = e \) or \( x' = e \). As above, we don’t distinguish between the solutions \( x = g_1, x' = g_2, x'' = g_3 \) and \( x = g_2, x' = g_1, x'' = g_3 \) for generators \( g_1, g_2, g_3 \) as we analyze the words \( xx'x''-1 \) and \( xx'xx''-1 \) for each such solution in both cases. We may also restrict to cases in which at least one of the generators involves a generator \( y_{r,j,k} \) for \( 1 \leq k \leq 36 \) as otherwise the condition was already checked in Lemma 6.15. We begin by assuming that \( x'' = y_{r,j,k} \) for some \( 1 \leq k \leq 36 \). This yields the following cases.

**Case 1:** Suppose \( x'' = y_{r,j,1} \). In this case the only solution is \( x = x_a, x' = w_{r_j} \) which yields the words \( w_{x_a}w_{x_a^{-1}}w_{r_j^{-1}} \) and \( w_{x_a}w_{x_a^{-1}}w_{r_j^{-1}} \). The former is sufficiently generic by Lemma 6.2 (ii) and the latter is clearly trivial in \( G' \).

**Case 2:** Suppose \( x'' = y_{r,j,k} \) with \( 2 \leq k \leq 6 \). In this case there are the following solutions:
(1) If $k = 2$ there is $x = u_{a,t_{r_j}}$, $x' = w_r$ which yields the words $x_a t_r, w_r t_r^{-1} x_a^{-1} w_r^{-1}$ and $w_r x_a t_r, t_r^{-1} x_a^{-1} w_r^{-1}$. Since $t_{r_j}$ commutes with all other involved letters this case reduces to the previous one.

(2) If $k = 2$ there is $x = x_a$, $x' = u_{r_j,t_{r_j}}$ which yields the words $x_a u_{r_j} t_r, t_r^{-1} x_a^{-1} w_r^{-1}$ and $w_r u_{r_j} t_r, t_r^{-1} x_a^{-1} w_r^{-1}$. These words again reduce to the $k = 1$ case.

(3) If $k = 3$ there is $x = u_{a,t_{r_j}}$, $x' = u_{r_j,t_{r_j}}$ which yields the words $x_a t_r, w_r t_r^{-1} t_r x_a^{-1} w_r^{-1}$ and $w_r x_a t_r, t_r^{-1} x_a^{-1} w_r^{-1}$ which also reduces to the $k = 1$ case.

(4) For all $k = 2, \ldots, 6$ there is $x = y_{r_j,k-1}$, $x' = t_{r_j}$ which yields trivial words in $G'$ in both orders.

**Case 3:** Suppose $x'' = y_{r_j,k}$ with $7 \leq k \leq 12$. In this case we have the solution $x = y_{r_j,k-1}$, $x' = t_{r_j}$ which yields either the trivial element in $G'$ or (after canceling $t_{r_j}$) the word

$$x_b w_r x_a x_c^{-1} x_a^{-1} w_r^{-1} = [x_b, w_r x_a].$$

This word is sufficiently generic by Lemma 6.2 (iii). For $k = 7$ there is the additional solution $x = y_{r_j,5}$, $x' = u_{b,t_{r_j}}$ which yields the same words as the previous solution.

**Case 4:** Suppose $x''' = y_{r_j,13}$. There is $x = y_{r_j,12}$, $x' = x_c$ and $x = y_{r_j,11}$, $x' = u_{c,t_{r_j}}$ which yields a trivial word in $G'$ and the word

$$x_c w_r x_a x_b x_c^{-1} x_b^{-1} x_a^{-1} w_r^{-1} = [x_c, w_r x_a x_b].$$

This word is sufficiently generic by Lemma 6.2 (iii). Furthermore there are solutions $x = y_{r_j,14}, x' = t_a$ and $x = y_{r_j,15}, x' = u_{a,t_{r_j}}$. Both solutions yield in both orders trivial words in $G'$ as all $t$’s commute with all other letters.

**Case 5:** Suppose $x'''' = y_{r_j,k}$ with $14 \leq k \leq 34$. The prefixes $y_{r_j,k}$ all involve $f_{r_j}$ and at least three different bases elements of $B$ with $b_{r_j}$-coefficient at least two. Thus the only solutions involve the two previous or the two following prefixes and the appropriate letters that got added between these prefixes. Denoting by $l_k$ the $k$-th letter of the word (♣) we have the following solutions:

(1) $x = y_{r_j,k-2}$, $x' = u_{l_{k-1}^{-1},l_{k+1}^{-1}}$ where $u_{l_{k-1}^{-1},l_{k+1}^{-1}}$ is the commutator symbol of the letters $l_{k}^{-1}$ and $l_{k+1}^{-1}$.

(2) $x = y_{r_j,k-1}$, $x' = l_{k}^{-1}$.

(3) $x = y_{r_j,k+1}$, $x' = l_{k+1}^{-1}$.

(4) $x = y_{r_j,k+2}$, $x' = u_{l_{k+1}^{-1},l_{k-1}^{-1}}$ where $u_{l_{k+1}^{-1},l_{k-1}^{-1}}$ is the commutator symbol of the letters $l_{k+1}^{-1}$ and $l_{k-1}^{-1}$.

The case $k = 14$ and $x = y_{r_j,12}$, $x' = u_{c,t_{r_j}}$ reduces to the sufficiently generic word given in Case 4. All other resulting words are trivial in $G'$ as they involve the “noncommutative block” $w_r x_a x_b x_c$ in the right order on both sides and the $t$’s cancel.

**Case 6:** Suppose $x''''' = y_{r_j,35}$. There are also solutions of the same shape as in the previous case, namely $x = y_{r_j,33}$, $x' = u_{b,t_{r_j}}$, $x = y_{r_j,34}$, $x' = t_b$, and $x = y_{r_j,36}$, $x' = b_{r_j}$ which all yield trivial words in $G'$. Furthermore, there is also the solution $x = u_{r_j,t_{r_j}}$, $x' = u_{c,t_{r_j}}$ which after reordering some $t$’s yields the word

$$w_r t_{r_j}^2 t_c y_{r_j,35}^{-1} w_r^{-1} y_{r_j,36}^{-1} u_{t_c,t_{r_j}}.$$

This word is trivial in $G'$ as there is the relation $w_r^{-1} y_{r_j,36} u_{t_c,t_{r_j}} = e$ in this group.

**Case 7:** Suppose $x'''''' = y_{r_j,36}$. There are the solutions $x = y_{r_j,34}$, $x' = u_{b,t_{r_j}}$ and $x = y_{r_j,35}$, $x' = t_b$ which also yield trivial words as above. Furthermore, there are the solution $x = w_r$, $x' = u_{c,t_{r_j}}$, $x = y_{r_j,t_c}$, $x' = t_{r_j}$, and $x = u_{r_j,t_c}$, $x' = t_c$ which yield the same trivial word as in Equation (2) after reordering the $t$’s.
The only remaining cases left to check are the ones where \( x = y_{r_j,k} \) for some \( 1 \leq k \leq 36 \) and \( x'' \) is a generator of Table 2. As the \( b_{r_j} \)-coefficient of the generator \( x \) can be at most one and the generators \( x, x', x'' \) satisfy Equation (\( \pi_{F,2}^{ab} \)) there are only the following cases to consider.

**Case 8:** Suppose \( x = y_{r_j,1} \). The only solution is \( x' = w_{r_j}^{-1} \) and \( x'' = x_n \). This yields once a trivial word and once the word \( w_{r_j}x_{a}w_{r_j}^{-1}x_{a}^{-1} \). This word is sufficiently generic by Lemma 6.2.

**Case 9:** Suppose \( x = y_{r_j,2} \). The only solution is \( x' = w_{r_j}^{-1} \) and \( x'' = u_{a,lr_j} \). As the \( i \)'s commute and cancel we obtain the same words as in the previous case.

**Case 10:** Suppose \( x = y_{r_j,36} \). The only solution is \( x' = w_{r_j}^{-1} \) and \( x'' = u_{e,lr_j} \). Both words are trivial due to the relation \( w_{r_j}^{-1}y_{r_j,36}u_{e,lr_j} = e \) in the group \( G' \).

Thus, condition (PS4) holds for all generators \( x, x', x'' \in S' \) which completes the proof. \( \square \)

7. **Entropic matroid representability is undecidable**

We have now all necessary tools at our disposal to complete the proof that there is no algorithm that checks whether a matroid is entropic. We prove this result by connecting the uniform word problem for finite groups with the entropic representations of the associated generalized Dowling geometries. The first part of this relation is described in the following theorem.

**Theorem 7.1.** Let \( \langle S \mid R \rangle, s \in S \) be an instance of the uniform word problem for finite groups. Furthermore let \( \langle S'' \mid R'' \rangle \) be the augmented presentation from Construction 6.7 and \( \mathcal{M} \) the set of generalized Dowling geometries subordinate to this presentation. If there exists a finite quotient of \( G_{S,R} \) with \( s \neq e \) then some matroid in \( \mathcal{M} \) is entropic.

**Proof.** Assume there is a group homomorphism \( \varphi : G_{S,R} \to G \) for some finite group \( G \) with \( \varphi(s) \neq e \). Set \( n := |G| \) and identify the elements of \( G \) with \( \{1, \ldots, n\} \). Let \( \rho : \varphi : G_{S,R} \to GL_n(\mathbb{C}) \) the representation where each \( \rho(g) \) is the permutation matrix corresponding to the action of \( g \) by left-multiplication on \( G \).

By assumption we have \( \rho(s) \neq \rho(e) \). Therefore we can apply Proposition 6.10 and obtain a representation \( \tilde{\rho} : G_{S'',R''} \to GL_n(\mathbb{F}) \) for some \( n \in \mathbb{N} \) and some field \( \mathbb{F} \supseteq \mathbb{C} \) such that

(a) \( \tilde{\rho}(s) - \tilde{\rho}(s') \) is invertible for any distinct \( s, s' \in S'' \) and

(b) whenever \( s, s', s'' \in S'' \) (not necessarily distinct) satisfy \( \tilde{\rho}(s'')^{-1} \neq \tilde{\rho}(s's) \) then the matrix \( \tilde{\rho}(s'')^{-1} - \tilde{\rho}(s's) \in \text{End}(W) \) is invertible.

Hence by Theorem 5.4 some of the generalized Dowling geometries \( \mathcal{M} \) subordinate to \( \langle S \mid R \rangle \) is multilinear over \( \mathbb{F} \). Thus by [Mat99] some matroid in \( \mathcal{M} \) is entropic. \( \square \)

The next theorem describes the converse implication.

**Theorem 7.2.** Let \( \langle S \mid R \rangle, s \in S \) be an instance of the uniform word problem for finite groups and \( M \) be the generalized Dowling geometry of the presentation \( \langle S'' \mid R'' \rangle \) obtained from Construction 6.7. Assume that some matroid of the generalized Dowling geometries \( \mathcal{M} \) subordinate to \( \langle S'' \mid R'' \rangle \) is entropic. Then there exists a group homomorphism \( \varphi : G_{S,R} \to G \) to a finite group \( G \) with \( \varphi(s) \neq e \).

**Proof.** Say the matroid \( M \in \mathcal{M} \) is entropic. This is the generalized Dowling geometry of a quotient of \( G_{S'',R''} \). Composing the quotient map with the group homomorphism stemming from Theorem 4.5 applied to the entropic matroid \( M \) we obtain an \( n \in \mathbb{N} \) and a group homomorphism \( \rho : G_{S'',R''} \to S_n \) with \( \rho(x) \neq \rho(x') \) for distinct \( x, x' \in S'' \). Recall from Construction 6.7 that there is an isomorphism

\[ \nu : (G_{S,R} \ast F_R \ast \langle z_1, \ldots, z_k \rangle) \times \mathbb{Z}^N \to G_{S'',R''} \]
such that \( \nu(z_1) = s_z \) for some generator \( s_z \in S'' \) and \( \nu(sz_1s) = t \) with \( t \in S'' \).

As \( \nu \) is an isomorphism the generators \( s_z \) and \( t \) must be distinct. Hence we obtain \( \rho(t) \neq \rho(s_z) \). Composing these maps therefore yields \( \rho \circ \nu(sz_1s) \neq \rho \circ \nu(z_1) \). Thus \( \rho \circ \nu(s) \neq \rho \circ \nu(e) \). Restricting \( \rho \circ \nu \) to \( G_{S,R} \leq (G \ast F_R \ast \langle z_1, \ldots, z_4 \rangle) \times \mathbb{Z}^N \) therefore yields the desired map from \( G_{S,R} \) to the finite group \( S_n \) with \( \rho \circ \nu(s) \neq \rho \circ \nu(e) \).

Combining the last two theorems with Slobodskoi’s undecidability of the uniform word problem for finite groups immediately yields:

**Theorem 7.3.** There is no algorithm that can decide if a matroid \( M \) is entropic. Equivalently, there is no algorithm to check if \( M \) has a probability space representation.

**Proof.** The Theorems 7.1 and 7.2 imply that solving an instance of the uniform word for finite groups is equivalent to checking whether at least one member in finite set of matroids is entropic. The conclusion therefore follows from Slobodskoi’s theorem that the uniform word problem for finite groups is undecidable (Theorem 2.10).

### 8. Conditional Independence Implication Problem

We fix some finite ground set \( E \) for the entire section.

**Lemma 8.1.** A family of discrete random variables \( \{X_e\}_{e \in E} \) realizes the CI statement \((i \perp i \mid J)\) with \( i \in E \) and \( J \subseteq E \setminus \{i\} \) if and only if \( X_i \) is determined by \( \{X_j\}_{j \in J} \).

**Proof.** The random variables \( \{X_e\}_{e \in E} \) realize a CI statement \((A \perp B \mid C)\) for \( A, B, C \subseteq E \) if and only if

\[
H(X_A \mid X_C) + H(X_B \mid X_C) - H(X_{A\cup B} \mid X_C) = 0,
\]

where \( H(X_S \mid X_T) \) is the entropy of \( X_S \) conditioned on \( X_T \) for any \( S, T \subseteq E \). Applying this to the CI statement \((i \perp i \mid J)\) implies that \( H(X_i \mid X_J) = 0 \) which is the case if and only if \( X_i \) is determined by \( \{X_j\}_{j \in J} \).

We relate probability space representations of matroids to the following variant of the conditional independence implication (CII) problem.

**Problem 8.2.** The conditional independence realization (CIR) problem asks:

**Instance:** A set \( C \) of CI statements on a finite ground set \( E \).

**Question:** Does there exist a nontrivial family of discrete random variables \( \{X_e\}_{e \in E} \) realizing all CI statements in \( C \)? By nontrivial we mean that there is at least one random variable that is not constant (i.e., at least one random variable does not take a single value with probability 1).

**Theorem 8.3.** Let \( M \) be a connected matroid on the ground set \( E \). There exists a set of CI statements \( C_M \) on the ground set \( E \) such that \( M \) has a discrete probability space representation if and only if \( C_M \) can be realized by a nontrivial family of discrete random variables.

**Proof.** Given a connected matroid \( M \) we construct a set of CI statements \( C_M \):

(a) For every independent set \( A \subseteq E \) in \( M \) we add the CI statements \((i \perp A \setminus \{i\} \mid \emptyset)\) for all \( i \in A \) to \( C_M \).

(b) For every circuit \( C \subseteq E \) in \( M \) we add the CI statements \((i \perp i \mid C \setminus \{i\})\) for all \( i \in C \) to \( C_M \).

Let \( \{X_e\}_{e \in E} \) be a set of discrete random variables. Suppose \( A = \{a_1, \ldots, a_k\} \subseteq E \) is an independent subset of \( M \). The random variables \( \{X_e\}_{e \in A} \) are independent if and only if they realize the CI statements \((a_{i+1} \perp \{a_1, \ldots, a_i\} \mid \emptyset)\) for all \( 1 \leq i \leq k - 1 \). By construction, \( C_M \) contains all these CI statements, because a subset of an independent set
of $M$ is independent. Therefore if $\{X_e\}_{e \in E}$ satisfy $C_M$ then $\{X_a\}_{a \in A}$ are independent for every independent set $A$ of $M$.

Conversely, it is clear that if the variables $\{X_e\}_{e \in E}$ give a probability space representation of $M$, they satisfy every CI statement in $C_M$ constructed in (a).

Let $C \subseteq E$ be a circuit of $M$. Lemma 8.1 yields that the random variables $\{X_e\}_{e \in C \setminus \{i\}}$ determine $X_i$ for all $i \in C$ if and only if the random variables realize the CI statements corresponding to this circuit. Thus, for the family $\{X_e\}_{e \in E}$ it is equivalent to realize all CI statements corresponding to circuits of the matroid and to fulfill all determination properties dictated by the matroid in Definition 4.2.

Finally, the probability space representation being nontrivial implies that the random variable corresponding to an element that is not a loop is not constant with probability 1. Hence, if $\{X_e\}_{e \in E}$ are random variables corresponding to a probability space representation of $M$ then they are a nontrivial realization of $\mathcal{C}_M$.

Conversely, assume that $\{X_e\}_{e \in E}$ is a nontrivial family of random variables realizing $C_M$, so that there exists $e \in E$ such that $X_e$ is a nontrivial random variable. We show that this implies the nontriviality condition of a probability space representation in Definition 4.2: Let $f \in E$ be any element that is not a loop in the matroid $M$. Since the matroid is connected, there exists a circuit $C$ of $M$ with $\{e, f\} \subseteq C$. By the above arguments we know that the family $\{X_e\}_{e \in E}$ satisfies the independence and determination assumptions. In particular, the subfamily $\{X_g\}_{g \in C \setminus \{e\}}$ is independent and determines $X_e$. Thus, the subfamily $\{X_g\}_{g \in C \setminus \{e, f\}}$ does not determine $X_e$ which implies that $X_f$ must be nontrivial too. □

**Corollary 8.4.** The conditional independence realization (CIR) problem is algorithmically undecidable.

**Proof.** This follows directly form the Theorems 7.3 and 8.3 since the generalized Dowling geometries are connected matroids. □

Now we are finally ready to prove that the conditional independence implication problem is undecidable.

**Theorem 8.5.** The conditional independence implication (CII) problem is algorithmically undecidable.

**Proof.** Assume there is an oracle to decide the CII problem. We will show that using this oracle one can also decide the CIR problem. By Corollary 8.4 this then also shows that the CII problem is algorithmically undecidable.

Let $\mathcal{C}$ be a CIR problem instance and denote by $A_E$ the set of all CI statements on the ground set $E$. We claim that $\mathcal{C}$ has a nontrivial realization, that is the associated CIR problem has a positive solution, if and only if at least one of the following finite set of CII problem instances has a negative answer:

\[
\left\{ \bigwedge_{A \in \mathcal{C}} A \Rightarrow c \mid c \in A_E \setminus \mathcal{C} \right\}.
\]

Suppose the family $\{X_e\}_{e \in E}$ is nontrivial and realizes $\mathcal{C}$. Since the family is nontrivial there is some $c \in A_E$ that is not realized by this family: $(e \perp e|\emptyset)$ is not realized whenever $X_e$ is not constant. Hence, the CII problem instance $\bigwedge_{A \in \mathcal{C}} A \Rightarrow c$ that appears in (3) has a negative answer.

Conversely, assume that $\bigwedge_{A \in \mathcal{C}} A \Rightarrow c$ for some $c \in A_E \setminus A$ has a negative answer. Hence, there exists a family $\{X_e\}_{e \in E}$ of discrete random variables that realize $\mathcal{C}$ but not $c$. Thus, they also realize $\mathcal{C}$. Since $\{X_e\}_{e \in E}$ does not realize $c$ the family is nontrivial and therefore the CIR problem has a positive answer. □
9. Almost Multilinear Matroids

Next we generalize Definitions 5.1 and 5.2 to the approximate setting. We use the notation for collection of linear maps introduced in Section 5.1.

**Definition 9.1.** Let $V$ be a vector space, $c \in \mathbb{N}$ and $E$ be a finite set. Further, let $\{W_e\}_{e \in E}$ be a collection of vector spaces with $\dim W_e = c$ and let $\{T_e : V \to W_e\}_{e \in E}$ be a collection of surjective linear maps. Fix some $\varepsilon > 0$.

(a) The maps $\{T_e\}_{e \in E}$ are independent with error $\varepsilon$ if $\rk(T_E) \geq c(|E| - \varepsilon)$.

(b) Fix $x \in E$. The map $T_x$ is determined with error $\varepsilon$ by $\{T_e\}_{e \in E \setminus \{x\}}$ if there exists a linear map $S : W_{E \setminus \{x\}} \to W_x$ such that

$$\rk(T_x - S \circ T_{E \setminus \{x\}}) \leq c\varepsilon.$$

That is, the normalized rank distance of $T_x$ and $S \circ T_{E \setminus \{x\}}$ is at most $\varepsilon$. In this case, $S$ is called an $\varepsilon$-determination map.

For the sake of brevity we sometimes write that a set of maps is $\varepsilon$-independent, or that some map is $\varepsilon$-determined by a given collection of maps.

**Lemma 9.2.** Let $A \in M_c(\mathbb{F})$ be a matrix over a field $\mathbb{F}$ and let $\delta \geq 0$ be a real number. Then $\rk(A) \geq c(1 - \delta)$ if and only if there exists an invertible matrix $D \in M_c(\mathbb{F})$ such that $\rk(I_c - DA) \leq c\delta$.

**Proof.** Suppose $\rk(A) \geq c(1 - \delta)$. Then there exists an invertible matrix $A'$ such that $A' - A$ has at most $c\delta$ nonzero rows: To construct such an $A'$ from the given matrix $A$, iteratively find a row of the matrix which is in the span of the others, and replace it by a row which is not in the row span. After $c - \rk(A)$ row replacements we obtain an invertible matrix and the process ends.

For $D = A'^{-1}$, we have

$$\rk(I_c - DA) = \rk(DA' - DA) = \rk(A' - A) \leq c\delta.$$

Conversely, suppose there exists a matrix $D$ with $\rk(I_c - DA) \leq c\delta$. By the triangle inequality $\rk(I_c) \leq \rk(I_c - DA) + \rk(DA)$, and hence $\rk(DA) \geq c(1 - \delta)$, which implies the claim. \qed

The following corollary is obvious from the lemma.

**Corollary 9.3.** Let $T : V \to W$ be a linear transformation between vector spaces of the same (finite) dimension $c$ and let $\delta \geq 0$. Then $\rk(T) \geq c(1 - \delta)$ if and only if there exists an invertible transformation $S : W \to V$ such that $\rk(\id_V - S \circ T) \leq c\delta$.

**Definition 9.4.** Let $M$ be a matroid on $E$. An $\varepsilon$-approximate vector space representation of $M$ consists of $c \in \mathbb{N}$, a vector space $V$ and a collection of surjective linear maps $\{T_e : V \to W_e\}_{e \in E}$ with $\dim W_e = c$ such that

(a) If $A \subseteq E$ is independent, the maps $\{T_e\}_{e \in A}$ are independent with error $\varepsilon$.

(b) If $C \subseteq E$ is a circuit and $e \in C$, then $T_e$ is determined with error $\varepsilon$ by $\{T_f\}_{f \in C \setminus \{e\}}$.

**Theorem 9.5.** A simple matroid $M$ is multilinear if and only if it has a vector space representation. It is almost-multilinear if and only if it has an $\varepsilon$-approximate vector space representation for every $\varepsilon > 0$.

The proof consists of simple but slightly lengthy calculations, and is given in Appendix B.

**Theorem 9.6.** Let $G = \langle S \mid R \rangle$ be a symmetric triangular presentation of a sofic group and assume that:

(a) $s \neq s'$ in $G$ for all distinct $s, s' \in S$, and
(b) For all \( s, s', s'' \in S \) (not necessarily distinct) if \( s''s's = e \) holds in \( G \) then it is a relation in \( R \).

Then the generalized Dowling geometry of \( \langle S \mid R \rangle \) is almost multilinear over every field.

**Corollary 9.7.** Let \( \langle S \mid R \rangle \) be a symmetric triangular presentation of a sofic group \( G \) that satisfies the following condition: \( s \neq s' \) in \( G \) for every pair of distinct elements \( s, s' \in S \). Then one of the generalized Dowling geometries subordinate to \( \langle S \mid R \rangle \) is almost multilinear.

**Proof.** Add to \( \langle S \mid R \rangle \) the collection of all three-generator relations that hold in \( G \). The generalized Dowling geometry of the resulting presentation is subordinate to \( \langle S \mid R \rangle \), and satisfies conditions (a) and (b) of the theorem above. \( \boxed{} \)

**Proof of the theorem.** Fix some \( \varepsilon > 0 \) and a field \( \mathbb{F} \). Define \( F := \{ a \in G \mid a = ss's'' \text{ for } s, s', s'' \in S \} \subseteq G \). By Definition 2.11 there exists an \( n \in \mathbb{N} \) and a map \( \theta : F \rightarrow S_n \) such that:

(a) If \( g, h, gh \in F \) then \( d_{\text{hamm}}(\theta(g)\theta(h), \theta(gh)) < \varepsilon/18 \),

(b) If the neutral element \( e \in F \) then \( d_{\text{hamm}}(\theta(e), \text{id}) < \varepsilon/18 \), and

(c) For all distinct \( x, y \in F \), \( d_{\text{hamm}}(\theta(x), \theta(y)) \geq 1 - \varepsilon/18 \).

Define

\[
\rho_\theta : G \rightarrow \text{GL}_n(\mathbb{F}) \quad \rho_\theta(s) = M_{\theta(s)}
\]

where \( M_{\theta(s)} \) is the permutation matrix of \( \theta(s) \in S_n \). Then \( \rho_\theta \) satisfies the assumptions of Theorem 9.8, and therefore the generalized Dowling geometry of \( \langle S \mid R \rangle \) is almost multilinear. \( \boxed{} \)

**Theorem 9.8.** Let \( G = \langle S \mid R \rangle \) be a group with a given symmetric triangular presentation and fix \( \varepsilon \geq 0 \). Let \( \rho : S \rightarrow \text{GL}(W) \) be a function, where \( W \) is a finite dimensional vector space over a field \( \mathbb{F} \). Suppose that

(a) \( d_{\text{rk}}(\rho(s), \rho(s')) \geq 1 - \varepsilon/18 \) for all distinct \( s, s' \in S \),

(b) If \( s, s', s'' \in S \) (not necessarily distinct) satisfy \( s''s's \neq e \) then

\[
d_{\text{rk}}(\rho(s''), \rho(s') \rho(s), \text{id}_W) \geq 1 - \varepsilon/18.
\]

(c) If \( s, s', s'' \in S \) (not necessarily distinct) satisfy \( s''s's = e \) then

\[
d_{\text{rk}}(\rho(s''), \rho(s') \rho(s), \text{id}_W) \leq \varepsilon/18.
\]

Further, \( d_{\text{rk}}(\rho(e), \text{id}_W) \leq \varepsilon/18 \).

(d) For all \( s, s', s'' \in S \) (not necessarily distinct) if \( s''s's = e \) holds in \( G \) then it is a relation in \( R \).

Then the generalized Dowling geometry corresponding to the presentation \( \langle S \mid R \rangle \) has an \( \varepsilon \)-approximate vector space representation.

**Proof.** As in Definition 3.7, we denote the generalized Dowling geometry of \( \langle S \mid R \rangle \) by \( M \), the ground set by \( E \), and the special basis by \( B = \{ b_1, b_2, b_3 \} \). We construct an \( \varepsilon \)-approximate vector space representation of \( M \).

Set \( e = \dim W \) and for each \( e \in E \) set \( W_e = W \). Let \( V = W_{b_1} \oplus W_{b_2} \oplus W_{b_3} \), and let \( T_{b_i} : V \rightarrow W_{b_i} \) be given by the projection. Let \( i, j \in \{ 1, 2, 3 \} \) be two distinct indices, and suppose \( j \) is the element following \( i \) in the cyclic ordering. Let \( s \in S \) be any element. Define

\[
T_{s_i} : V = W_{b_1} \oplus W_{b_1} \oplus W_{b_3} \rightarrow W_{s_i} \\
T_{s_i}(v_1, v_2, v_3) = v_j - \rho(s)(v_i),
\]
or in other words $T_{s_i} = T_{b_j} - \rho(s)T_{b_j}$.

(One can come up with this guess for the maps by starting with the following determination map for $v_j$ given $v_{s_i} = T_{s_i}(v_1, v_2, v_3)$ and $v_i: S(v_i, v_{s_i}) = \rho(s_i)v_i + v_{s_i}$. Such determination maps “compose correctly” in the sense of Theorem 4.6, condition (b). Another way is to inspect the matrix representations of Dowling geometries.) In order to prove the required $\varepsilon$-independence and $\varepsilon$-determination conditions we first establish the following claims.

**Claim 1:** $d_{rk}(\rho(s)^{-1}, \rho(s^{-1})) \leq \varepsilon/9$.

**Claim 2:** Fix $\varepsilon' \geq 0$. Let $S \subseteq E$ with $|S| = 3$. If $T_b$ is determined by $\{T_e\}_{e \in S}$ with error $\varepsilon'$ for all $1 \leq i \leq 3$ then $\{T_e\}_{e \in S}$ is independent with error $\varepsilon'$.

**Claim 3:** Let $S \subseteq E$ with $|S| = 3$. If $\{T_e\}_{e \in S}$ is independent with error $\varepsilon'/3$ then $T_b$ is determined by $\{T_e\}_{e \in S}$ with error $\varepsilon'$ for all $1 \leq i \leq 3$.

**Proof of Claim 1.** Applying assumption (c) to the relation $s^{-1}s = e$, we obtain

$$d_{rk}(\rho(s^{-1})\rho(s), \text{id}_W) \leq 1/18.$$ 

Since $d_{rk}(\rho(e), \text{id}_W) \leq \varepsilon/18$, we have

$$d_{rk}(\rho(s^{-1})\rho(s), \text{id}_W) \leq d_{rk}(\rho(s^{-1})\rho(s) \circ \text{id}_W, \rho(s^{-1})\rho(s)\rho(e)) + d_{rk}(\rho(s^{-1})\rho(s), \text{id}_W) \leq \varepsilon/9.$$ 

by Remark 2.9 and the triangle inequality. \qed

**Proof of Claims 2 and 3.** Given a basis $S \subseteq E$ of $M$ (so that in particular $|S| = 3$) consider the map

$$T_S : V = W_{b_1} \oplus W_{b_2} \oplus W_{b_3} \to W_S = \bigoplus_{e \in S} W_e.$$ 

Suppose each $T_{b_i}$ is $(\varepsilon'/3)$-determined by $\{T_e\}_{e \in S}$ . Then there exist maps $\hat{T}_1$, $\hat{T}_2$, and $\hat{T}_3$ such that

$$\text{rk}(T_{b_i} - \hat{T}_i \circ T_S) \leq c\varepsilon'/3$$

for each $1 \leq i \leq 3$. Define

$$\hat{T} : W_S \to V = W_{b_1} \oplus W_{b_2} \oplus W_{b_3} \quad \text{with} \quad w = (w_e)_{e \in S} \mapsto (\hat{T}_1(w), \hat{T}_2(w), \hat{T}_3(w))$$

and observe that $T_P$ differs from $\hat{T} \circ T_S$ on a subspace of dimension at most $3 \cdot c\varepsilon'/3 = c\varepsilon'$. In particular $T_S$ has rank at least $\text{rk}(T_P) - c\varepsilon'$, and thus $\{T_e\}_{e \in S}$ are $\varepsilon'$-independent.

Suppose $\{T_e\}_{e \in S}$ are independent with error $\varepsilon'/3$. Then by definition $T_S$ has rank at least $c(1 - \varepsilon'/3)$. Thus by Corollary 9.3 there exists a map $\hat{T} : W_S \to V$ such that

$$\text{rk}(\text{id}_V - \hat{T} \circ T_S) \leq 3c(\varepsilon'/3) = c\varepsilon'.$$

Composing with $T_{b_i}$ for $1 \leq i \leq 3$, we find

$$\text{rk}(T_{b_i} - (T_{b_i} \circ \hat{T}) \circ T_S) \leq c\varepsilon',$$

so that each $T_{b_i}$ is determined by $\{T_e\}_{e \in S}$ with error $\varepsilon'$.

We now verify that the correct independence and determination conditions hold with error at most $\varepsilon$ for the maps $\{T_e : V \to W_e\}_{e \in E}$.

For the independence conditions there are several cases. It suffices to check the condition for bases of $M$ (recall these are all of size $3 = \text{rk}(M)$). In each case we will show that $\{T_e\}_{e \in S}$ $\varepsilon/3$-determines $T_{b_i}$ for all $1 \leq i \leq 3$, which suffices by Claim 2.

(a) For $\{b_1, b_2, b_3\}$ the statement is clear: $T_{b_i}$ ($i = 1, 2, 3$) are distinct projections onto summands of $V = W_{b_1} \oplus W_{b_2} \oplus W_{b_3}$.
(b) For subsets of the form \( \{b_1, b_2, s_2\} \), we have
\[
T_{s_2} + \rho(s)T_{b_2} = T_{b_1},
\]
so that \( T_{b_1} \) is determined (with error 0) by \( \{T_{b_1}, T_{b_2}, T_{s_2}\} \), and we reduce to the previous case. The same holds for subsets of the form \( \{b_1, b_2, s_3\} \), or similar subsets with cyclic shifts of the indices.

(c) Subsets of the form \( \{s_1, s_2, b_1\} \) (up to shifts of the indices, with \( s = s' \) allowed) are similar: we first observe that \( T_{b_1} \) is determined (with error 0) by \( \{T_{b_1}, T_{s_1}\} \) and then reduce to (b). The same idea works for subsets of the form \( \{s_1, s_2', b_2\} \).

(d) For subsets of the form \( \{s_1, s'_1\} \) we note that
\[
\rho(s)T_{b_1} + T_{s_1} = \rho(s')T_{b_1} + T_{s'_1} = T_{b_2}
\]
and therefore \( (\rho(s) - \rho(s'))T_{b_1} = T_{s'_1} - T_{s_1} \). By assumption we know that \( \text{rk}(\rho(s) - \rho(s')) \geq c(1 - \frac{\varepsilon}{18}) \). Thus by Corollary 9.3, there is a \( \tilde{T} \in \text{GL}(W) \) such that
\[
\text{rk}(\text{id}_W - \tilde{T} \circ (\rho(s) - \rho(s'))) \leq c\varepsilon/18.
\]
Precomposing with \( T_{b_1} \) and using the identity \( (\rho(s) - \rho(s'))T_{b_1} = T_{s'_1} - T_{s_1} \), we find
\[
\text{rk}(T_{b_1} - \tilde{T} \circ (T_{s'_1} - T_{s_1})) \leq c\varepsilon/18.
\]
Thus \( T_{b_1} \) is determined by \( \{T_{s'_1}, T_{s_1}\} \) with error \( \varepsilon/18 \).

Using \( \rho(s)T_{b_1} + T_{s_1} = T_{b_2} \) and composing the maps in the previous rank inequality with \( \rho(s) \), we find
\[
\text{rk}(T_{b_2} - [\rho(s)\tilde{T} \circ (T_{s'_1} - T_{s_1})] - T_{s_1})
\]
\[
= \text{rk}(\rho(s)T_{b_1} + T_{s_1} - [\rho(s)\tilde{T} \circ (T_{s'_1} - T_{s_1})] - T_{s_1})
\]
\[
= \text{rk}(\rho(s) \circ T_{b_1} - \rho(s)\tilde{T} \circ (T_{s'_1} - T_{s_1})) \leq c\varepsilon/18.
\]
Observe that \( \rho(s)\tilde{T} \circ (T_{s'_1} - T_{s_1}) - T_{s_1} \) is the composition of a map
\[
W_{s'_1} \oplus W_{s_1} \to W = W_{b_2}
\]
on \( T_{s'_1,s_1} \). Therefore \( T_{b_2} \) is determined with error \( \varepsilon/18 \) by \( T_{s'_1,s_1} \).

By claims 2 and 3, this computation yields the independence condition for subsets of the form \( S = \{s_1, s'_1, b_2\} \): by our computation, the maps \( \{T_e\}_{e \in S} \) determine \( T_{b_1} \) and \( T_{b_2} \) with error \( \varepsilon/18 \) each, so that \( T_B \) is determined with error at most \( \varepsilon/9 \) and the maps are \( \varepsilon/3 \)-independent.

It also yields the independence condition for subsets of the form \( S = \{s_1, s'_1, s''_2\} \) (up to shifts of the indices, with \( s, s', s'' \) not necessarily distinct), the maps \( \{T_e\}_{e \in S} \) determine each \( T_{b_1} \) with error \( \varepsilon/18 \).

(e) Finally, for subsets of the form \( \{s_1, s'_2, s''_3\} \) with \( s''s \neq e \), we have
\[
T_{s'_2} + \rho(s'')T_{s'_2} + \rho(s'')\rho(s')T_{s_1}
\]
\[
= [T_{b_1} - \rho(s'')T_{b_1}] + \rho(s'') [T_{b_2} - \rho(s')T_{b_2}] + \rho(s'')\rho(s') [T_{b_2} - \rho(s)T_{b_1}]
\]
\[
= T_{b_1} - \rho(s'')\rho(s') = [\text{id}_W - \rho(s'')\rho(s')\rho(s)] T_{b_1}
\]
By assumption (b), \( \text{rk}([\text{id}_W - \rho(s'')\rho(s')\rho(s)] \leq c(1 - \varepsilon/18) \). By Corollary 9.3 there exists a \( \tilde{T} \in \text{GL}(W) \) such that
\[
\text{rk}([\text{id}_W - \tilde{T} \circ \rho(s'')\rho(s')\rho(s)] \leq c\varepsilon/18.
\]
As in case (d), this implies that \( T_{b_1} \) is determined by \( \{T_e\}_{e \in S} \) with error \( \varepsilon/18 \) for each \( 1 \leq i \leq 3 \). By permuting the indices \( (1, 2, 3) \) and generators \( (s, s', s'') \) cyclically, we find similar expressions for \( T_{b_2} \) and \( T_{b_3} \). This shows each \( T_{b_i} \) is determined by \( \{T_{s_1}, T_{s'_2}, T_{s''_3}\} \) with error \( \varepsilon/18 \), which by claim 2 implies the claimed independence.
We now consider the circuits and show that the determination conditions are satisfied.

(a) If $C$ is a circuit of size 4, let $x \in C$. The subset $C \setminus \{x\}$ is a basis of $M$ (since this subset is independent and $M$ has rank 3), so $\{T_e\}_{e \in C \setminus \{x\}}$ determine $T_{b_1}, T_{b_2},$ and $T_{b_3}$ with error $\varepsilon/3$ by the above arguments.

By construction we can express $T_x$ by $T_x = \sum_{i=1}^3 A_i T_{b_i}$ for some maps $A_i \in GL(W)$. The above argument also implies that $\{T_e\}_{e \in C \setminus \{x\}}$ determines $A_i T_{b_i}$ with error $\varepsilon/3$ for all $1 \leq i \leq 3$. Therefore $\{T_e\}_{e \in C \setminus \{x\}}$ determines $T_x$ with error $\varepsilon$.

(b) If $C$ consists of 3 elements of the flat spanned by $\{b_1, b_2\}$ then any subset consisting of two elements is of the form $S = \{b_1, b_2\}$, $S = \{b_i, s_1\}$ (for $i \in \{1, 2\}$), or $S = \{s_1, s'_1\}$ (where $s \neq s'$ in $S$). In the first case it is clear that $\{T_e\}_{e \in S}$ determines $T_x$ (with error 0) for $x$ the unique element of $C \setminus S$.

For the latter two cases, note that in the cases (b) and (d) of the independence conditions it is shown that $\{T_e\}_{e \in S}$ determines $T_{b_1}$ and $T_{b_2}$ in either case with error $\varepsilon/18$. Therefore, $\{T_e\}_{e \in S}$ determines $T_{e'}$ with error $\varepsilon/18$ for any $e'$ in the flat spanned by $\{b_1, b_2\}$ by an analogous argument as in the previous case, and in particular for $x$ the unique element of $C \setminus S$.

(c) Suppose $C = \{s_1, s'_2, s'_3\}$ where $s''s = e$, or equivalently $s'' = (s's)^{-1} = s^{-1}s^{-1}$. We show that $T_{s''}$ is determined by $\{T_{s_1}, T_{s'_2}\}$ with error $\varepsilon$. To this end, we compute
\[
- \rho(s)^{-1}T_{s_1} - \rho(s)^{-1}\rho(s')^{-1}T_{s'_2} = - \rho(s)^{-1}\left[ T_{b_2} - \rho(s)T_{b_1} \right] - \rho(s)^{-1}\rho(s')^{-1}\left[ T_{b_3} - \rho(s')T_{b_2} \right] = T_{b_1} - \rho(s)^{-1}\rho(s')^{-1}T_{b_1}
\]
By assumption we have $\text{rk}(\rho(s')\rho(s')\rho(s) - \text{id}_W) \leq \varepsilon/18$. Composing the transformation with $\rho(s)^{-1}\rho(s')^{-1}$ from the right, we obtain
\[
\text{rk}(\rho(s'') - \rho(s)^{-1}\rho(s')^{-1}) \leq \varepsilon/18.
\]
Therefore
\[
\text{rk}(T_{s''} - [T_{b_1} - \rho(s)^{-1}\rho(s')^{-1}T_{b_1}]) \leq \varepsilon/18,
\]
which implies
\[
\text{rk}([-\rho(s)^{-1}T_{s_1} - \rho(s)^{-1}\rho(s')^{-1}T_{s'_2}] - T_{s''}) \leq \varepsilon/18,
\]
so the map $T_{s''}$ is determined by $\{T_{s_1}, T_{s'_2}\}$ as required. \qed

Theorem 9.9. Suppose the generalized Dowling geometry $M = (E, r)$ associated to a finitely presented group $G = \langle S \mid R \rangle$ is almost multilinear. Then $s \neq s'$ in $G$ for all distinct $s, s' \in S$.

Proof. We first apply Theorem C.10 to construct a representation of the Dowling groupoid $G$ associated to $G$. Recall that this is a finitely presented category with objects $\{b_1, b_2, b_3\}$ and with generating morphisms
\[
\{g_{s, i, j} : b_i \to b_j \mid s \in S, \text{ and } i, j \in \{1, 2, 3\} \text{ with } i \neq j\}.
\]
These objects and generating morphisms define a directed graph $H$.

For each $n \in \mathbb{N}$ let a $\frac{1}{18n}$-approximate vector space representation of $M$ be given by the vector space $V_n$ and the linear maps $\{T_{e,n} : V_n \to W_{e,n}\}_{e \in E}$. Suppose the spaces $\{W_{e,n}\}_{e \in E}$ all have dimension $c_n \in \mathbb{N}$, and define $D_n$ to be the category of vector spaces of dimension $c_n$ over the underlying field of $V_n$.

Fix $n \in \mathbb{N}$. We define a graph homomorphism $f_n : H \to \text{Graph}(D_n)$ as follows. On objects define $f_n$ by $f_n(b_i) = W_{b_i,n}$ for all $1 \leq i \leq 3$. To define $f_n$ on the morphisms,
suppose $1 \leq i, j \leq 3$ and $i$ precedes $j$ in the cyclic ordering. Given $s \in S$, choose $\frac{1}{18n}$-approximate determination maps

$$\varphi_{s,i,j} : W_{b_i,n} \oplus W_{s,i,n} \to W_{b_j,n} \text{ and } \varphi_{s,j,i} : W_{b_j,n} \oplus W_{s,i,n} \to W_{b_i,n}$$

for $T_{b_i,n}$ given $\{T_{b_i,n}, T_{s,i,n}\}$ and for $T_{b_j,n}$ given $\{T_{b_j,n}, T_{s,i,n}\}$, respectively. Then define $f_n (g_{s,i,j}) : W_{b_i,n} \to W_{b_j,n}$ by

$$(f_n (g_{s,i,j})) (w) = \varphi_{s,i,j} (w, 0)$$

and similarly define

$$(f_n (g_{s,j,i})) (w) = \varphi_{s,j,i} (w, 0).$$

It remains to show that for any relation $\varphi_1 = \varphi_2$ in the presentation of $G$ we have $d (f_n (\varphi_1), f_n (\varphi_2)) \leq \frac{1}{n}$ for each $n$.

Let $n \in \mathbb{N}$ be fixed for the rest of the proof. For convenience, we denote $c = c_n$ and similarly omit $n$ from the notation for the spaces $V_n$ and $\{W_{b,n}\}_{b \in E}$ and the maps $\{T_{b,n}\}_{b \in E}$.

**Case 1:** For $i, j$, and $s$ as above consider the relation $g_{s,j,i} \circ g_{s,i,j} = \text{id}_{b_i}$. Since $T_{b_i,s_i}$ is $1/18n$-independent, its image intersects the subspace $W_{b_i} \oplus \{0\} \subset W_{b_i} \oplus W_{s_i}$ in a subspace of dimension at least $c (1 - 1/18n)$. In the same way, the image of $T_{b_j,s_i}$ intersects $W_{b_j} \oplus \{0\}$ in a subspace of dimension at least $c (1 - 1/18n)$. Define

$$V' = T_{s_i}^{-1} (0).$$

The previous considerations imply precisely that $T_{b_i,s_i} (V') \simeq T_{b_i} (V')$ and $T_{b_j,s_i} (V') \simeq T_{b_j} (V')$ have dimension at least $c (1 - 1/18n)$. It is clear that

$$\text{rk} (T_{b_j} | V' - \varphi_{s,i,j} \circ T_{b_i,s_i} | V') \leq \text{rk} (T_{b_j} - \varphi_{s,i,j} \circ T_{b_i,s_i}) \leq c/18n$$

(the inequality on the right is from the definition of $\varphi_{s,i,j}$ as a determination map). In the same way,

$$\text{rk} (T_{b_i} | V' - \varphi_{s,j,i} \circ T_{b_j,s_i} | V') \leq c/18n.$$

Therefore

$$V'' = \left[ \ker (T_{b_i} | V' - \varphi_{s,i,j} \circ T_{b_j,s_i} | V') \right] \cap \ker (T_{b_j} | V' - \varphi_{s,i,j} \circ T_{b_i,s_i})$$

is a subspace of $V'$ of dimension at least $\dim V' - c/9n$. Its image under $T_{b_i}$ therefore has codimension at most $c/9n$ within the image of $V'$, and similarly for $T_{b_j}$. That is,

$$\dim T_{b_i} (V'') \geq c_n \left( 1 - 1/6n \right) \quad \text{and} \quad \dim T_{b_j} (V'') \geq c_n \left( 1 - 1/6n \right).$$

By definition, if $w \in T_{b_i} (V'')$ then $w = T_{b_i} (v)$ for some $v \in V''$ and

$$(f_n (g_{s,i,j})) (w) = \varphi_{s,i,j} (w, 0) = \varphi_{s,i,j} (T_{b_i,s_i} (v)) = T_{b_j} (v)$$

where the rightmost equality is because $v \in V''$ is contained in the kernel of $T_{b_i} - \varphi_{s,i,j} \circ T_{b_i,s_i}$. In the same way, if $w \in T_{b_j} (V'')$ then $w = T_{b_j} (v)$ for some $v \in V''$ and

$$(f_n (g_{s,j,i})) (w) = T_{b_i} (v).$$

It follows that

$$f_n (g_{s,j,i}) \circ f_n (g_{s,i,j}) |_{T_{b_i} (V'')} = \text{id}_{T_{b_i} (V'')} ,$$

and the normalized rank distance between $f_n (g_{s,i,j}) \circ f_n (g_{s,j,i})$ and $\text{id}_{W_{b_i}}$ is at most

$$\frac{1}{c} (\dim W_{b_i} - \dim T_{b_i} (V'')) \leq \frac{1}{6n}.$$

**Case 2:** Suppose $(i, j, k)$ is an even permutation of $(1, 2, 3)$ (so that $i < j < k < i$ in the cyclic ordering) and let $s, s', s'' \in S$ such that $s''s' s = e$ is a relation in $R$. We verify
that
\[ f_n(g_{s', k, i}) \circ f_n(g_{s', j, k}) \circ f_n(g_{s, i,j}) \]
has small normalized rank distance from \( \text{id}_{W_{b_i}} \). Define
\[ V' = T_{s_i}^{-1}(0) \cap T_{s_j'}^{-1}(0) \cap T_{s_k''}^{-1}(0) = T_{(s_i, s_j', s_k'')}^{-1}(0). \]

By \( 1/18n \)-determination of \( T_{s_k''} \) by \( \{ T_{s_i}, T_{s_j'} \} \), the map \( T_{(s_i, s_j', s_k'')} \) has rank at most \( c(2 + 1/18n) \). Therefore \( V' \) is a subspace of \( V \) with dimension at least
\[ \dim V - \text{rk} \left( T_{(s_i, s_j', s_k'')} \right) \geq \dim V - c(2 + 1/18n). \]

We have
\[ \text{rk} \left( T_{b_j} \mid V' - \varphi_{s, i,j} \circ T_{(b_i, s_i)} \mid V' \right) \leq \text{rk} \left( T_{b_j} - \varphi_{s, i,j} \circ T_{(b_i, s_i)} \right) \leq c/18n, \]
and in the same way also
\[ \text{rk} \left( T_{b_i} \mid V' - \varphi_{s', j,k} \circ T_{(b_j, s_j')} \mid V' \right) \leq c/18n \]
and
\[ \text{rk} \left( T_{b_k} \mid V' - \varphi_{s', k,i} \circ T_{(b_i, s_i)} \mid V' \right) \leq c/18n. \]

Define
\[ V'' = \ker \left( T_{b_j} \mid V' - \varphi_{s, i,j} \circ T_{(b_i, s_i)} \mid V' \right) \cap \]
\[ \ker \left( T_{b_k} \mid V' - \varphi_{s', j,k} \circ T_{(b_j, s_j')} \mid V' \right) \cap \]
\[ \ker \left( T_{b_i} \mid V' - \varphi_{s', k,i} \circ T_{(b_i, s_i)} \mid V' \right). \]

Then \( V'' \) has codimension at most \( c/6n \) within \( V' \).

We now compute \( \dim T_{b_i}(V'') \): observe that \( V'' \subseteq V' \subseteq T_{s_i}^{-1}(0) \cap T_{s_j'}^{-1}(0) \). Since \( \{ T_{s_i}, T_{s_j'} \} \) determine \( T_{s_k''} \) with error at most \( 1/18n \), the codimension of \( V' \) within \( T_{s_i}^{-1}(0) \cap T_{s_j'}^{-1}(0) \) is at most \( c/18n \). Thus the codimension of \( V'' \) within \( T_{s_i}^{-1}(0) \cap T_{s_j'}^{-1}(0) \) is at most \( c \left( \frac{1}{18} + \frac{1}{6} \right) n = \frac{4c}{18n} \). Since \( \{ T_{b_i}, T_{s_i}, T_{s_j'} \} \) are \( 1/18n \)-independent, the image of \( T_{(b_i, s_i, s_j')} \) intersects \( W_{b_i} \oplus \{ 0 \} \oplus \{ 0 \} \subseteq W_{b_i} \oplus W_{s_i} \oplus W_{s_j'} \)
in a subspace of codimension at most \( c/18n \). This intersection is isomorphic to \( T_{b_i} \left( T_{s_i}^{-1}(0) \cap T_{s_j'}^{-1}(0) \right) \), which thus has codimension at most \( c/18n \) in \( W_{b_i} \). It follows that \( T_{b_i}(V'') \) has codimension at most \( \frac{4c}{18n} + \frac{c}{18n} = \frac{5c}{18n} \) within \( W_{b_i} \).

Fix \( v \in V'' \). Then \( v \in \ker \left( T_{b_j} - \varphi_{s, i,j} \circ T_{(b_i, s_i)} \right) \), and
\[ (f_n (g_{s, i,j}) (T_{b_j} (v))) = \varphi_{s, i,j} (T_{b_j} (v), 0) = \varphi_{s, i,j} (T_{(b_i, s_i)} (v)) = T_{b_j} (v). \]

In the same way we have
\[ (f_n (g_{s', j,k}) (T_{b_j} (v))) = T_{b_k} (v) \quad \text{and} \quad (f_n (g_{s', k,i}) (T_{b_k} (v))) = T_{b_i} (v). \]

It follows that
\[ f_n (g_{s', j,k}) \circ f_n (g_{s', j,k}) \circ f_n (g_{s, i,j}) \mid T_{b_j}(V'') = \text{id}_{T_{b_j}(V''}, \]
so the normalized rank distance between \( f_n (g_{s', j,k}) \circ f_n (g_{s', j,k}) \circ f_n (g_{s, i,j}) \) and \( \text{id}_{W_{b_i}} \) is at most
\[ \frac{1}{c} \left[ c - \dim T_{b_i}(V'') \right] \leq 1/n. \]

This shows that there exists a representation of the Dowling groupoid of \( M \) in some metrics ultraproduct of vector spaces. Let \( s, s' \in S \) be distinct generators, and observe that
\{T_{n,s_1}, T_{n,s_1}'\} \text{ are } 1/18n\text{-independent for every } n \in \mathbb{N}. \text{ It follows that the sequences } (T_{n,s_1})_{n \in \mathbb{N}} \text{ and } (T_{n,s_1}')_{n \in \mathbb{N}} \text{ are not identified in the metric ultraproduct. By Lemma 3.4 and Lemma 3.5 we see that there is a representation of } G \text{ (considered as a groupoid with one object) in some category such that } s \text{ and } s' \text{ are represented by distinct morphisms; in particular } s \neq s' \text{ in } G. \qedhere

9.1. Almost-multilinear matroid representability is undecidable. Here we use the theorems proved in the beginning of this section to prove the following theorem.

**Theorem 9.10.** The following problem is algorithmically undecidable: given a matroid \( M \), decide whether it is almost multilinear.

We prove the theorem using the next trivial lemma.

**Lemma 9.11.** Let \( \langle S \mid R \rangle \) be a finite presentation of a group and let \( \sim \) be an equivalence relation on \( S \). Denote by \( \langle S/ \sim \mid R/ \sim \rangle \) the group presentation which is obtained from \( \langle S \mid R \rangle \) by replacing \( S \) with \( S/ \sim \), and replacing each letter in each relation in \( R \) by its equivalence class in \( S/ \sim \).

If \( \langle S \mid R \rangle \) is symmetric and triangular then so is \( \langle S/ \sim \mid R/ \sim \rangle \). There is a group homomorphism

\[
\langle S \mid R \rangle \to \langle S/ \sim \mid R/ \sim \rangle
\]

that maps each \( s \in S \) to its equivalence class \( [s]_\sim \).

**Proof of Theorem 9.10.** We construct a reduction from the word problem for a finitely presented sofic group to the almost-multilinear matroid representability problem. Undecidability follows by Theorem 2.12.

Let \( G = \langle S \mid R \rangle \) be a finitely presented sofic group and let \( w \) be a word in the generators \( S \). It is easy to compute a symmetric triangular presentation of \( G \) such that \( w \) is a generator; abusing notation slightly, we denote this presentation by \( \langle S \mid R \rangle \).

Let \( \{\sim_i\}_{i=1}^N \) be the set of all equivalence relations on \( S \) satisfying that \( w \in S \) is not equivalent to \( e \in S \) (this set is finite and computable). Define

\[
\mathcal{M} = \bigcup_{i=1}^N \mathcal{M}_{S/\sim_i, R/\sim_i}
\]

the set of all generalized Dowling geometries subordinate to a group presentation in \( \{\langle S/ \sim_i \mid R/ \sim_i \rangle\} \). We show that at least one \( M \in \mathcal{M} \) is almost-multilinear if and only if \( w \neq e \) in \( G \):

In one direction, suppose some \( M \in \mathcal{M} \) is almost-multilinear. Then for some \( 1 \leq i \leq N \), \( M \) is a generalized Dowling geometry subordinate to \( \langle S/ \sim_i \mid R/ \sim_i \rangle \). By Theorem 9.9 we have that \( [w]_{\sim_i} \neq [e]_{\sim_i} \) in \( \langle S/ \sim_i \mid R/ \sim_i \rangle \). Since \( \langle S/ \sim \mid R/ \sim \rangle \) is a quotient of \( \langle S \mid R \rangle \) (and the quotient map takes \( w \) to \( [w]_{\sim_i} \)) we have \( w \neq e \) in \( G \).

In the other direction suppose \( w \neq e \) in \( G \). Then the relation \( \sim \) on \( S \) defined by setting \( s_1 \sim s_2 \) for \( s_1, s_2 \in S \) if and only if \( s_1 = s_2 \) in \( G \) is among \( \{\sim_i\}_{i=1}^N \) since it does not identify \( w \) with \( e \). By Corollary 9.7 one of the generalized Dowling geometries subordinate to the group presentation \( \langle S/ \sim \mid R/ \sim \rangle \) is almost multilinear.

It follows that any given instance of the word problem for \( G \) can be (computably) reduced to finitely many instances of the almost-multilinear representability problem. Thus, if the latter is decidable then so is the former. But by Theorem 2.12 there is a finitely presented sofic group \( G \) with an undecidable word problem, so almost-multilinear representability is undecidable. \( \Box \)
Appendix A. Proof of Theorem 4.4

The proof relies on these two properties of entropy functions found for instance in [Yeu08].

Lemma A.1. Suppose \( \{X_e\}_{e \in E} \) is finite collection of random variables on a discrete probability space \((\Omega, P)\) and assume \( H(X_A) < \infty \) for all \( A \subseteq E \).

(a) Then it holds that
\[
H(X_E) \leq \sum_{e \in E} H(X_e)
\]
and equality holds if and only if the family \( \{X_e\}_{e \in E} \) is independent.

(b) Furthermore, it holds that
\[
H(X_{E \setminus \{c\}}) \leq H(X_E)
\]
and equality holds if and only if the family \( \{X_e\}_{e \in E \setminus \{c\}} \) determines \( X_c \).

We now proceed with proving one part of the first statement in Theorem 4.4.

Lemma A.2. An entropic matroid \( M = (E, r) \) has a discrete probability space representation.

Proof. By assumption there exists a collection \( \{X_e\}_{e \in E} \) of random variables on a discrete probability space \((\Omega, P)\) and a scalar \( \lambda \in \mathbb{R}_+ \) such that \( r(A) = \lambda H(X_A) \) for all \( A \subseteq E \).

Let \( e \in E \) be a non-loop. Then \( 1 = r(e) = \lambda H(X_e) \), that is, \( H(X_e) = \frac{1}{\lambda} \) for all non-loops. Hence \( X_e \) is not a trivial random variable.

Let \( A \subseteq E \) be an independent subset. Thus \( |A| = r(A) = \lambda H(X_A) \). Also, Lemma A.1 (a) yields
\[
|A| = \lambda H(X_A) \leq \lambda \sum_{e \in A} H(X_e) = \lambda \sum_{e \in A} \frac{1}{\lambda} = |A|.
\]

Hence, the second part of Lemma A.1 (a) yields that \( \{X_e\}_{e \in A} \) is independent.

Now let \( C \subseteq E \) be a circuit and \( c \in C \) an element of the circuit. Thus,
\[
\lambda H(X_{C \setminus \{c\}}) = r(C \setminus \{c\}) = r(C) = \lambda H(X_C).
\]

There \( \{X_e\}_{e \in C \setminus \{c\}} \) determines \( X_c \) by Lemma A.1 (b) which verifies the determination property of collections of random variables associated to circuits.

The second part of Theorem 4.4 follows from the next lemma which is a trivial generalization of a result proved by Matûs in [Mat93, p.190-191].

Lemma A.3. Let \( M = (E, r) \) be a connected matroid of rank at least two and suppose \( \{X_e\}_{e \in E} \) is a probability space representation of \( M \). Then every \( X_e \) is a uniformly distributed random variables and its underlying probability space can be chosen to be finite.

Proof. Let \( \{X_e\}_{e \in E} \) be a collection of random variables on a discrete probability space \((\Omega, P)\) is forming a probability space representation of \( M \). Consider a pair \( \{e, e'\} \subseteq E \) of distinct elements of \( M \). If \( r(\{e, e'\}) = 1 \), that is \( e \) and \( e' \) are parallel elements, then \( X_e \) and \( X_{e'} \) determine each other which means that the probability distributions of these two random variables agree up to a bijection between \( \Omega_e \) and \( \Omega_{e'} \).

If \( r(\{e, e'\}) = 2 \) then by assumption there exists a circuit \( C \) with \( \{e, e'\} \subseteq C \). Set \( L = C \setminus \{e, e'\} \). Let \( \omega_e \in \Omega_e \) and \( \omega_{e'} \in \Omega_{e'} \) be two elements with \( P_e(\omega_e) > 0 \) and \( P_{e'}(\omega_{e'}) > 0 \). Since \( \{e, e'\} \) is independent this implies
\[
P_{\{e,e'\}}(\omega_e, \omega_{e'}) = P_e(\omega_e)P_{e'}(\omega_{e'}) > 0.
\]
Thus, there exists a $\omega_L \in \Omega_e$ with $P_C(\omega_L, \omega_e, \omega_{e'}) > 0$ and $P_L(\omega_L) > 0$. Using the determination condition we then obtain

$$P_L(\omega_L)P_{e'}(\omega_e) = P_C(\omega_L, \omega_e, \omega_{e'}) = P_L(\omega_L)P_{e'}(\omega_{e'}).$$

Hence, $P_e(\omega_e) = P_{e'}(\omega_{e'})$ for all non-trivial events $\omega_e$ and $\omega_{e'}$. Therefore, all random variables associated to non-loops of the matroid are uniformly distributed. Thus they all have finite support which must be of equal size. Removing all events in $\Omega_e$ that occur with probability zero yields the second claim. \qed

This allows us to prove the last missing piece of Theorem 4.4.

**Lemma A.4.** Let $M = (E, r)$ be a connected matroid that has a discrete probability space representation. Then $M$ is also entropic.

**Proof.** By assumption there exists a collection $\{X_e\}_{e \in E}$ of random variables on a discrete probability space $(\Omega, P)$ satisfying the assumptions of Definition 4.2. Using Lemma A.3 we can assume that the probability spaces $\Omega_e$ for $e \in E$ are finite and therefore $H(X_A) < \infty$ for all $A \subseteq E$. For every non-loop $e \in E$, the random variable $X_e$ is non-trivial which implies $H(X_e) > 0$.

Let $\{e, e'\} \subseteq E$ be a pair of non-loops elements. Since $M$ is connected there exists a circuit $C$ with $\{e, e'\} \subseteq C$. Then Lemma A.1 implies

$$H(X_e) + H(X_{C\setminus\{e,e'\}}) = H(X_{C\setminus\{e'\}}) = H(X_{C\setminus\{e\}}) = H(X_{e'}) + H(X_{C\setminus\{e,e'\}}).$$

Thus, $H(X_e) = H(X_{e'})$ for all non-loops $e, e'$ and we set $\lambda := \frac{1}{H(X_e)}$ for some non-loop $e$ which is well-defined as $H(X_e) > 0$ by assumption on $X_e$ being non-trivial.

Lemma A.1 (a) then implies $r(A) = \lambda H(X_A)$ for all independent subsets $A \subseteq E$. Lemma A.1 (b) and entropy functions being submodular yields this equality for all subsets of $E$ which completes the proof. \qed

**Appendix B. Proof of Theorem 9.5**

For $a, b \in \mathbb{R}$, the notation $a \approx_\varepsilon b$ means $|a - b| \leq \varepsilon$.

**Lemma B.1.** Let $M = (E, r)$ be a simple matroid. A vector space $V$ and a collection of linear maps $\{T_e : V \to W_e\}_{e \in E}$ define a vector space representation of $M$ if and only if there exists $c \in \mathbb{N}$ such that for all $S \subseteq E$

$$r(S) = \frac{1}{c} \text{rk}(T_S).$$

**Proof.** Suppose $V$ and the maps $\{T_e\}_{e \in E}$ define a vector space representation of $M$. Then $c := \dim W_e = \text{rk}(T_e)$ is independent of $e \in E$. Each $S \subseteq E$ contains a maximal independent subset $S' \subseteq S$ with $r(S) = r(S') = |S'|$, which then satisfies

$$\text{rk}(T_{S'}) = \sum_{e \in S'} \text{rk}(T_e) = c|S'|.$$

If $e \in S \setminus S'$ then $e$ is in the closure of $S'$, so $T_e$ is determined by $\{T_f\}_{f \in S'}$. It follows that $\text{rk}(T_S) = \text{rk}(T_{S'}) = c|S'| = cr(S)$.

Conversely, suppose a vector space $V$ and linear maps $\{T_e : V \to W_e\}_{e \in E}$ are given such that $\text{rk}(T_S) = cr(S)$ for all $S \subseteq E$. If $S \subseteq E$ is independent then $r(S) = |S|$, so that $\text{rk}(T_S) = c|S| = \sum_{e \in S} \text{rk}(T_e)$, and the maps $\{T_e\}_{e \in S}$ are independent. If $C = \{e_1, \ldots, e_n\}$ is a circuit of $M$ then $r(C) = |C| - 1$ and $C \setminus \{e_1\}$ is independent, so

$$\text{rk}(T_{C\setminus\{e_1\}}) = c(|C| - 1) = \text{rk}(T_C).$$
The map $\pi : \bigoplus_{e \in C} W_e \to \bigoplus_{e \in C \setminus \{e_1\}} W_e$ which drops the $W_{e_1}$ coordinate satisfies $T_{C \setminus \{e_1\}} = \pi \circ T_C$, so it induces an isomorphism $\text{im}(T_C) \to \text{im}(T_{C \setminus \{e_1\}})$ ($\pi$ must be a surjection onto $\text{im}(T_{C \setminus \{e_1\}})$ because $T_{C \setminus \{e_1\}}$ is a surjection; the dimensions of the two spaces are equal, so it is injective as well). Let $\psi : \text{im}(T_{C \setminus \{e_1\}}) \to \text{im}(T_C)$ be its inverse and let $\pi_{e_1} : \bigoplus_{e \in C} W_e \to W_{e_1}$ be the projection to the $W_{e_1}$ summand. Then

$$(\pi_{e_1} \circ \psi) \circ T_{C \setminus \{e_1\}} = \pi_{e_1} \circ T_C = T_{e_1},$$

and $T_{e_1}$ is determined by $\{T_e\}_{e \in C \setminus \{e_1\}}$ as required. \hfill \Box

The proof of the analogous statement for almost-multilinear matroids is very similar. The following simple claim is useful:

**Lemma B.2.** Let $T : W_1 \to W_2$ be a surjection. Then there exists a map $S : W_2 \to W_1$ such that $\text{rk}(S \circ T - \text{id}_{W_1}) \leq \dim W_1 - \dim W_2$.

**Proof.** Pick a basis $v_1, \ldots, v_n$ of $W_2$ and choose $w_1 \in T^{-1}(v_1), \ldots, w_n \in T^{-1}(v_n)$. Then $w_1, \ldots, w_n$ are independent since they have an independent image, and they can be completed to a basis $w_1, \ldots, w_n, w_{n+1}, \ldots, w_{n+r}$ of $W_1$. Define $S : W_2 \to W_1$ on $v_1, \ldots, v_n$ by $S(v_i) = w_i$ and extend linearly. Then the map $S \circ T - \text{id}_{W_1}$ vanishes on span $(w_1, \ldots, w_n)$, so its image is equal to the image of its restriction to span $(w_{n+1}, \ldots, w_{n+r})$, and therefore has dimension at most $r = \dim W_1 - \dim W_2$. \hfill \Box

**Lemma B.3.** Let $M = (E, r)$ be a simple matroid, let $V$ be a vector space and let $\{T_e : V \to W_e\}_{e \in E}$ be a collection of linear maps. If $\{T_e\}_{e \in E}$ defines an $\varepsilon$-approximate vector space representation of $M$ then there exists $c \in \mathbb{N}$ such that

$$\text{rk}(T_S) \approx_{c|E|c} c \cdot r(S) \quad \text{for all } S \subseteq E.$$

Conversely, if there exists $c \in \mathbb{N}$ such that $\text{rk}(T_e) = c$ for all $e \in E$ and

$$\text{rk}(T_S) \approx_{c|E|c} c \cdot r(S) \quad \text{for all } S \subseteq E$$

then the maps $\{T_e\}_{e \in E}$ define a $2\varepsilon$-approximate vector space representation of $M$.

**Proof.** Suppose $V$ and the maps $\{T_e\}_{e \in E}$ define an $\varepsilon$-approximate vector space representation of $M$. Then $c := \dim W_e = \text{rk}(T_e)$ is independent of $e \in E$. Each nonempty $S \subseteq E$ contains a maximal independent subset $S' \subseteq S$ with $r(S) = r(S') = |S'|$, which then satisfies

$$\text{rk}(T_{S'}) \approx_{c|E|c} c \cdot \sum_{e \in S'} \text{rk}(T_e) = c |S'|.$$

If $e \in S \setminus S'$ then $e$ is in the closure of $S'$, so $T_e$ is determined by $\{T_f\}_{f \in S'}$ with error $\varepsilon$. It follows that

$$\text{rk}(T_S) \approx_{c|S|\cdot |S'|\cdot c} \text{rk}(T_{S'}) \approx_{c|S'|c} c \cdot r(S),$$

so

$$\text{rk}(T_S) \approx_{c|S|\cdot |S'|+1\cdot c} c \cdot r(S),$$

where $|S| - |S'| + 1 \leq |E|$ because $S' \neq \emptyset$ (or $S$ consists of loops, and $M$ is not simple).

Conversely, suppose a vector space $V$ and linear maps $\{T_e : V \to W_e\}_{e \in E}$ are given such that $\text{rk}(T_S) \approx_{c|E|c} c \cdot r(S)$ for all $S \subseteq E$. If $S \subseteq E$ is independent then $r(S) = |S|$, so that $\text{rk}(T_S) \approx_{c|E|c} c |S| = \sum_{e \in S} \text{rk}(T_e)$, and the maps $\{T_e\}_{e \in S}$ are independent with error $\varepsilon$. If $C = \{e_1, \ldots, e_n\}$ is a circuit of $M$ then $r(C) = |C| - 1$ and $C \setminus \{e_1\}$ is independent, so

$$\text{rk}(T_{C \setminus \{e_1\}}) \approx_{c|C|\cdot (|C|-1)} \approx_{c|E|c} \text{rk}(T_C),$$

and $\text{rk}(T_{C}) - \text{rk}(T_{C \setminus \{e_1\}}) \leq 2c \varepsilon$. The map $\pi : \bigoplus_{e \in C} W_e \to \bigoplus_{e \in C \setminus \{e_1\}} W_e$ which drops the $W_{e_1}$-coordinate satisfies $T_{C \setminus \{e_1\}} = \pi \circ T_C$, so it induces a surjection $\text{im}(T_C) \to \text{im}(T_{C \setminus \{e_1\}})$ ($\pi$ is a surjection onto $\text{im}(T_{C \setminus \{e_1\}})$ because $T_{C \setminus \{e_1\}}$ is a surjection). Lemma B.2 implies that
there exists $\psi : \text{im}(T_{c \setminus \{e_1\}}) \to \text{im}(T_C)$ such that
\[
\text{rk} \left( \psi \circ \pi - \text{id}_{\text{im}(T_C)} \right) \leq 2c\varepsilon.
\]
Denote the projection to the $e_1$-summand $\bigoplus_{e \in C} W_e \to W_{e_1}$ by $\pi_{e_1}$. Then $\pi_{e_1} \circ T_C = T_{e_1}$ by definition, and
\[
\pi_{e_1} \circ \left( \psi \circ \pi - \text{id}_{\text{im}(T_C)} \right) \circ T_C = \pi_{e_1} \circ \psi \circ (\pi \circ T_C) - \pi_{e_1} \circ T_C
\]
has rank at most $2c\varepsilon$ (since $\left( \psi \circ \pi - \text{id}_{\text{im}(T_C)} \right)$ has rank at most $2c\varepsilon$). This shows that $T_{e_1}$ is determined by $\{T_e\}_{e \in C \setminus \{e_1\}}$ with error at most $2\varepsilon$.

Lemma B.4. A matroid $M = (E, r)$ is almost multilinear if and only if for every $\varepsilon > 0$ there exists a linear polymatroid \( (\tilde{E}, \tilde{r}) \) and a $c \in \mathbb{N}$
\[
\|r - \frac{1}{c} \tilde{r}\|_\infty < \varepsilon
\]
and in addition $\tilde{r}(e) = c$ for all $e \in E$.

Proof. One direction is trivial: if for every $\varepsilon > 0$ there exists a polymatroid as in the statement then $M$ is almost multilinear. Conversely, suppose $M$ is almost multilinear and let $\varepsilon > 0$. Denote $\varepsilon' = \frac{1}{|E| + 1}\varepsilon$. Take a linear polymatroid \( (\tilde{E}, \tilde{r}) \) and a $c \in \mathbb{N}$
\[
\lim_{n \to \infty} \left\|r - \frac{1}{c} \tilde{r}\right\|_\infty < \varepsilon'.
\]
Let $V$ be a vector space and let $\{W_e\}_{e \in E}$ be subspaces representing \( (\tilde{E}, \tilde{r}) \). Assume $\dim V \geq c$ (by enlarging $V$ if necessary). For each $e \in E$ denote $d_e = \dim W_e$, and take a basis $b_1, \ldots, b_{d_e}$ for $W_e$. If $c > d_e$ add vectors to the basis such that $b_1, \ldots, b_{d_e}, \ldots, b_c$ are linearly independent; if $c < d_e$ remove the last vectors from the list. Then define $W'_e = \text{span} \{b_1, \ldots, b_{c+1}\}$.

Consider the subspaces $\{W'_e\}_{e \in E}$. For any $S \subseteq E$ we have
\[
\left| \dim \left( \sum_{e \in S} W'_e \right) - \dim \left( \sum_{e \in S} W_e \right) \right| \leq \sum_{e \in S} \left| c - d_e \right| \leq \sum_{e \in E} \left| c - d_e \right|
\]
where $|c - d_e| = c \left| 1 - \frac{1}{c} \tilde{r}(e) \right| \leq c \left| r - \frac{1}{c} \tilde{r}\right|_\infty$.

In particular, if $r'$ is the rank function of the polymatroid represented by $\{W'_e\}_{e \in E}$ then
\[
\left| r' - \tilde{r}\right|_\infty \leq |E| \left| r - \frac{1}{c} \tilde{r}\right|_\infty,
\]
and therefore
\[
\left| r - \frac{1}{c} r'\right|_\infty \leq \left| r - \frac{1}{c} r\right|_\infty + \left| \frac{1}{c} r' - \frac{1}{c} r\right|_\infty = \left| r - \frac{1}{c} \tilde{r}\right|_\infty + \frac{1}{c} \left| r' - \tilde{r}\right|_\infty
\]
\[
\leq \left| r - \frac{1}{c} \tilde{r}\right|_\infty (|E| + 1) < \varepsilon.
\]

Proof of Theorem 9.5. Let $V$ be a finite dimensional vector space and let $\{W_e\}_{e \in E}$ be a finite indexed collection of subspaces. For each $W \leq V$ denote by $W^0 \leq V^*$ the annihilator of
W in the dual space, and recall \( \dim W^0 = \dim V - \dim W \). Define \( T_e : V^* \to V^*/W_e^0 \) to be the quotient map. The indexed collection of maps \( \{ T_e : V^* \to V^*/W_e^0 \}_{e \in E} \) satisfies
\[
\ker T_S = \bigcap_{e \in S} W_e^0 = \left( \sum_{e \in S} W_e \right)^0
\]
for any \( S \subseteq E \), where \( T_S \) is the map
\[
T_S : V^* \to \bigoplus_{e \in S} V^*/W_e^0.
\]
Thus
\[
\operatorname{rk}(T_S) = \dim V^* - \dim \ker T_S = \dim V^* - \left( \dim V - \dim \left( \sum_{e \in S} W_e \right) \right)
\]
and \( \dim V^*/W_e^0 = \dim W_e \) for all \( e \in E \).

It follows that the subspaces \( \{ W_e \}_{e \in E} \) define a multilinear representation of a matroid \((E, r)\) if and only if the maps \( \{ T_e \}_{e \in E} \) define a vector space representation. Similarly, by Lemma B.4 and Lemma B.3 the matroid \( M = (E, r) \) is almost multilinear if and only if for every \( \varepsilon > 0 \) it has an \( \varepsilon \)-approximate vector space representation. \( \square \)

**Appendix C. Ultraproducts of Small Categories with Metric Hom-sets**

We define categories with metric hom-sets and their metric ultraproducts.

Much of the notation and terminology in this appendix is nonstandard, and we are not aware of analogous notions in the literature (though they likely exist).

**Definition C.1.** A category with metric hom-sets is a category \( C \) such that for any \( x, y \in \text{ob}(C) \) the set \( \text{Hom}_C(x, y) \) is endowed with the structure of a metric space. In this case we denote the metric on each hom-set \( \text{Hom}_C(x, y) \) by \( d_{(x,y)} \), or \( d \) if the context is clear.

We define categories with pseudometric hom-sets analogously: each hom-set is endowed with a pseudometric.\(^1\)

A small category \( C \) with metric (or pseudometric) hom-sets has composition that does not increase errors if for any \( x, y, z \in \text{ob}(C) \) and morphisms \( f_1, f_2 : x \to y \) and \( g_1, g_2 : y \to z \):
\[
d_{(x,z)}(g_1 \circ f_1, g_2 \circ f_2) \leq d_{(y,z)}(g_1, g_2) + d_{(x,y)}(f_1, f_2).
\]

**Lemma C.2.** Let \( C \) be the category of \( c \)-dimensional vector spaces and linear maps over a fixed field \( \mathbb{F} \). Endow each hom-set with the normalized rank metric. Then the composition in \( C \) does not increase errors.

**Proof.** Let \( U, V, \) and \( W \) be vector spaces of dimension \( c \) over \( \mathbb{F} \). Let \( f_1, f_2 : U \to V \) and \( g_1, g_2 : V \to W \) be linear maps. Then by the triangle inequality and the fact that \( \operatorname{rk}(f \circ g) \leq \min(\operatorname{rk}(f), \operatorname{rk}(g)) \) for any composable linear maps \( f, g \) between finite-dimensional vector spaces:
\[
d_{U,W}(g_1 \circ f_1, g_2 \circ f_2) \leq d_{U,W}(g_1 \circ f_1, g_2 \circ f_1) + d_{U,W}(g_2 \circ f_1, g_2 \circ f_2)
\]
\[
= \frac{1}{c} \left[ \operatorname{rk}((g_1 - g_2) \circ f_1) + \operatorname{rk}(g_2 \circ (f_1 - f_2)) \right]
\]
\[
\leq \frac{1}{c} \left[ \operatorname{rk}(g_1 - g_2) + \operatorname{rk}(f_1 - f_2) \right] = d_{V,W}(g_1, g_2) + d_{U,V}(f_1, f_2). \quad \square
\]

\(^1\)Recall that a pseudometric is just like a metric, except that the distance between distinct points may be
Definition C.3. Let \((D_n)_{n \in \mathbb{N}}\) be a sequence of small categories and let \(\mathcal{U}\) be a non-principal ultrafilter. The ultraproduct \(\prod_{\mathcal{U}} D_n\) is the category \(D\) defined as follows:

1. The objects are sequences \((x_n)_{n \in \mathbb{N}}\) with \(x_n \in \text{ob}(D_n)\), modulo the equivalence relation \(\sim\) defined by setting \((x_n)_{n \in \mathbb{N}} \sim (x'_n)_{n \in \mathbb{N}}\) whenever \(\{n \in \mathbb{N} \mid x_n = x'_n\} \in \mathcal{U}\).

The equivalence class of a sequence \((x_n)_{n \in \mathbb{N}}\) is denoted by \([x_n]_{n \in \mathbb{N}}\).

2. For \(x, y \in \text{ob}(D)\), the hom-set \(\text{hom}_D(x, y)\) is defined as follows. Choose representative sequences \((x_n)_{n \in \mathbb{N}}\) and \((y_n)_{n \in \mathbb{N}}\) in the equivalence class of \(x\) and \(y\) respectively.

Define a pre-morphism \(f : x \to y\) to be a sequence \((f_n)_{n \in \mathbb{N}}\) such that each \(f_n\) is either a morphism \(f_n : x_n \to y_n\) or the formal symbol \(\bot\) (which is assumed to not be a member of any hom-set,

and which in addition satisfies the condition \(\{n \in \mathbb{N} \mid f_n \neq \bot\} \in \mathcal{U}\).

A morphism \(f : x \to y\) is an equivalence class of pre-morphisms under the equivalence relation \(\sim\) defined by setting \((f_n)_{n \in \mathbb{N}} \sim (g_n)_{n \in \mathbb{N}}\) whenever \(\{n \in \mathbb{N} \mid f_n = g_n\} \in \mathcal{U}\).

The equivalence class of a sequence \((f_n)_{n \in \mathbb{N}}\) is denoted by \([f_n]_{n \in \mathbb{N}}\).

This is well-defined (and does not depend on the choice of representative sequences for \(x\) and \(y\)). The use of the same notation for both equivalence relations will not cause confusion: we do not need to denote either of them explicitly.

If the categories \(\{D_n\}_{n \in \mathbb{N}}\) have metric hom-sets of uniformly bounded diameter, the hom-sets in \(D\) are pseudometric spaces of bounded diameter: the distance between two morphisms \([f_n]_{n \in \mathbb{N}}, [g_n]_{n \in \mathbb{N}} \in \text{hom}_D(x, y)\) is defined to be

\[
\lim_{n \to \mathcal{U}} d(f_n, g_n)
\]

(where we may set the value of the expressions \(d(\bot, g_n)\) and \(d(f_n, \bot)\) arbitrarily). Again this is well-defined: although the expression in the definition depends on representative sequences \((f_n)_{n \in \mathbb{N}}\) and \((g_n)_{n \in \mathbb{N}}\), its value does not.

Remark C.4. If there is no uniform bound on the diameters of the hom-sets, the pseudometric may also achieve the value \(\infty\). This causes no issues, but does not occur in our application.

Lemma C.5. Suppose \((D_n)_{n \in \mathbb{N}}\) is a sequence of small categories with metric hom-sets in which the composition does not increase errors. Let \(D = \prod_{\mathcal{U}} D_n\) be the ultraproduct with respect to a non-principal ultrafilter. Then the composition in \(D\) does not increase errors.

Proof. Let \(f_1, f_2 : x \to y\) and \(g_1, g_2 : y \to z\) be morphisms in \(D\). Choose representative sequences \((x_n)_{n \in \mathbb{N}}, (y_n)_{n \in \mathbb{N}},\) and \((z_n)_{n \in \mathbb{N}}\) for the objects \(x, y,\) and similarly \((f_{i,n})_{n \in \mathbb{N}}\) and \((g_{i,n})_{n \in \mathbb{N}}\) for the morphisms (where \(i = 1, 2\)). We have

\[
d(f_1 \circ g_1, f_2 \circ g_2) = \lim_{n \to \mathcal{U}} d(f_1 \circ g_{1,n}, f_2 \circ g_{2,n})
\]

\[
\leq \lim_{n \to \mathcal{U}} [d(f_1, f_2) + d(g_{1,n}, g_{2,n})] = d(f_1, f_2) + d(g_1, g_2)
\]

since the limit is additive. 

Definition C.6. Suppose \((D_n)_{n \in \mathbb{N}}\) is a sequence of small categories with metric hom-sets and assume composition in each \(D_n\) does not increase errors. Let \(\mathcal{U}\) be a non-principal ultrafilter. The congruence of infinitesimals on \(D = \prod_{\mathcal{U}} D_n\) is the congruence relation \(\sim_{\inf}\) zero.
defined as follows. For each \( x, y \in \text{ob}(\mathcal{D}) \), morphisms \( f_1, f_2 : x \to y \) are equivalent under 
the congruence relation if \( d(f_1, f_2) = 0 \).

The metric ultraproduct of \((\mathcal{D}_n)_{n \in \mathbb{N}}\) is the quotient \( \mathcal{D} / \sim_{\inf} \). The metric ultraproduct has a metric defined on each \( \text{hom}_{\mathcal{D}}(x, y) \) well defined in the quotient \( \text{hom}_{\mathcal{D} / \sim_{\inf}}(x, y) \).

We denote objects and morphisms of the metric ultraproduct \( \mathcal{D} / \sim_{\inf} \) in just the same way as we denote objects and morphisms of the corresponding ultraproduct. This causes no confusion because the category under discussion is always clear from context.

**Remark C.7.** This is a congruence (i.e., an equivalence relation such that composition is well-defined in the quotient, which is thus a category) because composition in \( \mathcal{D} \) does not increase errors. Observe that if \( f_1, f_2 : x \to y \) and \( g_1, g_2 : y \to z \) are morphisms in \( \mathcal{D} \) such that \( f_1 \sim_{\inf} f_2 \) and \( g_1 \sim_{\inf} g_2 \) then \( d(g_1, g_2) = 0 \) and \( d(f_1, f_2) = 0 \), so we have \( d(g_1 \circ f_1, g_2 \circ f_2) = 0 \). Therefore also \( g_1 \circ f_1 \sim_{\inf} g_2 \circ f_2 \).

Note that for the existence of a metric ultraproduct it suffices that the infinitesimal equivalence relation is in fact a congruence. This is weaker than the requirement that composition does not increase errors, but continuous compositions do not suffice.

For the following definitions see also Awodey’s book [Aw10]. All our directed graphs may have multiple edges between the same pair of edges.

**Definition C.8 (Free and finitely presented categories).** The free category on a directed graph \( G \) is the category \( \mathcal{C}(G) \) in which objects are the vertices of \( G \), morphisms are (directed) paths in \( G \), and composition is given by concatenating paths.

Let \( \mathcal{C} \) be a category and let \( R = \{ f_i = g_i \}_{i \in I} \) be a set of expressions (“relations”) such that for each \( i \), \( f_i, g_i : x_i \to y_i \) are two morphisms between the same two objects of \( \mathcal{C} \). Denote by \( \sim_R \) the minimal congruence satisfying that \( f_i \sim_R g_i \) for each \( i \in I \). We call \( \sim_R \) the congruence generated by the relations in \( R \).

A finitely presented category is a category of the form \( \mathcal{C}(G) / \sim_R \), where \( G \) is a finite directed graph and \( R \) is a finite set of relations between morphisms of \( \mathcal{C}(G) \).

The underlying graph of a category \( \mathcal{C} \) is the directed graph \( \text{Graph}(\mathcal{C}) \) in which vertices are objects of \( \mathcal{C} \) and edges are morphisms, given the appropriate orientation (a morphism \( f : x \to y \) gives rise to an edge from \( x \) to \( y \)). In other words, it is a category with its composition forgotten.

A homomorphism of directed graphs \( f : G_1 \to G_2 \) is a function that maps the vertices of \( G_1 \) to the vertices of \( G_2 \) and maps the edges of \( G_1 \) to the edges of \( G_2 \) in a manner that respects the sources and terminals of the edges (if an edge \( e_1 \) of \( G_1 \) maps to an edge \( e_2 \) of \( G_2 \), the source and terminal of \( e_1 \) map to the source and terminal of \( e_2 \) respectively).

**Remark C.9.** To construct a functor \( F \) from a finitely presented category \( \mathcal{C} = \mathcal{C}(G) / \sim_R \) into a category \( \mathcal{D} \), it suffices to define \( F \) on the objects and morphisms of \( \mathcal{C} \) corresponding to vertices and edges of \( G \), and to show that if \( \varphi_1 = \varphi_2 \) is a relation in \( R \) then \( F(\varphi_1) = F(\varphi_2) \) in \( \mathcal{D} \) (see [Aw10]).

**Theorem C.10.** Let \( \mathcal{C} = \mathcal{C}(G) / \sim_R \) be the finitely presented category generated by the directed graph \( G \) and set of relations \( R \). For each \( n \in \mathbb{N} \) let \( \mathcal{D}_n \) be a small category with metric hom-sets in which the composition does not increase errors, and let \( f_n : G \to \text{Graph}(\mathcal{D}_n) \) be a homomorphism from \( G \) to the underlying graph of \( \mathcal{D}_n \). Let \( U \) be a non-principal ultrafilter, and denote the metric ultraproduct of \((\mathcal{D}_n)_{n \in \mathbb{N}}\) by \( \mathcal{D} = (\prod_U \mathcal{D}_n) / \sim_{\inf} \).

Assume that for each relation \( \varphi_1 = \varphi_2 \) in \( R \), \( d(f_n(\varphi_1), f_n(\varphi_2)) \leq \frac{1}{n} \) in \( \mathcal{D}_n \). Then there is a functor \( F : \mathcal{C} \to \mathcal{D} \) defined on objects \( x \in \text{ob}(\mathcal{C}) \) by \( f_n(x) \) and on morphisms \( \varphi \in \text{hom}_{\mathcal{C}}(x, y) \) by \( f_n(\varphi) \).
Proof. Observe that if $\varphi_1 = \varphi_2$ is a relation in $R$ then
\[ d(F(\varphi_1), F(\varphi_2)) = \lim_{n \to \infty} d(f_n(\varphi_1), f_n(\varphi_2)) = 0 \]
because for each $k \in \mathbb{N}$ we have $d(f_n(\varphi_1), f_n(\varphi_2)) \leq \frac{1}{k}$ for all $n \geq k$. Therefore $F(\varphi_1) = F(\varphi_2)$. The result follows by Remark C.9. □

REFERENCES

[Awo10] Steve Awodey, *Category theory*, second ed., Oxford Logic Guides, vol. 52, Oxford University Press, Oxford, 2010.

[BBEPT14] Amos Beimel, Aner Ben-Efraim, Carles Padró, and Ilya Tyomkin, *Multi-linear secret-sharing schemes*, Theory of cryptography, Lecture Notes in Comput. Sci., vol. 8349, Springer, Heidelberg, 2014, pp. 394–418.

[BD91] Ernest F. Brickell and Daniel M. Davenport, *On the classification of ideal secret sharing schemes*, Journal of Cryptology 4 (1991), no. 2, 123–134.

[Dow73] Thomas A. Dowling, *A class of geometric lattices based on finite groups*, Journal of Combinatorial Theory, Series B 14 (1973), no. 1, 61 – 86.

[ES06] Gábor Elek and Endre Szabó, *On sofic groups*, J. Group Theory 9 (2006), no. 2, 161–171.

[ESG10] S. El Rouayheb, A. Sprintson, and C. Georghiades, *On the index coding problem and its relation to network coding and matroid theory*, IEEE Transactions on Information Theory 56 (2010), no. 7, 3187–3195.

[Fuj78] Satoru Fujishige, *Polymatroidal dependence structure of a set of random variables*, Information and Control 39 (1978), 55–72.

[GP93] Dan Geiger and Judea Pearl, *Logical and algorithmic properties of conditional independence and graphical models*, Ann. Statist. 21 (1993), no. 4, 2001–2021.

[Kha81] Olga Kharlampovich, *A finitely presented solvable group with unsolvable word problem*, Izv. Akad. Nauk SSSR Ser. Mat. 45 (1981), no. 4, 852–873, 928.

[Kin11] Ryan Kinser, *New inequalities for subspace arrangements*, Journal of Combinatorial Theory, Series A 118 (2011), no. 1, 152 – 161.

[KKNS20] Mahmoud Abo Khamis, Phokion G. Kolaitis, Hung Q. Ngo, and Dan Suciu, *Decision Problems in Information Theory*, 47th International Colloquium on Automata, Languages, and Programming (ICALP 2020) (Dagstuhl, Germany), vol. 168, 2020, pp. 106:1–106:20.

[KPY20] Lukas Kühne, Rudi Pendavingh, and Geva Yashfe, *Von Staudt constructions for skew-linear and multilinear matroids*, arXiv e-prints (2020), arXiv:2012.07361.

[KY19] Lukas Kühne and Geva Yashfe, *Representability of matroids by c-arrangements is undecidable*, arXiv e-prints (2019), arXiv:1912.06123, to appear in the Israel Journal of Mathematics.

[Li21] Cheuk Ting Li, *The undecidability of conditional affine information inequalities and conditional independence implication with a binary constraint*, 2021 IEEE Information Theory Workshop (ITW), 2021, pp. 1–6.

[Li22] Cheuk Ting Li, *Undecidability of network coding, conditional information inequalities, and conditional independence implication*, arXiv e-prints (2022), arXiv:2205.11461.

[LS77] Roger C. Lyndon and Paul E. Schupp, *Combinatorial group theory*, Springer-Verlag, Berlin-New York, 1977, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 89.

[Mar91] Keith Murray Martin, *Discrete structures in the theory of secret sharing*, 1991.

[Mat93] František Matuš, *Probabilistic conditional independence structures and matroid theory: Background*, International Journal of General Systems 22 (1993), no. 2, 185–196.

[Mat99] František Matuš, *Matroid representations by partitions*, Discrete Math. 203 (1999), no. 1-3, 169–194.

[Mat07] František Matuš, *Two constructions on limits of entropy functions*, IEEE Transactions on Information Theory 53 (2007), no. 1, 320–330.

[Mat19] František Matuš and Aner Ben-Efraim, *A note on representing Dowling geometries by partitions*, Kybernetika (Prague) 56 (2020), no. 5, 934–947.

[NGSVG13] Mathias Niepert, Marc Gyssens, Bassem Sayrafi, and Dirk Van Gucht, *On the conditional independence implication problem: a lattice-theoretic approach*, Artificial Intelligence 202 (2013), 29–51.
[Oxl11] James Oxley, *Matroid theory*, second ed., Oxford Graduate Texts in Mathematics, vol. 21, Oxford University Press, Oxford, 2011.

[Pes08] Vladimir G. Pestov, *Hyperlinear and sofic groups: a brief guide*, Bull. Symbolic Logic 14 (2008), no. 4, 449–480.

[PP86] Judea Pearl and Azaria Paz, *Graphoids: Graph-based logic for reasoning about relevance relations or when would x tell you more about y if you already know z?*, Proceedings of the 7th European Conference on Artificial Intelligence - Volume 2, ECAI’86, North-Holland, 1986, p. 357–363.

[SA98] Juriaan Simonis and Alexei Ashikhmin, *Almost affine codes*, Designs, Codes and Cryptography 14 (1998), no. 2, 179–197.

[Sey92] Paul D. Seymour, *On secret-sharing matroids*, J. Combin. Theory Ser. B 56 (1992), no. 1, 69–73.

[Slo81] A. M. Slobodskoi, *Unsolvability of the universal theory of finite groups*, Algebra and Logic 20 (1981), no. 2, 139–156.

[Sti92] Doug Stinson, *An explication of secret sharing schemes*, Des. Codes Cryptogr. 2 (1992), no. 4, 357–390.

[Stu90] Milan Studený, *Conditional independence relations have no finite complete characterization*, 1990.

[Yeu08] R.W. Yeung, *Information theory and network coding*, Information Technology: Transmission, Processing and Storage, Springer US, 2008.

[Zas03] Thomas Zaslavsky, *Biased graphs. IV. Geometrical realizations*, J. Combin. Theory Ser. B 89 (2003), no. 2, 231–297.

**Fakultät für Mathematik, Universität Bielefeld, Bielefeld, Germany**

*Email address: lukas.kuehne@math.uni-bielefeld.de*

**Einstein Institute of Mathematics, The Hebrew University of Jerusalem, Giv’at Ram, Jerusalem, 91904, Israel**

*Email address: geva.yashfe@mail.huji.ac.il*