PhD

William Troiani

December 23, 2023

Contents

1 Introduction

The beating heart of this thesis can be described very easily as follows. Let P, Q, R be propositions and assume $P \Rightarrow Q$, and $Q \Rightarrow R$ hold. Then *modus ponens*, or the *cut rule*, allow us to infer that $P \Rightarrow R$ holds. In this process, the proposition Q is *eliminated.* On the other hand, consider variables p, q, r satisfying $p = q$ and $q = r$. Then using the elimination method for solving systems of linear equations, we can infer that $p = r$, which *eliminates* the varable q.

This thesis defends the proposition that this connection is more than superficial. We will show that viewing proofs in intuitionistic logics as *patterns of equality*, and cut-elimination as a process of elimination of variables from systems of equations forms a deep connection between logic, algebra, geometry, quantum information theory, and intersection theory (for schemes).

This perspective on proofs emerged from work done to resolve a dissatisfaction with the Curry-Howard correspondence. As a theorem, the Curry-Howard correspondence is the observation that the formulas of implicational propositional logic are the same as the types of simply-typed λ-calculus, and that there is a surjective map from the set of all proofs of a sequent $\Gamma \vdash \alpha$ in "sequent calculus" to the set of all lambda terms of type α with free variables in Γ (due to Howard [?, §3] building on ideas of Curry and Tait).

Despite its philosophical importance, this correspondence is not *mathematically* of great interest, because natural deduction and λ-calculus are so similar that the bijection is close to tautological (in the case of closed terms it is left as an exercise in one standard text [?, Ex. 4.8]).

In [18] this dissatisfaction is explained more thoroughly, but in brief, the problem is that the notion of *proof* in [?, §1] is somewhat vague in that the system called "sequent calculus" by Howard is actually a hybrid of intuitionistic sequent calculus in the sense of Gentzen's LJ and natural deduction in the sense of Gentzen [?] and Prawitz [?].

In resolving this ambiguity subsequent authors writing about the correspondence have almost universally decided that *proof* means *natural deduction proof*; see for example [?, §4.8,§7.4, §7.6] and [?]. The correspondence may then be interpreted as a bijection between lambda terms and natural deduction proofs [?, §6.5]. This bijection represents the natural conclusion of one line of development starting with [?] and henceforth we refer to this bijection as the *Curry-Howard correspondence.* Despite its philosophical importance, this correspondence is not *mathematically* of great interest, because natural deduction and lambda calculus are so similar that the bijection is close to tautological (in the case of closed terms it is left as an exercise in one standard text [?, Ex. 4.8]).

In [18] we decided once and for all that "proof" meant "a proof in the implicative fragment of intuitionistic sequent calculus", and the main theorem there is an equivalence of categories between the category of proofs $\mathcal{S}_\Gamma$ of sequents with hypotheses Γ (where we assume that Γ is repetition free), and the category of term $\mathcal{L}_{|\Gamma|}$ whose set of free variables is the underlying set $|\Gamma|$ of Γ.

Proofs are equivalence classes of *preproofs* which take as equivalent proofs which differ only by inconsequential re-ordering of applications of deduction rules. The full list of such trivialities is given in [18], and logical justifications for each of these are also given. It can be helpful to think of the equivalence of categories as a surjective map from the class of preproofs, where two preproofs are mapped to the same term if they define the same proof. This means that considering the fiber of each term yields a collection of preproofs, all belonging to the same equivalence class. Observing these equivalence classes induces a *local* vs *global* perspective on the dynamical aspects of both systems, however, what is more interesting for the this thesis is that the λ-term can be read *inside* the corresponding preproofs where variables identified inside the term are explicitly related by the structure of the proof. It is exactly here where the idea that *proofs are patterns of equality between variables* first emerged.

For example, let τ be a type and consider the Church numeral $\underline{2}_\tau = ffx$ written as a term, with respect to the context $\{f : \tau \to \tau, x : \tau\}$. Terms in the untyped λ-calculus are not expressive enough to describe along with a term t the particular choice of *construction* of that term. This can be seen concretely in $\underline{2}_\tau$ as ffx and $(ff'x)[f' \coloneqq f]$ are identical terms on the level of the syntax.

That is, the decision to, as well as the decision *when* to, identify f' and f is abscent from the syntax of terms. This equality of variables, however, is precisely the information present in a sequent calculus proof which maps onto the term in question. The following, for instance, maps onto the term ffx and the moment where f and f' are identified is made completely explicit by the contraction rule.

$$\dfrac{\dfrac{x:\tau\vdash\tau \qquad \dfrac{x':\tau\vdash\tau \qquad x'':\tau\vdash\tau}{f':\tau\supset\tau, x':\tau\vdash\tau}\,(\mathrm{L}\supset)}{f:\tau\supset\tau, f':\tau\supset\tau, x:\tau\vdash\tau}\,(\mathrm{L}\supset)}{f:\tau\supset\tau, x:\tau\vdash\tau}\,(\mathrm{ctr})$$

In [18] the *strong ancestors* of a variable in a sequent calculus proof is defined, which makes precise the variable occurrences which are identified and those which are genuinely distinct. Colour coding the above proof according to the variables' strong ancestors yields the following:

$$\dfrac{\dfrac{x:\tau\vdash\tau \qquad \dfrac{x':\tau\vdash\tau \qquad x'':\tau\vdash\tau}{f':\tau\supset\tau, x':\tau\vdash\tau}\,(\mathrm{L}\supset)}{f:\tau\supset\tau, f':\tau\supset\tau, x:\tau\vdash\tau}\,(\mathrm{L}\supset)}{f:\tau\supset\tau, x:\tau\vdash\tau}\,(\mathrm{ctr})$$

Since any term t in the simply λ-calculus can perform arbitrary many substitutions in a single β-reduction step, whereas the sequent calculus proof mapping onto t explicates these substitutions step-by-step, we describe the dynamics of the formal as *global* and the dynamics of the latter as *local*. Thus, the implicative fragment of intuitionistic sequent calculus can be seen as refinement of the untyped λ-calculus. In fact, the sequent calculus can itself be even further refined to *Linear Logic*. We claim that the "patterns of equality" perspective on proofs is still fruitful for proofs in Linear Logic too, and to make this claim precise we must understand how exactly Linear Logic is a refinement of intuitionistic sequent calculus.

Historically, this is how Linear Logic was first discovered, by refining a model of the untyped λ-calculus (which is automatically a model of the simply typed λ-calculus). We revisit this history, and simplify the original model in Section ? If the reader is willing to accept Linear Logic as a refinement of intuitionistic sequent calculus, then they may skip this section.

Need to talk about matrix factorisations here.

2 Gentzen-Mints-Zucker duality and patterns of equality

There is an infinite set of atomic formulas and if p and q are formulas then so is $p \supset q$. Let $\Psi_\supset$ denote the set of all formulas. For each formula p let Y_p be an infinite set of variables associated with p. For distinct formulas p, q the sets Y_p, Y_q are disjoint. We write $x : p$ for $x \in Y_p$ and say x *has type* p. Let $\mathcal{P}^n$ be the set of all length n sequences of variables with $\mathcal{P}^0 := \{\varnothing\}$, and $\mathcal{P} := \cup_{n=0}^{\infty}\mathcal{P}^n$. A *sequent* is a pair (Γ, p) where $\Gamma \in \mathcal{P}$ and $p \in \Psi_\supset$, written $\Gamma \vdash p$. We call Γ the *antecedent* and p the *succedent* of the sequent. Given Γ and a variable $x : p$ we write $\Gamma, x : p$ for the element of $\mathcal{P}$ given by appending $x : p$ to the end of Γ. A variable $x : p$ may occur more than once in a sequent.

Our intuitionistic sequent calculus is the system LJ of [**?**, §III] restricted to implication, with formulas in the antecedent tagged with variables and a more liberal set of deduction rules (see Remark 2.0.5). We follow the convention of [3, §5.1] in grouping (ax) and (cut) together rather than including the latter in the structural rules.

Definition 2.0.1. A *deduction rule* results from one of the schemata below by a substitution of the following kind: replace p, q, r by arbitrary formulas, x, y by arbitrary variables, and Γ, Δ, Θ by arbitrary (possibly empty) sequences of formulas separated by commas:

- the **identity group**:
  - **Axiom**:

$$\frac{}{x : p \vdash p}\ (\text{ax})$$

  - **Cut**:

$$\frac{\Gamma \vdash p \qquad \Delta, x : p, \Theta \vdash q}{\Gamma, \Delta, \Theta \vdash q}\ (\text{cut})$$

- the **structural rules**:
  - **Contraction**:

$$\frac{\Gamma, x : p, y : p, \Delta \vdash q}{\Gamma, x : p, \Delta \vdash q}\ (\text{ctr})$$

  - **Weakening**:

$$\frac{\Gamma, \Delta \vdash q}{\Gamma, x : p, \Delta \vdash q}\ (\text{weak})$$

  - **Exchange**:

$$\frac{\Gamma, x : p, y : q, \Delta \vdash r}{\Gamma, y : q, x : p, \Delta \vdash r}\ (\text{ex})$$

- the **logical rules**:
  - **Right introduction**:

$$\frac{\Gamma, x : p, \Delta \vdash q}{\Gamma, \Delta \vdash p \supset q}\ (R \supset)$$

  - **Left introduction**:

$$\frac{\Gamma \vdash p \qquad \Delta, x : q, \Theta \vdash r}{y : p \supset q, \Gamma, \Delta, \Theta \vdash r}\ (L \supset)$$

Definition 2.0.2. A *preproof* is a finite rooted planar tree where each edge is labelled by a sequent and each node except for the root is labelled by a valid deduction rule. If the edge connected to the root is labelled by the sequent $\Gamma \vdash p$ then we call the preproof a *preproof of* $\Gamma \vdash p$.

Observe that the only valid label for a leaf node is an axiom rule, so a preproof reads from the leaves to the root as a deduction of $\Gamma \vdash p$ from axiom rules.

Example 2.0.3. Here is the Church numeral $\underline{2}$ in our sequent calculus

$$\dfrac{\dfrac{\dfrac{\dfrac{}{x : p \vdash p}\,(\mathrm{ax}) \qquad \dfrac{\dfrac{}{x : p \vdash p}\,(\mathrm{ax}) \quad \dfrac{}{x : p \vdash p}\,(\mathrm{ax})}{y' : p \supset p, x : p \vdash p}\,(L \supset)}{y : p \supset p, y' : p \supset p, x : p \vdash p}\,(L \supset)}{y : p \supset p, x : p \vdash p}\,(\mathrm{ctr})}{y : p \supset p \vdash p \supset p}\,(R \supset)$$

Remark 2.0.4. Multiple occurrences of a deduction rule are communicated in the notation with doubled horizontal lines. For example if $\Gamma = x_1 : p_1, \ldots, x_n : p_n$ then the preproof

$$\begin{array}{c} \hline y : q \vdash q \\ \hline\hline \Gamma, y : q \vdash q \end{array}\ \begin{array}{l} (\mathrm{ax}) \\ (\mathrm{weak}) \end{array}$$

weakens in every formula in the sequence. The doubled horizontal line therefore stands for n occurrences of the rule (weak). The preproofs which perform these weakenings in a different order are, of course, not equal as preproofs, so the notation is an abuse. We will only use it below in the context of defining generating pairs of equivalence relations in cases where any reading of this notation leads to the same equivalence relation.

Remark 2.0.5. A deduction rule is *strict* if it is an arbitrary (ax) or (ex) rule, or it is one of the other rules and the occurrence of $x : p$ in the rule is leftmost in the antecedent. A *strict preproof* is a preproof in which every deduction rule is strict. These are the deduction rules and preproofs of Gentzen's original sequent calculus [**?**, §III]. A general deduction rule is clearly derivable from the strict rules by exchange, and so we may choose to view non-strict deduction rules as derived rules; see Lemma **??**.

We adopt the more liberal rules since they make the commuting conversions, cut-elimination transformations and the proof of cut-elimination easier to present. A similar calculus is adopted, for similar reasons, in [**?**] and elsewhere.

Remark 2.0.6. We follow Gentzen [**?**, §III] in putting the variable introduced by a $(L \supset)$ rule at the first position in the antecedent. This choice is correct from the point of view of the relationship between sequent calculus proofs and lambda terms, as may be seen in Lemma **??** and Section **??**.

2.1 The category of proofs

Under the Brouwer-Heyting-Kolmogorov interpretation of intuitionistic logic [**?**] a proof of $\Gamma \vdash p \supset q$ is viewed as a transformation from proofs of p to proofs of q. Thus it is natural to view such proofs as *morphisms* from p to q in a category where objects are formulas, morphisms are proofs and composition is (cut). Throughout this section Γ is a sequence of variables. Let $\Psi_\supset$ denote the set of formulas.

Definition 2.1.1. For a formula p we denote by Σ_p^Γ the set of preproofs of $\Gamma \vdash p$.

Definition 2.1.2. Given a preproof π of $\Gamma \vdash p \supset q$ and $x : p$ let $\pi\{x\}$ denote

$$\dfrac{\begin{matrix}\pi\\ \vdots\\ \Gamma\vdash p\supset q\end{matrix} \qquad \dfrac{\dfrac{}{x:p\vdash p}\,(\mathrm{ax}) \qquad \dfrac{}{y:q\vdash q}\,(\mathrm{ax})}{z:p\supset q, x:p\vdash q}\,(L\supset)}{\Gamma, x:p\vdash q}\,(\mathrm{cut}) \tag{1}$$

This preproof is independent up to $\sim_p$ of $y : p, z : q$ by (**??**) and (**??**).

Lemma 2.1.3. *Any preproof π of $\Gamma \vdash p \supset q$ where $p \supset q$ is introduced by means of an $(R\supset)$ rule is equivalent under $\sim_p$ to*

$$\begin{array}{cl}
\pi\{x\} & \\
\vdots & \\
\Gamma, x:p\vdash q & \\ \hline
\Gamma\vdash p\supset q & (R\supset)
\end{array} \tag{2}$$

Proof. See ?? □

Definition 2.1.4. The category $\mathcal{S}_\Gamma$ has objects $\Psi_\supset \cup \{\mathbf{1}\}$ and morphisms

$$\mathcal{S}_\Gamma(p,q) = \Sigma^\Gamma_{p\supset q} \,/ \sim_p$$
$$\mathcal{S}_\Gamma(\mathbf{1},q) = \Sigma^\Gamma_{q} \,/ \sim_p$$

with special cases $\mathcal{S}_\Gamma(p,\mathbf{1}) = \{*\}$, $\mathcal{S}_\Gamma(\mathbf{1},\mathbf{1}) = \{*\}$. For formulas p, q, r composition

$$\mathcal{S}_\Gamma(q,r) \times \mathcal{S}_\Gamma(p,q) \to \mathcal{S}_\Gamma(p,r)$$

sends the pair (ψ, π) to the proof $\psi \circ \pi$ given by

$$\begin{array}{cl}
\begin{array}{c}\pi\{x\}\\ \vdots\\ \hline \Gamma,x:p\vdash q\end{array} \qquad \begin{array}{c}\psi\{y\}\\ \vdots\\ \hline \Gamma,y:q\vdash r\end{array} & \\ \hline
\Gamma,x:p,\Gamma\vdash r & (\mathrm{cut}) \\ \hline\hline
\Gamma,x:p\vdash r & (\mathrm{ex}/\mathrm{ctr}) \\ \hline
\Gamma\vdash p\supset r & (R\supset)
\end{array} \tag{3}$$

The special cases of the composition map are defined as follows: for formulas p, q the map $\mathcal{S}_\Gamma(p,q) \times \mathcal{S}_\Gamma(\mathbf{1},p) \to \mathcal{S}_\Gamma(\mathbf{1},q)$ sends (ψ, π) to

$$\begin{array}{cl}
\begin{array}{c}\pi\\ \vdots\\ \hline \Gamma\vdash p\end{array} \qquad \begin{array}{c}\psi\{x\}\\ \vdots\\ \hline \Gamma,x:p\vdash q\end{array} & \\ \hline
\Gamma,\Gamma\vdash q & (\mathrm{cut}) \\ \hline\hline
\Gamma\vdash q & (\mathrm{ex}/\mathrm{ctr})
\end{array} \tag{4}$$

and the map $\mathcal{S}_\Gamma(\mathbf{1},q) \times \mathcal{S}_\Gamma(p,\mathbf{1}) \to \mathcal{S}_\Gamma(p,q)$ sends $(\pi, *)$ to

$$\dfrac{\dfrac{\dfrac{\begin{matrix}\pi\\ \vdots\end{matrix}}{\Gamma \vdash q}}{\Gamma, x : p \vdash q}\,(\text{weak})}{\Gamma \vdash p \supset q}\,(R \supset) \tag{5}$$

and $\mathcal{S}_\Gamma(\mathbf{1}, p) \times \mathcal{S}_\Gamma(\mathbf{1}, \mathbf{1}) \to \mathcal{S}_\Gamma(\mathbf{1}, p)$ is the projection.

Note that the composition $\psi \circ \pi$ depends as a preproof on the choices of intermediate variables $x : p, y : q$ but is independent of these choices by (**??**) and (**??**). The identity morphism $1_p : p \longrightarrow p$ in $\mathcal{S}_\Gamma$ for a formula p is the proof

$$\dfrac{\genfrac{}{}{2pt}{0}{\dfrac{}{x : p \vdash p}\,(\text{ax})}{\Gamma, x : p \vdash p}\,(\text{weak})}{\Gamma \vdash p \supset p}\,(R \supset)$$

2.2 Simply typed λ-calculus and the category of terms

We define a category $\mathcal{L}$ whose objects are the types of simply-typed lambda calculus, and whose morphisms are the terms of that calculus. The natural desiderata for such a category are that the fundamental algebraic structure of lambda calculus, function application and lambda abstraction, should be realised by categorical algebra.

We assume familiarity with simply-typed λ-calculus; some details are recalled in Appendix **??**. Following Church's original presentation our lambda calculus only contains function types and $\Phi_\to$ denotes the set of simple types. We write Λ_σ for the set of α-equivalence classes of lambda terms of type σ.

Definition 2.2.1 ((Category of lambda terms))**.** The category $\mathcal{L}$ has objects

$$\mathrm{ob}(\mathcal{L}) = \Phi_\to \cup \{\mathbf{1}\}$$

and morphisms given for types $\sigma, \tau \in \Phi_\to$ by

$$\begin{aligned}
\mathcal{L}(\sigma, \tau) &= \Lambda_{\sigma \to \tau} / {=_{\beta\eta}}\\
\mathcal{L}(\mathbf{1}, \sigma) &= \Lambda_\sigma / {=_{\beta\eta}}\\
\mathcal{L}(\sigma, \mathbf{1}) &= \{\star\}\\
\mathcal{L}(\mathbf{1}, \mathbf{1}) &= \{\star\},
\end{aligned}$$

where $\star$ is a new symbol. For $\sigma, \tau, \rho \in \Phi_\to$ the composition rule is the function

$$\begin{aligned}
\mathcal{L}(\tau, \rho) \times \mathcal{L}(\sigma, \tau) &\longrightarrow \mathcal{L}(\sigma, \rho)\\
(N, M) &\longmapsto \lambda x^\sigma \ldots (N\,(M\,x)),
\end{aligned}$$

where $x \notin \mathrm{FV}(N) \cup \mathrm{FV}(M)$. We write the composite as $N \circ M$. In the remaining special cases the composite is given by the rules

$$\begin{aligned}
\mathcal{L}(\tau, \rho) \times \mathcal{L}(\mathbf{1}, \tau) &\longrightarrow \mathcal{L}(\mathbf{1}, \rho), && N \circ M = (N\,M),\\
\mathcal{L}(\mathbf{1}, \rho) \times \mathcal{L}(\mathbf{1}, \mathbf{1}) &\longrightarrow \mathcal{L}(\mathbf{1}, \rho), && N \circ \star = N,\\
\mathcal{L}(\mathbf{1}, \rho) \times \mathcal{L}(\sigma, \mathbf{1}) &\longrightarrow \mathcal{L}(\sigma, \rho), && N \circ \star = \lambda t^\sigma \ldots N,
\end{aligned}$$

where in the final rule $t \notin \mathrm{FV}(N)$. All other cases are trivial. Note that these functions, which have been described using a choice of representatives from a $\beta\eta$-equivalence class, are nonetheless well-defined.

For terms M, N the expression $M = N$ always means equality of terms (that is, up to α-equivalence) and we write $M =_{\beta\eta}$ if we want to indicate equality up to $\beta\eta$-equivalence (for example as morphisms in the category $\mathcal{L}$). Since the free variable set of a lambda term is not invariant under β-reduction, some care is necessary in defining the category $\mathcal{L}_Q$ below. Let $\twoheadrightarrow_\beta$ denote multi-step β-reduction [**?**, Definition 1.3.3].

Lemma 2.2.2. *If $M \twoheadrightarrow_\beta N$ then* $\mathrm{FV}(N) \subseteq \mathrm{FV}(M)$.

Definition 2.2.3. Given a term M we define

$$\mathrm{FV}_\beta(M) = \bigcap_{N =_\beta M} \mathrm{FV}(N)$$

where the intersection is over all terms N which are β-equivalent to M.

Clearly if $M =_\beta M'$ then $\mathrm{FV}_\beta(M) = \mathrm{FV}_\beta(M')$.

Lemma 2.2.4. *Given terms $M : \sigma \to \rho$ and $N : \sigma$ we have*

$$\mathrm{FV}_\beta((MN)) \subseteq \mathrm{FV}_\beta(M) \cup \mathrm{FV}_\beta(N)\,.$$

Proof. We may assume M, N β-normal, in which case there is a chain of β-reductions $(MN) \twoheadrightarrow_\beta \widehat{(MN)}$ whence we are done by Lemma 2.2.2. □

By the same argument

Lemma 2.2.5. *Given $M : \sigma \to \rho$ and $N : \tau \to \sigma$ we have*

$$\mathrm{FV}_\beta(M \circ N) \subseteq \mathrm{FV}_\beta(M) \cup \mathrm{FV}_\beta(N)\,. \tag{6}$$

Given a set Q of variables we write Λ^Q_σ for the set of lambda terms M of type σ with $\mathrm{FV}(M) \subseteq Q$. Let $=_{\beta\eta}$ denote the induced relation on this subset of Λ_σ.

Lemma 2.2.6. *For any type σ and set Q of variables the image of the injective map*

$$\Lambda^Q_p / =_{\beta\eta} \longrightarrow \Lambda_p / =_{\beta\eta} \tag{7}$$

is the set of equivalence classes of terms M with $\mathrm{FV}_\beta(M) \subseteq Q$.

Proof. Since the simply-typed lambda calculus is strongly normalising [**?**, Theorem 3.5.1] and confluent [**?**, Theorem 3.6.3] there is a unique normal form $\widehat{M}$ in the β-equivalence class of M, and $\mathrm{FV}_\beta(M) = \mathrm{FV}(\widehat{M})$. Hence if $\mathrm{FV}_\beta(M) \subseteq Q$ then $\mathrm{FV}(\widehat{M}) \subseteq Q$ and so M is in the image of (7). □

Definition 2.2.7. For a set of variables Q we define a subcategory $\mathcal{L}_Q \subseteq \mathcal{L}$ by

$$\mathrm{ob}(\mathcal{L}_Q) = \mathrm{ob}(\mathcal{L}) = \Phi_\to \cup \{\mathbf{1}\}$$

and for types σ, ρ

$$\begin{aligned}
\mathcal{L}_Q(\sigma,\rho) &= \{M \in \mathcal{L}(\sigma,\rho) l \, \mathrm{FV}_\beta(M) \subseteq Q\}\,,\\
\mathcal{L}_Q(\mathbf{1},\sigma) &= \{M \in \mathcal{L}(\mathbf{1},\sigma) l \, \mathrm{FV}_\beta(M) \subseteq Q\}\,,\\
\mathcal{L}_Q(\sigma,\mathbf{1}) &= \mathcal{L}(\sigma,\mathbf{1}) = \{\star\}\,,\\
\mathcal{L}_Q(\mathbf{1},\mathbf{1}) &= \mathcal{L}(\mathbf{1},\mathbf{1}) = \{\star\}\,.
\end{aligned}$$

Note that the last two lines have the same form using the convention that $\mathrm{FV}_\beta(\star) = \varnothing$.

The fact that $\mathcal{L}_Q$ is a subcategory follows from Lemma 2.2.5.

Remark 2.2.8. We sketch how function application and lambda abstraction in the simply-typed lambda calculus are realised as natural categorical algebra in $\mathcal{L}$. Function application is composition, and lambda abstraction is given by a universal property involving factorisation of morphisms in $\mathcal{L}$ through morphisms in $\mathcal{L}_Q$.

To explain, let $M \in \mathcal{L}(\sigma,\rho)$ be a morphism and $q : \tau$ a variable. We can consider the set of all commutative diagrams in $\mathcal{L}$ of the form

$$\begin{tikzcd}
\sigma \arrow[rr, "M"] \arrow[dr, "f"'] & & \rho \\
& \kappa \arrow[ur] &
\end{tikzcd} \tag{8}$$

where $q \notin \mathrm{FV}_\beta(f)$. Taking $f = \lambda q.M$ gives the universal such factorisation.

Remark 2.2.9. In the standard approach to associating a category to the simply-typed lambda calculus, due to Lambek and Scott [**?**, §I.11], one extends the lambda calculus to include product types and the objects of the category $\mathcal{C}_{\to,\times}$ are the types of the extended calculus (which includes an empty product $\mathbf{1}$) and the set $\mathcal{C}_{\to,\times}(\sigma,\rho)$ is a set of equivalence classes of pairs $(x : \sigma, M : \rho)$ where x is a variable and M is a term with $\mathrm{FV}(M) \subseteq \{x\}$.

The relation to the approach given above is as follows: for Q finite $\mathcal{L}_Q$ may be viewed as a polynomial category over $\mathcal{L}_\varnothing$ and if we write $\mathcal{L}_\varnothing^{\neq \mathbf{1}} \subseteq \mathcal{L}_\varnothing$ for the subcategory whose objects are types $\Phi_\to$ there is an equivalence of categories $\mathcal{C}_\to \cong \mathcal{L}_\varnothing^{\neq\mathbf{1}}$ where $\mathcal{C}_\to$ denotes the full subcategory of $\mathscr{C}_{\to,\times}$ whose objects are elements of the set $\Phi_\to$.

Definition 2.2.10 ((Translation))**.** We let

$$f_p^\Gamma : \Sigma_p^\Gamma \longrightarrow \Lambda_p^Q \tag{9}$$

denote the function defined on well-labelled preproofs by annotating the succedent of the deduction rules of Definition 2.0.1 with lambda terms so that each preproof may be read as a construction of a term:

$$\frac{}{x : p \vdash x : p}\ (\text{ax}) \tag{10}$$

$$\frac{\Gamma \vdash N : p \qquad \Delta, x : p, \Theta \vdash M : q}{\Gamma, \Delta, \Theta \vdash M[x \coloneqq N] : q}\ (\text{cut}) \tag{11}$$

$$\frac{\Gamma, x : p, y : p, \Delta \vdash M : q}{\Gamma, x : p, \Delta \vdash M[y \coloneqq x] : q}\ (\text{ctr}) \tag{12}$$

$$\frac{\Gamma, \Delta \vdash M : q}{\Gamma, x : p, \Delta \vdash M : q}\ (\text{weak}) \tag{13}$$

$$\frac{\Gamma, x : p, y : q, \Delta \vdash M : r}{\Gamma, y : q, x : p, \Delta \vdash M : r}\ (\text{ex}) \tag{14}$$

$$\frac{\Gamma, x : p, \Delta \vdash M : q}{\Gamma, \Delta \vdash \lambda x.M : p \supset q}\ (R \supset) \tag{15}$$

$$\frac{\Gamma \vdash N : p \qquad \Delta, x : q, \Theta \vdash M : r}{y : p \supset q, \Gamma, \Delta, \Theta \vdash M[x \coloneqq (y\, N)] : r}\ (L \supset) \tag{16}$$

Given a well-labelled preproof π annotated as above, $f_p^\Gamma(\pi)$ is the lambda term annotating the succedent on the root of π. If π is not well-labelled, we first α-rename as necessary using (**??**), (**??**), (**??**), (**??**) any interior equivalence class under $\approx_{str}$ to obtain a preproof π' which is well-labelled and define $f_p^\Gamma(\pi) \coloneqq f_p^\Gamma(\pi')$. This term is independent of choices made during α-renaming. We refer to $f_p^\Gamma(\pi)$ as the *translation* of π.

Lemma 2.2.11. *For any sequence Γ there is a functor $F_\Gamma : \mathcal{S}_\Gamma \longrightarrow \mathcal{L}_Q$ which is the identity on objects and which is defined on morphisms for formulas p, q by*

$$F_\Gamma(p,q) = f_{p \supset q}^\Gamma : \mathcal{S}_\Gamma(p,q) \longrightarrow \mathcal{L}_\Gamma(p,q)\,,$$
$$F_\Gamma(\mathbf{1},q) = f_q^\Gamma : \mathcal{S}_\Gamma(\mathbf{1},q) \longrightarrow \mathcal{L}_\Gamma(\mathbf{1},q)\,.$$

Proof. See [**?**, GMZ]. □

Theorem 2.2.12 (Gentzen-Mints-Zucker duality)**.** *If Γ is repetition-free then the translation functor $F_\Gamma : \mathcal{S}_\Gamma \longrightarrow \mathcal{L}_Q$ is an isomorphism of categories.*

Proof. See [18, Theorem 4.15] □

2.3 From λ-calculus to Linear Logic

The language of mathematics is constrained by the finite means we have to express it. Simultaneously, we are interested in inherently infinite structures. Modern mathematical foundations threads this needle with great success; we indulge ourselves in the hypothesis that a new variable may always be introduced and distinguished from the finite set which are currently in use. This is instilled in the assumption that an infinite set (usually taken to be countable) of variables exists, yet any individual mathematical proof contains only a finite subset of these variables. In this way, the variables used inside mathematical proof are merely *potentially infinite*.

The untyped λ-calculus (Appendix **??**) reflects this "potential infinitude": in the context of a redex $(\lambda x.M)N$ there are an *arbitrary* yet *finite* number of free occurrences of x inside M, and thus an arbitrary yet finite number of substitutions performed in the single-step β-reduction $(\lambda x.M)N \longrightarrow_\beta M[x := N]$. This also holds for the simply typed λ-calculus, however the *untyped* λ-calculus admits another dimension of potential infinitude in that there are terms whose reductions grow *arbitrarily large*, although each term itself in the reduction sequence is finite. For instance we have, where ω denotes $\lambda x.xxx$:

$$\omega\omega \longrightarrow_\beta \omega\omega\omega \longrightarrow_\beta \omega\omega\omega\omega \longrightarrow_\beta \dots$$

In the origin of Linear Logic [**?**], an important part was played by a model of untyped λ-calculus [**?**] where terms are interpreted by finite polynomial functors [**?**]. This model has been studied through the lens of categorical semantics [**?**, **?**], and plays a fundamental role in the current work around two-categorical models of Linear Logic [**?**, **?**, **?**].

In this model [**?**], Girard proves his so-called Normal Form Theorem: an equivalence between *Normal Functors* and *Analytic Functors*[1], by way of a *normal form* common to each type of functor. Exploiting this result, he constructs a model of the untyped λ-calculus which can be understood as a *categorification* of Scott domains [**?**, **?**, **?**, **?**]: instead of interpreting terms as continuous functions between directed complete partially ordered sets, he interprets them as functors commuting to certain limits (normal functors) between categories which are sufficiently *complete* (i.e. possess the corresponding limits). More precisely, a term t (equipped with a valid context $\underline{x}$) is interpreted as a normal functor $[\![\underline{x} \mid t]\!] : (\mathrm{set}^A)^n \longrightarrow \mathrm{set}^A$, where A is a fixed countably infinite set.

Within this model, however, lurks more structure than that which is reflected in the syntax of the untyped λ-calculus. A defining property of normal functors is that they are given by their restriction to *integral* functors. Though this holds for *all* normal functors, the stronger condition that a functor is defined by its restriction to its underlying sets $A \times \ldots \times A \longrightarrow \mathrm{set}^A$ only holds for *linear* normal functors. Restricting the syntax of λ-calculus to the simply typed λ-calculus (a la Church) followed by extending the syntax to notate these linear functors, leads to the logical system Linear Logic.

How exactly it is that Linear Logic is modelled by normal functors was never written down in Girard's original paper. And it turns out that the origin of Linear Logic is most of the time explained by referencing coherence space semantics [**?**, **?**, **?**], a special case of domains that is obtained as a *qualitative* version of normal functors.

The starting point of the paper ?? was the realisation that what *is* written in Girard's paper is overcomplicated. One need not consider normal functors at all, as

[1] We stress here that the notion of analytic functor as introduced by Girard differs from that introduced and studied by Joyal [**?**].

the core mathematical ideas of his work can be understood by considering the much simpler normal *functions* instead. This leads to a simplification of the normal functors model which, contrarily to coherence spaces, remains *quantitative*. At face value, this simplified model bares similarities to the weighted relational model [**?**], and also to the "weighted Scott domains" model [**?**, Section 3]. However, it is distinct from these.

2.3.1 λ-terms as normal functions

There are several dissatisfying aspects of the model given in the previous sections. Firstly, from the perspective of category theory it is unnatural to have to choose particular representatives of finite sets (the Von Neumann integers). Moreover, requiring that A is a set renders naturality of transformations between functors vacuous, as *any* collection of A-indexed functions is natural. Lastly, the preservation of wide pullbacks plays no technical role in the model *per se*: it instead provides a feature of the model which may or may not be desired.

We eliminate these aspects in the present section by constructing a simpler model. We dispose of the preservation of wide pullbacks entirely, as well as the superfluous categorical structure. In the sequel to this paper [**?**] we will show that both Girard's model (minus wide pullback preservation) and our simplified model are special cases of a family of models.

Fix a set A. Denote by $\mathcal{Q}(A)$ the set of functions $\underline{a} : A \longrightarrow \mathbb{N} \cup \{\infty\}$ and by $\mathcal{I}(A)$ the subset consisting of those $\underline{a}$ such that $\sum_{n \in \mathbb{N}} \underline{a}(n) < \infty$. The set $\mathcal{Q}(A)$ admits a partial order $\leq$ given by $\underline{a}_1 \leq \underline{a}_2$ if and only if $\forall a \in A, \underline{a}_1(a) \leq \underline{a}_2(a)$.

Definition 2.3.1. We say a function $f : \mathcal{Q}(A) \longrightarrow \mathcal{Q}(B)$ is **normal** if it is order-preserving and preserves suprema of filtered sets. That is, if $\{\underline{a}_i\}_{i \in I}$ is a filtered set of elements in $\mathcal{Q}(A)$, then $f(\sup_{i \in I}\{\underline{a}_i\}) = \sup_{i \in I}\{f(\underline{a}_i)\}$.

Observe that $\mathcal{Q}(A) \times \mathcal{Q}(A') \cong \mathcal{Q}(A \sqcup A')$ and this bijection induces a natural ordering on the left-hand side, so we can extend this definition to functions of several variables as we did in Definition 2.3.1.

While we do not have a presentation of normal functions resembling power series and therefore do not have a direct analogue of analytic functors, we can still break our functions down into finite parts in a natural way to obtain a result comparable to Theorem **??** in this simplified context.

Theorem 2.3.2. *Let $f : \mathcal{Q}(A) \longrightarrow \mathcal{Q}(B)$ be order preserving. Then f is normal if and only if for any pair $(\underline{a}, b) \in \mathcal{Q}(A) \times B$ we have*

$$f(\underline{a})(b) = \sup_{\underline{u} \in \mathcal{I}(A)} f(\underline{u})(b)\delta_{\underline{u} \leq \underline{a}} \tag{17}$$

where $\delta_{\underline{u} \leq \underline{a}}$ is equal to 1 if and only if $\underline{u} \leq \underline{a}$ and is equal to 0 otherwise.

Proof. Suppose f is normal and let $(\underline{a}, b) \in \mathcal{Q}(A) \times B$. Consider the set

$$\mathscr{X}_{\underline{a}} := \{\underline{u} \in \mathcal{I}(A) \mid \underline{u} \leq \underline{a}\} \tag{18}$$

Then $\mathscr{X}_{\underline{a}}$ is filtered with respect to the ordering on $\mathcal{I}(A)$ and $\sup \mathscr{X}_{\underline{a}} = \underline{a}$. Since f is normal, we thus have

$$f(\underline{a})(b) = f(\sup_{\underline{u}\in\mathscr{X}_{\underline{a}}} \underline{u})(b) = \sup_{\underline{u}\in\mathscr{X}_{\underline{a}}} f(\underline{u})(b) = \sup_{\underline{u}\in\mathcal{I}(A)} f(u)(b)\delta_{\underline{u}\leq\underline{a}}. \tag{19}$$

On the other hand, suppose (17) holds. Let $\{\underline{a}_i\}_{i\in I}$ be a filtered set. Then for any $b \in B$ we have

$$f(\sup_{i\in I}\{\underline{a}_i\})(b) = \sup_{\underline{u}\in\mathcal{I}(A)} \left\{f(\underline{u})(b)\delta_{\underline{u}\leq\sup_{i\in I}\{\underline{a}_i\}}\right\} \tag{20}$$

Also,

$$\sup_{i\in I}\{f(\underline{a}_i)(b)\} = \sup_{i\in I}\Big\{ \sup_{\underline{u}\in\mathcal{I}(A)} \{f(\underline{u})(b)\delta_{\underline{u}\leq\underline{a}_i}\}\Big\} \tag{21}$$

One can verify that (20) and (21) are equal by a circle of inequalities, exploiting the fact that $\underline{a} \leq \underline{a}'$ implies $\delta_{\underline{u}\leq\underline{a}} \leq \delta_{\underline{u}\leq\underline{a}'}$ for all $\underline{u}$. □

As in Section **??**, we can "curry" normal functions $f : \mathcal{Q}(A) \times \mathcal{Q}(B) \longrightarrow \mathcal{Q}(C)$ to a function $f^+ : \mathcal{Q}(A) \longrightarrow \mathcal{Q}(\mathcal{I}(B) \times C)$.

Definition 2.3.3. Let $f : \mathcal{Q}(A) \times \mathcal{Q}(B) \longrightarrow \mathcal{Q}(C)$ be arbitrary. We can define a function $f^+ : \mathcal{Q}(A) \longrightarrow \mathcal{Q}(\mathcal{I}(B) \times C)$ as follows.

$$f^+(\underline{a})(\underline{u}, c) = f(\underline{a}, \underline{u})(c) \tag{22}$$

Conversely, given arbitrary $g : \mathcal{Q}(A) \longrightarrow \mathcal{Q}(\mathcal{I}(B) \times C)$ we define $g^- : \mathcal{Q}(A) \times \mathcal{Q}(B) \longrightarrow \mathcal{Q}(C)$ as:

$$g^-(\underline{a}, \underline{b})(c) := \sup_{\underline{u}\in\mathcal{I}(B)} g(\underline{a})(\underline{u}, c)\delta_{\underline{u}\leq\underline{b}} \tag{23}$$

We note that f^+ is normal if f, and g^- is normal if g is, by an extension of Theorem 2.3.2.

Proposition 2.3.4. *Given normal functions* $f : \mathcal{Q}(A) \times \mathcal{Q}(B) \longrightarrow \mathcal{Q}(C), g : \mathcal{Q}(A) \longrightarrow \mathcal{Q}(\mathcal{I}(B) \times C)$ *we have* $(f^+)^- = f$ *and* $(g^-)^+ \geq g$.

Proof. Let $(\underline{a}, \underline{b}) \in \mathcal{Q}(A) \times \mathcal{Q}(B), c \in C$. We have:

$$\begin{aligned}(f^+)^-(\underline{a}, \underline{b})(c) &= \sup_{\underline{u}\in\mathcal{I}(B)} f^+(\underline{a})(\underline{u}, c)\delta_{\underline{u}\leq\underline{b}} \\ &= \sup_{\underline{u}\in\mathcal{I}(B)} f(\underline{a}, \underline{b})(c)\delta_{\underline{u}\leq\underline{b}} \\ &= f(\underline{a}, \underline{b})(c).\end{aligned}$$

On the other hand,

$$\begin{aligned}(g^-)^+(\underline{a})(\underline{u}, c) &= g^-(\underline{a}, \underline{u})(c) \\ &= \sup_{\underline{u}'\in\mathcal{I}(B)} g(\underline{a})(\underline{u}', c)\delta_{\underline{u}'\leq\underline{u}} \\ &\geq g(\underline{a})(\underline{b}, c).\end{aligned}$$

□

Definition 2.3.5. We define a function App : $\mathcal{Q}(\mathcal{I}(A)\times B)\times\mathcal{Q}(A)\longrightarrow\mathcal{Q}(B)$ as follows. Let $(f,\underline{a})\in\mathcal{Q}(\mathcal{I}(A)\times B)\times\mathcal{Q}(A)$ and $b\in B$.

$$\mathrm{App}(f,\underline{a})(b) = \sup_{\underline{u}\in\mathcal{I}(A)} f(\underline{u},b)\delta_{\underline{u}\leq\underline{a}} \tag{24}$$

Remark 2.3.6. Observe that for $f:\mathcal{Q}(C)\longrightarrow\mathcal{Q}(\mathcal{I}(A)\times B)$, $g:\mathcal{Q}(C)\longrightarrow\mathcal{Q}(B)$ and $\underline{c}\in\mathcal{Q}(C)$ we have

$$\mathrm{App}(f(\underline{c}),g(\underline{c})) = f^{-}(\underline{c},g(\underline{c})). \tag{25}$$

Lemma 2.3.7. *The function* App *is normal.*

Proof. We will show directly that App preserves filtered suprema. Let $\{f_i\}_{i\in I}\subseteq\mathcal{Q}(\mathcal{I}(A)\times B)$ and $\{\underline{a}_j\}_{j\in J}\subseteq\mathcal{Q}(A)$ be arbitrary filtered sets, and f, $\underline{a}$ their respective suprema. Then for any $b\in B$, we have:

$$\begin{aligned}\mathrm{App}(f,\underline{a})(b) &= \sup_{\underline{u}\in\mathcal{I}(A)} f(\underline{u},b)\delta_{\underline{u}\leq\underline{a}}\\ &= \sup_{\underline{u}\in\mathcal{I}(A)}\sup_{i\in I}\{f_i(\underline{u},b)\}\delta_{\underline{u}\leq\sup_{j\in J}\underline{a}_j}\\ &= \sup_{\underline{u}\in\mathcal{I}(A)}\sup_{i\in I,j\in J} f_i(\underline{u},c)\delta_{\underline{u}\leq\underline{a}_j}\\ &= \sup_{i\in I,j\in J}\sup_{\underline{u}\in\mathcal{I}(A)} f_i(\underline{u},c)\delta_{\underline{u}\leq\underline{a}_j},\end{aligned}$$

as required, where we have employed the fact that I,J are filtered to exchange the order of limits and that

$$\delta_{\underline{u}\leq\underline{a}} = \sup_{j\in J}\delta_{\underline{u}\leq\underline{a}_j} \tag{26}$$

for filtered J. □

2.3.2 The λ-calculus model

Now fix a countably infinite set A. Since $\mathcal{I}(A)\times A$ is also countably infinite, we can fix a choice of bijection $q:\mathcal{I}(A)\times A\longrightarrow A$. There is an induced bijection $\overline{q}:\mathcal{Q}(A)\longrightarrow\mathcal{Q}(\mathcal{I}(A)\times A)$.

Definition 2.3.8. Let $\underline{x}=\{x_1,\dots,x_n\}$ be a set of variables and let t be a λ-term for which $\underline{x}$ is a valid context (Definition **??**). We associate to each such pair $(\underline{x},t)$ a normal function $[\![\underline{x}\mid t]\!]:\mathcal{Q}(A)^n\longrightarrow\mathcal{Q}(A)$ inductively on the structure of t:

- when $t=x_i$ is a variable, $[\![\underline{x}\mid x_i]\!]:=\pi_i$;
- when $t=(t_1)t_2$ is an application, $[\![\underline{x}\mid(t_1)t_2]\!]:=\mathrm{App}\big(\langle\overline{q}[\![\underline{x}\mid t_1]\!],[\![\underline{x}\mid t_2]\!]\rangle\big)$;
- when $t=\lambda y.t'$ is an abstraction, $[\![\underline{x}\mid\lambda y.t']\!]:=\overline{q}^{-1}[\![\underline{x},y\mid t']\!]^{+}$.

Remark 2.3.9. The definition of the interpretation just shown in Definition 2.3.8 is identical to that in Definition **??** but with the ingredients on the right-hand side denoting different structures. This shows how conceptually our model is capturing the essence of Girard's.

Example 2.3.10 (Church numeral $\underline{2}$ in λ-calculus)**.** Consider the term $(f)(f)x$ in the context (f, x). Its interpretation is as follows:

$$\begin{aligned} [\![f, x \mid (f)(f)x]\!] : \mathcal{Q}(A) \times \mathcal{Q}(A) &\longrightarrow \mathcal{Q}(A) \\ (\underline{a}_1, \underline{a}_2) &\longmapsto \overline{q}^{-}\Big(\underline{a}_1, \overline{q}^{-}(\underline{a}_1, \underline{a}_2)\Big) \end{aligned}$$

The interpretation of the Church numeral $\underline{2} \coloneqq \lambda f \lambda x.(f)(f)x$ is obtained by applying $\overline{q}^{-1}$ and $(-)^{+}$ twice, but the essence of the interpretation is captured by the above.

In our model, application is interpreted by introducing a new summand in the domain (via $\overline{q}^{-}$) and then substituting the interpretation of the second term into this new summand. So, in the above, we think of the interpretation of $(f)x$ as the substitution of $\underline{a}_2$ into the new argument of $\underline{a}_1$ introduced by $\overline{q}^{-}$. Then for $(f)(f)x$, this result $(\overline{q}^{-}(\underline{a}_1, \underline{a}_2))$ is substituted into the new argument of $\underline{a}_1$ introduced by the outermost $\overline{q}^{-}$.

Lemma 2.3.11 (Substitution Lemma)**.** *Let t, s be λ-terms and $\underline{x} = \{x_1, \dots, x_n\}$ be a collection of variables and y another variable so that $\underline{x} \cup \{y\}$ is a valid context for t and $\underline{x}$ is a valid context for s. Then for any $\alpha \in \mathcal{Q}(A)^n$ we have*

$$[\![\underline{x} \mid t[y \coloneqq s]]\!](\alpha) = [\![\underline{x}, y \mid t]\!](\alpha, [\![\underline{x} \mid s]\!](\alpha)) \tag{27}$$

Proof. We proceed by induction on the structure of the term t. We notice that the case where t is a variable is trivial.

Say $t = (t_1)t_2$ is an application. First, we have the following, where $(\alpha, \underline{a}) \in \mathcal{Q}(A)^n \times \mathcal{Q}(A)$, note that we suppress the contexts to ease notation.

$$[\![(t_1)t_2]\!](\alpha, \underline{a}) = \mathrm{App}\left(\overline{q}[\![t_1]\!](\alpha, \underline{a}), [\![t_2]\!](\alpha, \underline{a})\right) \tag{28}$$

On the other hand,

$$\begin{aligned} [\![(t_1[y \coloneqq s])(t_2[y \coloneqq s])]\!](\alpha) &= \mathrm{App}(\overline{q}[\![t_1[y \coloneqq s]]\!](\alpha), [\![t_2[y \coloneqq s]]\!](\alpha)) \\ &= \mathrm{App}(\overline{q}[\![t_1]\!](\alpha, [\![s]\!](\alpha)), [\![t_2]\!](\alpha, [\![s]\!](\alpha))) \end{aligned}$$

where in the final line we have used the inductive hypothesis.

Say $t = \lambda y'.t'$ is an abstraction. We have, where $(\alpha, \underline{a}) \in \mathcal{Q}(A)^n \times \mathcal{Q}(A)$:

$$[\![\underline{x}, y \mid \lambda y'.t]\!](\alpha, \underline{a}) = \overline{q}^{-1}[\![\underline{x}, y, y' \mid t']\!]^{+}(\alpha, \underline{a}) \tag{29}$$

On the other hand, we have for $\alpha \in \mathcal{Q}(A)^n$ and $c \in A$ the following (assume $q^{-1}(c) = (\underline{c}', c''))$.

$$\begin{aligned}
[\![\underline{x}, y \mid \lambda y'.t[y := s]]\!](\alpha)(c) &= \big(\overline{q}^{-1}[\![\underline{x}, y, y' \mid t'[y := s]]\!]^{+}\big)(\alpha)(c) \\
&= [\![\underline{x}, y, y' \mid t'[y := s]]\!]^{+}(\alpha)(\underline{c}', c'') \\
&= \sup\nolimits_{u \in \mathcal{I}(A)^n} [\![\underline{x}, y, y' \mid t'[y := s]]\!](u, \underline{c}')(c'')\delta_{u \leq \alpha} \\
&= \sup\nolimits_{u \in \mathcal{I}(A)^n} [\![\underline{x}, y, y' \mid t']\!](u, [\![\underline{x} \mid s]\!](u), \underline{c}')(c'')\delta_{u \leq \alpha} \\
&= [\![\underline{x}, y, y' \mid t']\!]^{+}(\alpha, [\![\underline{x} \mid s]\!](\alpha), \underline{c}')(c'') \\
&= \overline{q}^{-1}[\![\underline{x}, y, y' \mid t']\!]^{+}(\alpha, [\![\underline{x} \mid s]\!])(c)
\end{aligned}$$

where we have used the inductive hypothesis in the fourth line. □

Theorem 2.3.12. *The interpretation given in Definition 2.3.8 is a denotational model of the λ-calculus. That is, if t is a λ-term and $\underline{x}$ a valid context for t and for s, then we have the following equality*

$$[\![\underline{x} \mid (\lambda y.t)s]\!] = [\![\underline{x} \mid t[y := s]]\!] \tag{30}$$

Proof. By the substitution Lemma 2.3.11 we have for $\alpha \in \mathcal{Q}(A)^n$:

$$[\![\underline{x} \mid t[y := s]]\!](\alpha) = [\![\underline{x}, y \mid t]\!](\alpha, [\![\underline{x} \mid s]\!](\alpha)) \tag{31}$$

On the other hand, we have

$$\begin{aligned}
[\![\underline{x} \mid (\lambda y.t)s]\!](\alpha) &= \mathrm{App}(\big\langle(\overline{qq}^{-1}[\![\underline{x}, y \mid t]\!]^{+}), [\![\underline{x} \mid s]\!]\big\rangle)(\alpha) \\
&= ([\![\underline{x}, y \mid t]\!]^{+})^{-}(\alpha, [\![\underline{x} \mid s]\!](\alpha)) \\
&= [\![\underline{x}, y \mid t]\!](\alpha, [\![\underline{x} \mid s]\!](\alpha))
\end{aligned}$$

which concludes the proof. □

2.3.3 Linear proofs as linear functions

This model of the untyped λ-calculus is trivially a model of the simply-typed λ-calculus, but as suggested by the notation in the previous section, we can extend our model to a model of Linear Logic by decomposing the arrow type constructor $A \to A$ to $!A \multimap A$.

Recall that for a set A, $\mathcal{Q}(A)$ contains all functions $f : A \longrightarrow \overline{\mathbb{N}}$. Considering $\overline{\mathbb{N}}$ as a set equipped with the operation of natural number addition (extended in the intuitive way to include ∞), the set $\mathcal{Q}(A)$ with its point-wise addition inherits a commutative monoid structure.

Definition 2.3.13. Given an element $a \in A$, let $\delta_a \in \mathcal{Q}(A)$ be the function for which $\delta_a(a')$ evaluates to 1 if $a = a'$ and to 0 otherwise.

We say a function $f : \mathcal{Q}(A) \longrightarrow \mathcal{Q}(B)$ is **linear** if

$$f(\underline{a})(b) = \sum_{a \in A} \underline{a}(a) f(\delta_a)(b).$$

Given sets $A_1, \dots, A_n, B$, a function $f : \prod_{i=1}^n \mathcal{Q}(A_i) \longrightarrow \mathcal{Q}(B)$ is **multilinear** if it is linear in each argument (equivalently, if the function $\mathcal{Q}(A_1 \times \cdots \times A_n) \longrightarrow \mathcal{Q}(B)$ is linear). We denote the set of such functions $\mathrm{Lin}(\prod_{i=1}^n \mathcal{Q}(A_i), \mathcal{Q}(B))$.

Suppose we have a function $f : \mathcal{Q}(A) \times \mathcal{Q}(B) \longrightarrow \mathcal{Q}(C)$ which is linear in the variable $\mathcal{Q}(B)$. Then for any $\underline{a} \in \mathcal{Q}(A)$ and $\underline{b} \in \mathcal{Q}(B)$ we have

$$f(\underline{a}, \underline{b}) = f\left(\underline{a}, \sum_{b \in B} \underline{b}(b) \cdot \delta_a\right) = \sum_{b \in B} \underline{b}(b) \cdot f(\underline{a}, \delta_b) \tag{32}$$

We define $f^\times : \mathcal{Q}(A) \longrightarrow \mathcal{Q}(B \times C)$ as follows, where $\underline{a} \in \mathcal{Q}(A), (b, c) \in B \times C$:

$$f^\times(\underline{a})(b, c) = f(\underline{a}, \delta_b)(c) \tag{33}$$

Conversely, given a linear function $g : \mathcal{Q}(A) \longrightarrow \mathcal{Q}(B \times C)$ we define $g^\div : \mathcal{Q}(A) \times \mathcal{Q}(B) \longrightarrow \mathcal{Q}(C)$ as follows, where $(\underline{a}, \underline{b}) \in \mathcal{Q}(A) \times \mathcal{Q}(B), c \in C$:

$$g^\div(\underline{a}, \underline{b})(c) = \sum_{b \in B} \underline{b}(b) \cdot g(\underline{a})(b, c) \tag{34}$$

Clearly, if $f : \mathcal{Q}(A) \times \mathcal{Q}(B) \longrightarrow \mathcal{Q}(C)$ is linear in the final argument, then $(f^\times)^\div = f$. Conversely, for any $g : \mathcal{Q}(A) \longrightarrow \mathcal{Q}(B \times C)$ then $(g^\div)^\times = g$. We have proven:

Proposition 2.3.14. *There exists a bijection*

$$\mathrm{Lin}(\mathcal{Q}(A) \times \mathcal{Q}(B), \mathcal{Q}(C)) \longrightarrow \mathrm{Lin}(\mathcal{Q}(A), \mathcal{Q}(B \times C)). \tag{35}$$

Remark 2.3.15. We remark that a *normal* function $f : \mathcal{Q}(A) \longrightarrow \mathcal{Q}(B)$ is determined by its restriction to the domain $\mathcal{I}(A) \longrightarrow \mathcal{Q}(B)$, whereas if f is *linear* then it is determined by its restriction to the domain $A \longrightarrow \mathcal{Q}(B)$ (after identifying $a \in A$ with δ_a).

Definition 2.3.16. We define a function

$$\begin{aligned} \mathrm{LinApp}_{A,B} : \mathcal{Q}(A \times B) \times \mathcal{Q}(A) &\longrightarrow \mathcal{Q}(B) \\ (f, \underline{a}) &\longmapsto \sum_{a \in A} \underline{a}(a) \cdot f(a, -) \end{aligned}$$

Lemma 2.3.17. *The function* $\mathrm{LinApp}_{A,B}$ *is multilinear.*

Proof. This is a calculation, let $(f, \underline{a}), (f', \underline{a}') \in \mathcal{Q}(A \times B) \times \mathcal{Q}(B)$. Then:

$$\begin{aligned} \mathrm{LinApp}_{A,B}\left(f + f', \underline{a} + \underline{a}'\right) &= \sum_{a \in A} (\underline{a} + \underline{a}')(a) \cdot (f + f')(a, -) \\ &= \sum_{a \in A} (\underline{a}(a) + \underline{a}'(a)) \cdot (f(a, -) + f'(a, -)) \\ &= \mathrm{LinApp}_{A,B}(f, \underline{a}) + \mathrm{LinApp}_{A,B}(f, \underline{a}') \\ &\qquad + \mathrm{LinApp}_{A,B}(f', \underline{a}) + \mathrm{LinApp}_{A,B}(f', \underline{a}') \end{aligned}$$

□

3 Multiplicative Exponential Linear Logic (Sequent Calculus)

Definition 3.0.1. There is an infinite set of **unoriented atoms** $X, Y, Z, ...$ and an **oriented atom** (or **atomic proposition**) is a pair $(X, +)$ or $(X, -)$ where X is an unoriented atom. The set of **pre-formulas** is defined as follows.

- Any atomic proposition is a pre-formula.
- If A, B are pre-formulas then so are $A \otimes B$, $A \parr B$.
- If A is a pre-formula then so is $\neg A$.
- If A is a pre-formula then so are $\neg A, !A, ?A$.

The set of **formulas** is the quotient of the set of pre-formulas by the equivalence relation $\sim$ generated by, for arbitrary formulas A, B and unoriented atom X, the following.

$$\neg(A \otimes B) = \neg B \parr \neg A, \quad \neg(A \parr B) = \neg B \otimes A, \quad \neg(X, x) = (X, \overline{x})$$
$$\neg !A = ?\neg A, \quad \neg ?A = !\neg A$$

Remark 3.0.2. In [20] we define $\neg(A \otimes B)$ to be $\neg B \parr \neg A$, that is, the order of A and B is swapped by the negation. Here we do *not* swap the order so that Geometry of Interaction One (Theorem 4.6.7) is more transparent.

Lemma 3.0.3. *For all formulas A we have $\neg\neg A = A$.*

Definition 3.0.4. A finite sequence of formulas is a **sequent** and we write $\vdash A_1, ..., A_n$ for the sequent $(A_1, ..., A_n)$.

Definition 3.0.5. A **multiplicative, exponential, linear logic deduction rule** (or simply **deduction rule**) results from one of the schemata below by a substitution of the following kind: replace A, B by arbitrary formulas, and $\Gamma, \Gamma', \Delta, \Delta'$ by arbitrary (possibly empty) sequences of formulas separated by commas:

- the **identity group**:
  - **Axiom**:

$$\frac{}{\vdash \neg A, A}\ (\text{ax})$$

  - **Cut**:

$$\frac{\vdash \Gamma, A, \Gamma' \qquad \vdash \Delta, \neg A, \Delta'}{\vdash \Gamma, \Gamma', \Delta, \Delta'}\ (\text{cut})$$

- the **multiplicative rules**:

  - **Times**:

$$\frac{\vdash \Gamma, A, \Gamma' \qquad \vdash \Delta, B, \Delta'}{\vdash \Gamma, \Gamma', A \otimes B, \Delta, \Delta'} \otimes$$

  - **Par**:

$$\frac{\vdash \Gamma, A, B, \Gamma'}{\vdash \Gamma, A \parr B, \Gamma'} \parr$$

- the **structural rule**:

  - **Exchange**:

$$\frac{\vdash \Gamma, A, B, \Gamma'}{\vdash \Gamma, B, A, \Gamma'} \text{(ex)}$$

- the **exponential rules**:

  - **Dereliction**:

$$\frac{\vdash \Gamma, A}{\vdash \Gamma, ?A} \text{(der)}$$

  - **Promotion**

$$\frac{\vdash ?\Gamma, A}{\vdash ?\Gamma, !A} \text{(prom)}$$

  - **Weakening**

$$\frac{\vdash \Gamma}{\vdash ?A, \Gamma} \text{(weak)}$$

  - **Contraction**

$$\frac{\vdash \Gamma, ?A, ?A}{\vdash \Gamma ?A} \text{(ctr)}$$

Definition 3.0.6. A **proof in MELL** is a finite, rooted, planar, tree where each edge is labelled by a sequent and each node except for the root is labelled by a valid deduction rule. If the edge connected to the root is labelled by the sequent $\vdash \Gamma$ then we call the proof a **proof of** Γ and in such a situation, Γ is the **conclusion** of π.

Example 3.0.7. Church numeral 2

3.1 Proof nets

A proof in MELL is a highly bureaucratic in that every inconsequential decision is written down explicitly. For example, there is surely no difference from the perspective of logical reasoning between a proof which makes use of the following two substructures:

$$\dfrac{\dfrac{\vdash ?A, ?A, ?B, ?B}{\vdash ?A, ?B, ?B}\,(\mathrm{ctr})}{\vdash ?A, ?B}\,(\mathrm{ctr}) \qquad \dfrac{\dfrac{\vdash ?A, ?A, ?B, ?B}{\vdash ?A, ?A, ?B}\,(\mathrm{ctr})}{\vdash ?A, ?B}\,(\mathrm{ctr})$$

Enumerating all such redundancies is a labour intensive task, this was done for the Intuitionistic Sequent Calculus (implicative fragment) in [18].

To establish a framework where we only work with proofs in MELL up to this bureaucracy and simultaneously avoid labouriously working with equivalence classes, we introduce a new syntax for proofs.

First, we recall the definition of a directed multigraph.

Definition 3.1.1. A **directed multigraph** is a triple (V, E, φ) where:

- V is a set of **vertices**, or **nodes**.
- E is a set of **edges**, or **lines**.
- $r : E \longrightarrow \{(x, y) \mid x, y \in V\}$ is a function from the set of edges to the set of ordered pairs of vertices.

For all edges $e \in E$, the first element of $r(e)$ is the **source** and the second element is the **target**.

The following method for writing certain equivalence classes of proofs with a single calculus is due to Girard [1]. See [16] for his own explanation of how one may think of this graphical syntax. This particular presentation of proof structures is due to Laurent [19].

Definition 3.1.2. A **proof structure** is a directed multigraph with edges labelled by formulas and with vertices labelled by $(\mathrm{ax}), (\mathrm{cut}), \otimes, \parr, !, ?, \mathrm{ctr}, \mathrm{wk}, \mathrm{pax}$ or c. The incoming edges of a vertex are called its **premises**, the outgoing edges are its **conclusions**. Proof structures are required to adhere to the following conditions:

- Each vertex labelled (ax) has exactly two conclusions and no premise, the conclusions are labelled A and $\neg A$ for some A. We call this an **axiom link**.
- Each vertex labelled (cut) has exactly two premises and no conclusion, where the premises are labelled A and $\neg A$ for some A. We call this a **cut link**.
- Each vertex labelled $\otimes$ has exactly two premises and one conclusion. The premises are ordered, the smallest one is called the **left** premise of the vertex, the biggest one is called the **right** premise. The left premise is labelled A, the right premise is labelled B and the conclusions is labelled $A \otimes B$, for some A, B. We call this a **tensor link**.

- Each vertex labelled $\parr$ has exactly two ordered premises and one conclusion. The left premise is labelled A, the right premise is labelled B and the conclusion is labelled $A \parr B$, for some A, B. We call this a **par link**.

- Each vertex labelled ctr has exactly two premises and one conclusion. The left premise, the right premise, and the conclusion are all labelled $?A$ for some A. We call this a **contraction link**.

- Each vertex labelled pax has exactly one premise and one conclusion. The premise and conclusion are both labelled $?A$ for some formula A. We call this a **pax link**. Pax links are only allowed to exist when they are associated with promotion links, see the following clause.

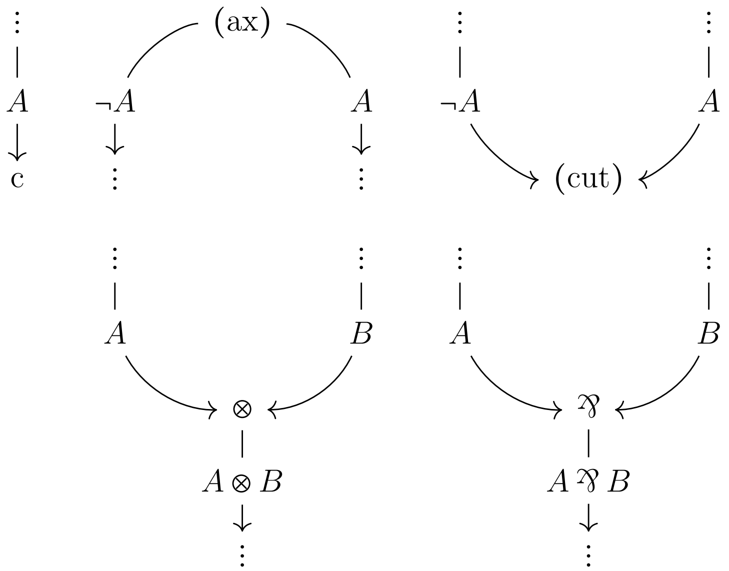
- Each vertex labelled ! has exactly one premise and one conclusion. The premise is labelled A for some A, and the conclusion by $!A$. We call this a **promotion link**. Each promotion link must come equipt with a selection of the pax links so that everything lying above these pax links and the promotion link itself form a proof structure, when these pax and promotion links are replaced with conclusion links.

- Each vertex labelled weak has no premises and one conclusion. The conclusion is labelled $?A$ for some A. We call this a **weakening link**.

- Each vertex labelled ? has exactly one premise and one conclusion. The premise is labelled A for some A, and the conclusion by $?A$. We call this a **dereliction link**.

- Each vertex labelled c has exactly one premise and no conclusion. Such a premise of a vertex labelled c is called a **conclusion** of the proof structure.

Let π be a proof structure. A **conclusion link** consists of a node labelled c along with its premise. An **axiom link** of π is a subgraph consisting of a node labelled (ax) along with its conclusions. A (cut) link consists of a node labelled (cut) along with its premises. A **tensor link** of π consists of a node labelled $\otimes$ along with its premises and conclusion. A **par link** consists of a node labelled $\parr$ along with its premises and conclusion. Missing: Exponential links



Definition 3.1.3. An **occurrence of a formula** A in a proof structure π is an edge e labelled by A.

We motivated proof nets as a less bureaucratic way of dealing with proofs. Loosely speaking, there is orthogonal to this though, is a concept which exists for proof structures which does *not* exist for proofs in MELL. Whilst every proof in MELL is a valid proof, the valid proof structures exist as a proper subset of the broader class of proof structures which may be valid or invalid.

Definition 3.1.4. Let Σ denote the set of MLL proofs and MPS the set of multiplicative proof structures. We let $T : \Sigma \longrightarrow \text{MPS}$ denote the function defined inductively by associating to each deduction rule of Definition 3.0.5 a multiplicative proof structure. More precisely, we simultaneously inductively prove that if π has height n and is constructed from either one proof π' with height less than n or from two proofs π_1, π_2 each with height less than n, then $T(\pi'), T(\pi_1), T(\pi_2)$ have conclusions corresponding to the conclusions of π', π_1, π_2, and we use this fact to inductively define $T(\pi)$ which in turn has conclusions corresponding to the formulas in the final sequent of π.

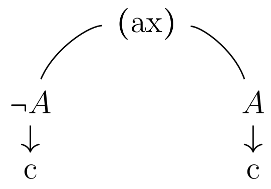
Given a proof π, the following notation:

$$\begin{tikzcd} T(\pi) \arrow[d, dash] \\ A \end{tikzcd} \tag{36}$$

means the translation $T(\pi)$, which admits a conclusion A, with the conclusion node c removed. Reformatting needed, and exponential fragment needed

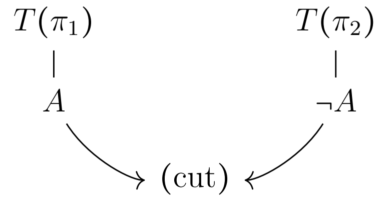
Axiom

$$\dfrac{}{\vdash A, \neg A}\,(\mathrm{ax}) \quad \xrightarrow{T}$$



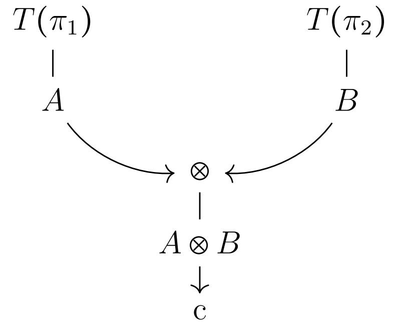
Cut

$$\dfrac{\begin{matrix}\pi_1\\ \vdots\\ \vdash \Gamma, A, \Gamma'\end{matrix}\qquad \begin{matrix}\pi_2\\ \vdots\\ \vdash \Delta, \neg A, \Delta'\end{matrix}}{\vdash \Gamma, \Gamma', \Delta, \Delta'}\,(\mathrm{cut}) \quad \xrightarrow{T}$$



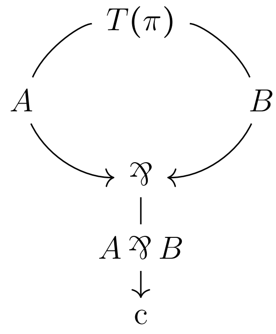
Times

$$\dfrac{\begin{matrix}\pi_1\\ \vdots\\ \vdash \Gamma, A, \Gamma'\end{matrix}\qquad \begin{matrix}\pi_2\\ \vdots\\ \vdash \Delta, B, \Delta'\end{matrix}}{\vdash \Gamma, \Gamma', A \otimes B, \Delta, \Delta'}\,\otimes \quad \xrightarrow{T}$$



Par

$$\dfrac{\begin{matrix}\pi\\ \vdots\\ \vdash \Gamma, A, B, \Gamma'\end{matrix}}{\vdash \Gamma, A \parr B, \Gamma'}\,\parr \quad \xrightarrow{T}$$



Exchange

$$\dfrac{\begin{matrix}\pi\\ \vdots\\ \vdash \Gamma, A, B, \Gamma'\end{matrix}}{\vdash \Gamma, B, A, \Gamma'}\,(\mathrm{ex}) \quad \xrightarrow{T} \quad T(\pi)$$

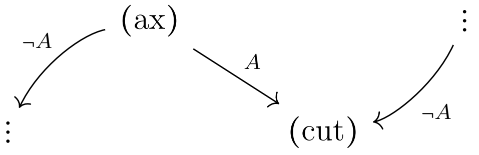
A **multiplicative proof net** (or simply **proof net**) is a multiplicative proof structure which lies in the image of T.

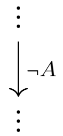
3.2 The dynamics of MELL

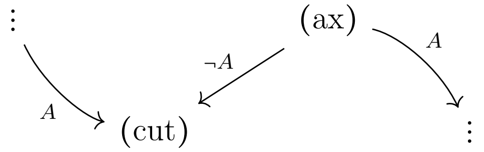
Linear logic is a *dynamic* system, in that it involves a proof *re-write* procedure. This procedure is the *cut-elimination* process and constitutes the content of this section.

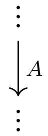
Definition 3.2.1.

- *a*-**reduction**. A subgraph of the form given by the first of these two diagrams is an *a*-redex.

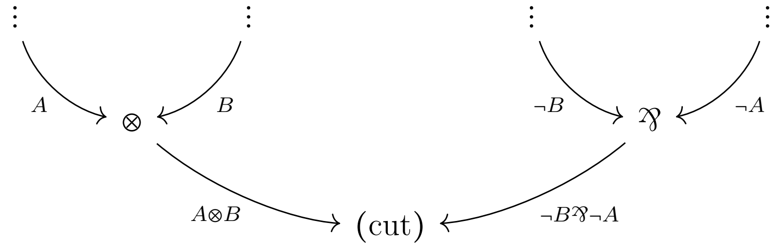


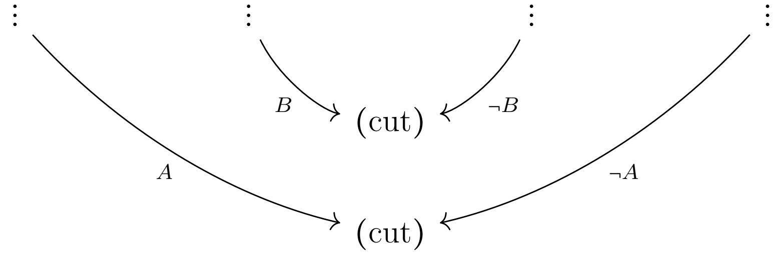




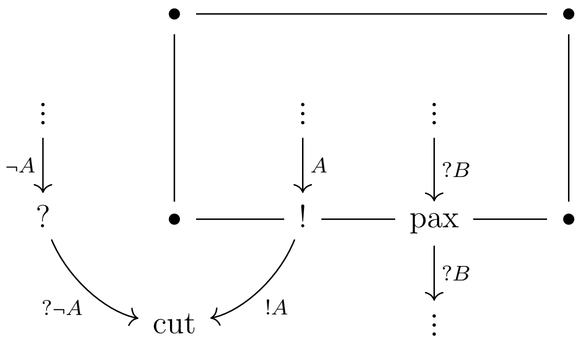


- $\otimes/⅋$-**reduction**. A subgraph of the form given by the first of these two diagrams is an m-redex.

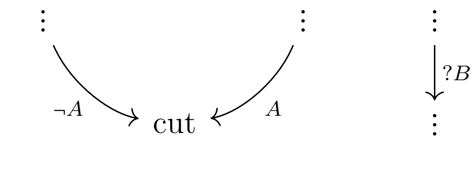




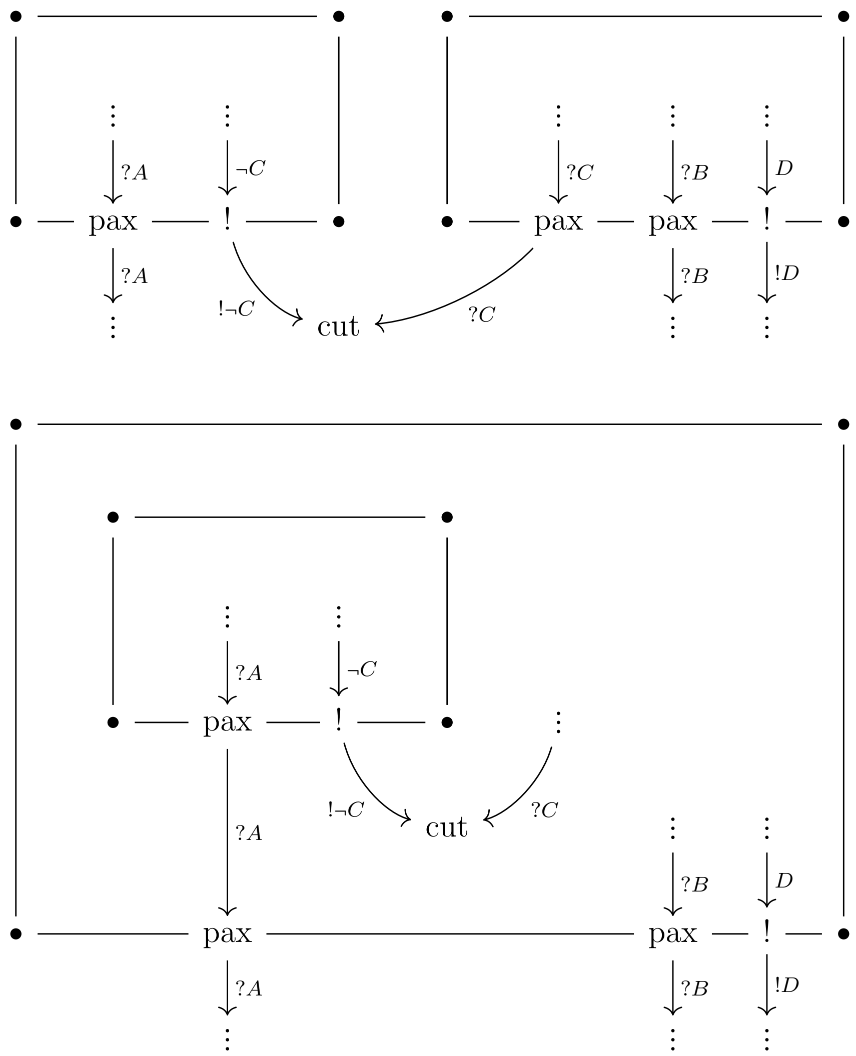
- **!/?-reduction**. A subgraph of the form given by the first of these two diagrams is a d-redex (as a dereliction link vanishes). Only one pax-link has been drawn in the diagram, but arbitrarily many may be present.



(37)

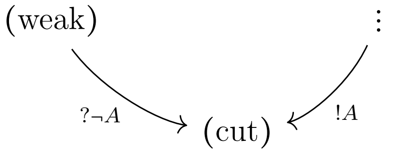


- !/ pax**-reduction**. A subgraph in the form of the first of these diagrams is a p-redex. For this rule, n and/or m may be equal to 0. Again, for succinctness, we have only drawn the situation with limited pax-links, but arbitrarily many may be present.



(38)

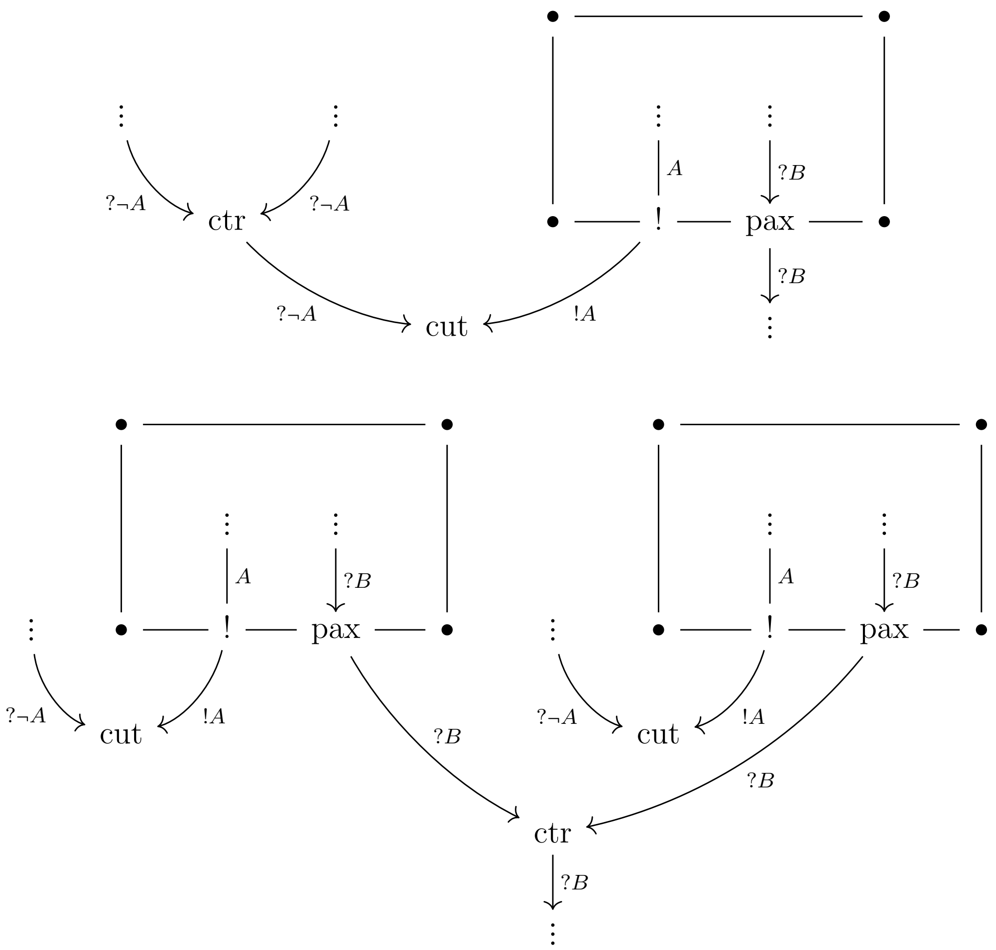
- !/(weak)**-reduction**. A subgraph in the form of the the following diagram is a w-redex, as a weakening is erased. The rule is that w-redexes can be erased completely.



(39)

- !/(ctr)**-reduction**. A subgraph in the form of the first of these diagrams is a

c-redex, as it features contraction, and also because data is copied.



(40)

A **reduction** is a pair of proof structures (π, π') where π' is the result of applying one of the reduction rules just described to π. We write $\pi \longrightarrow_{(\mathrm{cut})} \pi'$ when (π, π') is a reduction.

3.3 Linear Logic proofs as normal functions

We return to Section ? and extend our model of λ-calculus terms as normal functions to all of MELL.

Definition 3.3.1. We choose, for each atomic formula X, a set which we denote $\underline{X}$. For a formula, we define the interpretation inductively via the rules:

$$\underline{X \otimes Y} = \underline{X \multimap Y} = \underline{X} \times \underline{Y}, \qquad \underline{!A} = \mathcal{I}(A). \tag{41}$$

We will interpret a proof π of a sequent $A_1, \dots, A_n \vdash B$ as a multilinear function $\mathcal{Q}(\underline{A_1}) \times \cdots \times \mathcal{Q}(\underline{A_n}) \longrightarrow \mathcal{Q}(\underline{B})$.

Definition 3.3.2. We construct the translation of proofs to functions by induction on the structure of the proof. Let $d_A : \mathcal{Q}(\mathcal{I}(A)) \longrightarrow \mathcal{Q}(A)$ be the map sending $\delta_{\underline{a}}$ to $\sum_{a\in A} \underline{a}(a)\delta_a$, extended linearly. Similarly, let $\bar{d}_A : \mathcal{Q}(A) \longrightarrow \mathcal{Q}(\mathcal{I}(A))$ be the morphism that maps δ_a to δ_{δ_a}, extended linearly. We will also employ the diagonal map $\Delta_A : \mathcal{Q}(A) \longrightarrow \mathcal{Q}(A) \times \mathcal{Q}(A)$ and the swap map $s_A : \mathcal{Q}(A) \times \mathcal{Q}(A) \longrightarrow \mathcal{Q}(A) \times \mathcal{Q}(A)$. Throughout, when a composition symbol carries a subscript, this indicates the formula corresponding to the argument at which to compose.

- if π consists of a single axiom rule:

$$\dfrac{}{X \vdash X}\,(\mathrm{ax}),$$

  then $[\![\pi]\!] = \mathrm{id}_{\mathcal{Q}(\underline{X})}$;

- if π ends with a cut rule:

$$\dfrac{\begin{array}{c}\vdots\ \pi_1\\ \Gamma \vdash A\end{array}\quad \begin{array}{c}\vdots\ \pi_2\\ \Delta, A, \Delta' \vdash B\end{array}}{\Gamma, \Delta, \Delta' \vdash B}\,(\mathrm{cut}),$$

  then $[\![\pi]\!] = [\![\pi_2]\!] \circ_A [\![\pi_1]\!]$;

- if π ends with a left tensor rule:

$$\dfrac{\begin{array}{c}\vdots\ \pi'\\ \Gamma, A, B, \Delta \vdash C\end{array}}{\Gamma, A \otimes B, \Delta, \vdash C}\,(\mathrm{L}\otimes),$$

  then $[\![\pi]\!] := [\![\pi']\!]$ up to identifying multilinear maps out of $\mathcal{Q}(A) \times \mathcal{Q}(B)$ with linear maps out of $\mathcal{Q}(A \times B)$;

- if π ends with a right tensor rule:

$$\dfrac{\begin{array}{c}\vdots\ \pi_1\\ \Gamma \vdash A\end{array}\quad \begin{array}{c}\vdots\ \pi_2\\ \Delta \vdash B\end{array}}{\Gamma, \Delta \vdash A \otimes B}\,(\mathrm{R}\otimes),$$

  then $[\![\pi]\!](a, b) := [\![\pi_1]\!](a) \times [\![\pi_2]\!](b)$;

- if π ends with a right linear arrow rule:

$$\dfrac{\begin{array}{c}\vdots\ \pi'\\ \Gamma, A, \Delta \vdash B\end{array}}{\Gamma, \Delta \vdash A \multimap B}\,(\mathrm{R}\multimap),$$

  then $[\![\pi]\!] := [\![\pi']\!]^{\times}$;

- if π ends with a left linear arrow rule:

$$\dfrac{\overset{\vdots\;\pi_1}{\Gamma \vdash A} \qquad \overset{\vdots\;\pi_2}{B, \Delta \vdash C}}{A \multimap B, \Gamma, \Delta \vdash C}\,(\mathrm{L} \multimap),$$

  then for $a \in A$, $\llbracket \pi \rrbracket (f, \alpha, \beta) = \llbracket \pi_2 \rrbracket \big(\beta, \mathrm{LinApp}_{\underline{A},\underline{B}}(f, \llbracket \pi_1 \rrbracket(\alpha))\big)$;

- if π ends with a dereliction rule

$$\dfrac{\overset{\vdots\;\pi'}{\Gamma, A, \Gamma' \vdash \Delta}}{\Gamma, !A, \Gamma' \vdash \Delta}\,(\mathrm{der}),$$

  then $\llbracket \pi \rrbracket := \llbracket \pi' \rrbracket \circ_A d_A$,

- if π ends with a promotion rule

$$\dfrac{\overset{\vdots\;\pi'}{!\Gamma \vdash A}}{!\Gamma \vdash !A}\,(\mathrm{Prom}),$$

  then $\llbracket \pi \rrbracket := \bar{d}_A \circ \llbracket \pi' \rrbracket$,

- if π ends with a contraction rule

$$\dfrac{\overset{\vdots\;\pi'}{\Gamma, !A, !A \vdash B}}{\Gamma, !A \vdash B}\,(\mathrm{ctr}),$$

  then $\llbracket \pi \rrbracket = \llbracket \pi' \rrbracket \circ_{!A,!A} \Delta_{\underline{A}}$,

- if π ends with a weakening rule

$$\dfrac{\overset{\vdots\;\pi'}{\Gamma \vdash B}}{\Gamma, !A \vdash B}\,(\mathrm{weak}),$$

  then $\llbracket \pi \rrbracket (\underline{a}_1, \ldots, \underline{a}_n, \underline{a}) = \llbracket \pi' \rrbracket (\underline{a}_1, \ldots, \underline{a}_n)$,

- if π ends with an exchange rule

$$\dfrac{\overset{\vdots\;\pi'}{\Gamma, A, B, \Delta \vdash C}}{\Gamma, B, A, \Delta \vdash C}\,(\mathrm{ex}),$$

  then $\llbracket \pi \rrbracket := \llbracket \pi' \rrbracket \circ_{A,B} s_{\underline{B},\underline{A}}$.

Example 3.3.3 (Church numeral $\underline{2}_A$ in Linear Logic)**.** Consider the Church numeral $\underline{2}_A$ (without the penultimate right implication rules).

$$\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A \qquad \dfrac{A \vdash A \qquad A \vdash A}{A \multimap A, A \vdash A}\,\mathrm{L}\multimap}{A \multimap A, A \multimap A, A \vdash A}\,\mathrm{L}\multimap}{!(A \multimap A), A \multimap A, A \vdash A}\,\mathrm{Der}}{!(A \multimap A), !(A \multimap A), A \vdash A}\,\mathrm{Der}}{!(A \multimap A), A \vdash A}\,\mathrm{Ctr}$$

The interpretation of this is given as follows

$$\begin{aligned} \mathcal{Q}(\mathcal{I}(A \times A)) \times \mathcal{Q}(A) &\longrightarrow \mathcal{Q}(A) \\ (f, \underline{a}) &\longmapsto \mathrm{LinApp}\big(d_{A\multimap A}(f), \mathrm{LinApp}(d_{A\multimap A}(f), \underline{a})\big) \end{aligned}$$

Recall that composition is inside the Kleisli category of $\mathcal{Q}$, so $\mathrm{LinApp}(d_{A\multimap A}(f), \underline{a})$ for example is given as follows

$$\mathrm{LinApp}(d_{A\multimap A}(f), \underline{a}) = \sum_{\alpha \in A \multimap A} \sum_{a \in A} f(\alpha)\underline{a}(a) \cdot \alpha(a, -) \tag{42}$$

So the interpretation of $\underline{2}_A$ ultimately is

$$\sum_{\alpha, \alpha' \in A \multimap A} \sum_{a, a' \in A} f(\alpha) f(\alpha') \underline{a}(a) \underline{a}(a') \cdot \alpha'(a', (\alpha(a, -))) \tag{43}$$

Theorem 3.3.4. *Definition 3.3.2 gives a model of intuitionistic Linear Logic. That is, if π_1 and π_2 are* (cut)*-equivalent proofs, then*

$$[\![\pi_1]\!] = [\![\pi_2]\!] \tag{44}$$

Proof. We go through each (cut)-elimination rule methodically and prove invariance of the interpretations under these transformations.

Say $\gamma : \pi \longrightarrow \pi'$ is a reduction. If this reduction is either **anything**/(ax) or (ax)/**anything** then the constructions of $[\![\pi]\!]$ and $[\![\pi']\!]$ differ only by composition with an identity morphism, and so clearly $[\![\pi]\!] = [\![\pi']\!]$.

The cases of (R ⊗)/(L ⊗), **anything**/(ctr), (prom)/(weak) are similarly trivial. The interesting cases are (prom)/(der) and (R ⊸)/(L ⊸). First we consider (prom)/(der). The two interpretations are respectively

$$[\![\pi']\!] \circ_A d_A \circ_{!A} \bar{d}_A \circ [\![\pi]\!], \qquad [\![\pi']\!] \circ_A [\![\pi]\!] \tag{45}$$

So it suffices to show that $d_A \circ \bar{d}_A = \mathrm{id}_{\mathcal{Q}(\mathcal{I}(A))}$. It suffices to check this on elements of the form δ_a, and indeed

$$d_A(\bar{d}_A(\delta_a)) = d_A(\delta_{\delta_a}) = \delta_a$$

is the identity, as required.

Next we consider (R $\multimap$)/(L $\multimap$). The two interpretations are respectively

$$\begin{aligned} &\prod_{i=1}^{n} \mathcal{Q}(A_i) \times \prod_{i=1}^{m} \mathcal{Q}(B_i) \times \prod_{i=1}^{k} \mathcal{Q}(C_i) \longrightarrow \mathcal{Q}(C) \\ &(\alpha, \beta, \gamma) \longmapsto [\![\pi'']\!](\mathrm{LinApp}([\![\pi]\!]^{\times}(\alpha), [\![\pi']\!](\beta))) \end{aligned}$$

and

$$\begin{aligned} &\prod_{i=1}^{n} \mathcal{Q}(A_i) \times \prod_{i=1}^{m} \mathcal{Q}(B_i) \times \prod_{i=1}^{k} \mathcal{Q}(C_i) \longrightarrow \mathcal{Q}(C) \\ &(\alpha, \beta, \gamma) \longmapsto [\![\pi'']\!]([\![\pi]\!](\alpha, [\![\pi']\!](\beta))) \end{aligned}$$

So it suffices to show that for a general $g : \mathcal{Q}(A) \times \mathcal{Q}(C) \longrightarrow \mathcal{Q}(B)$ which is linear in $\mathcal{Q}(A)$, we have

$$\mathrm{LinApp}(g^{\times}(\underline{c}), \underline{a}) = g(\underline{a}, \underline{c}) \tag{46}$$

This follows from the following calculation.

$$\begin{aligned} \mathrm{LinApp}(g^{\times}(\underline{c}, \underline{a})) &= \sum_{a \in A} g^{\times}(\underline{c})(a, -) \\ &= \sum_{a \in A} \underline{a}(a) g(\delta_a, \underline{c})(-) \\ &= g(\underline{a}, \underline{c}) \end{aligned}$$

where the last line follows from linearity of g. □

4 Multiplicative Linear Logic

Something about considering the subsystem MLL

The Geometry of Interaction program has been initiated by Girard [3], [4], [5], [6], [7], and further developed by Regnier [8], Seiller [9], [10], [11], [12], as well as many others [13], [15]. None of the ideas presented here are new, the standard textbook reference is [16] however the following was developed from the original papers.

4.1 The Sequentialisation Theorem

As already mentioned, logic navigates the space of arguments and picks out the correct ones. The Sequentialisation Theorem 4.1.17 formalises this by finding an algorithmic method for determining whether a proof *structure* is in fact a proof *net*. That is, whether a proof structure comes from a sequent style proof or not. The Sequentialisation Theorem was first proved by Girard in [1]. The proof here follows the argument there but with some (mostly insignificant) changes and many extra details filled in.

Definition 4.1.1. Let π be a proof structure and denote the set of tensor and par links of π by $\operatorname{Link}_{\otimes,\parr}\pi$ (or simply $\operatorname{Link}\pi$). A **switching** of π is a function

$$S : \operatorname{Link}\pi \longrightarrow \{L, R\} \tag{47}$$

A **switching** of a particular link l is a choice of L, R associated to l.

Definition 4.1.2. Let π be a proof structure. Let $\mathcal{O}(\pi)$ denote the set of occurrences of formulas in π (Definition 3.1.3). We consider two disjoint copies of this set

$$\mathcal{U}(\pi) := \mathcal{O}(\pi) \coprod \mathcal{O}(\pi) \tag{48}$$

where elements from the first copy are the **up elements**, and elements from the second copy are the **down elements**. We write $\uparrow A$ for the up element corresponding to an occurrence of a formula A in π, and $A \downarrow$ for the down element. Given a switching S of π, a **pretrip of π with respect to S** is a finite sequence $(x_1, ..., x_n)$ of elements of $\mathcal{U}(\pi)$ satisfying the following.

1. The sequence is a loop, that is, $x_1 = x_n$, and all elements (except the first and the last) are distinct.

2. If $x_j = A\downarrow$ and A is part of a conclusion link, then $x_{j+1} =\uparrow A$, corresponding to the same conclusion link.

3. If $x_j =\uparrow A$ and A is part of an axiom link then $x_{j+1} = \neg A\downarrow$, corresponding to the other conclusion of the axiom link.

4. If $x_j = A\downarrow$ and A is part of a cut link then $x_{j+1} =\uparrow \neg A$, corresponding to the other premise of the cut link.

5. For any tensor link l with premises A, B such that l has switching L, we have the following, where all formulas considered are part of the same tensor link:

    - if $x_j = A\downarrow$ then $x_{j+1} = (A \otimes B)\downarrow$,
    - if $x_j =\uparrow (A \otimes B)$ then $x_{j+1} =\uparrow B$,
    - if $x_j = B\downarrow$ then $x_{j+1} =\uparrow A$.

    and if l has switching R, we have:

    - if $x_j = A\downarrow$ then $x_{j+1} =\uparrow B$,
    - if $x_j =\uparrow (A \otimes B)$ then $x_{j+1} =\uparrow A$,
    - if $x_j = B\downarrow$ then $x_{j+1} = (A \otimes B)\downarrow$.

    (see Figure 1)

6. for any par link l with premises A, B such that l has switching L, we have, where all formulas considered are part of the same par link:

- if $x_j = \uparrow (A \parr B)$ then $x_{j+1} = \uparrow A$,
- if $x_j = A \downarrow$ then $x_{j+1} = (A \parr B) \downarrow$,
- if $x_j = B \downarrow$ then $x_{j+1} = \uparrow B$.

and if l evaluates under S to R, we have:

- if $x_j = A \downarrow$ then $x_{j+1} = \uparrow A$,
- if $x_j = \uparrow (A \parr B)$ then $x_{j+1} = \uparrow B$,
- if $x_j = B \downarrow$ then $x_{j+1} = (A \parr B) \downarrow$.

(see Figure 2)

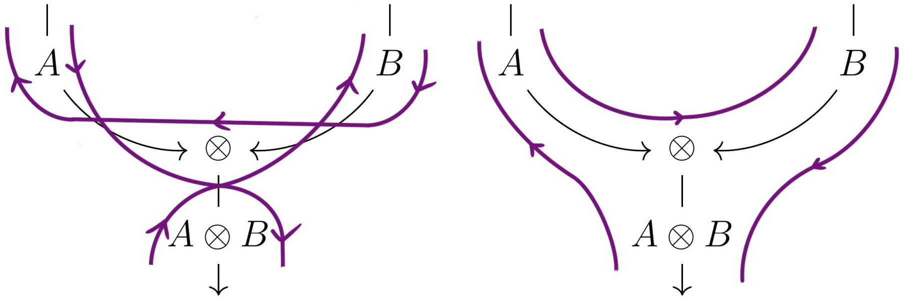


Figure 1: Tensor link, L switching, R switching

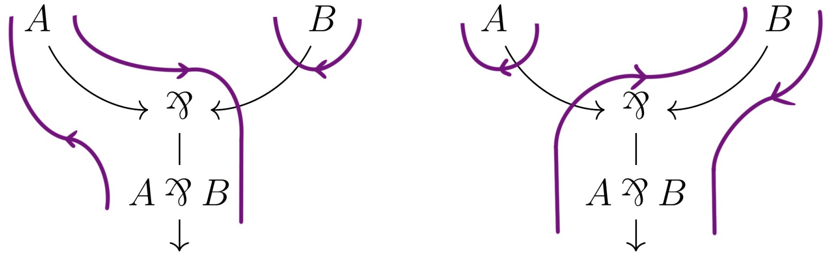


Figure 2: Par link, L switching, R switching.

Definition 4.1.3. Let $\mathrm{Pre}\mathcal{T}(\pi, S)$ denote the set of all pretrips of π with respect to S. We define an equivalence relation $\sim$ on this set where two pretrips $(x_1, ..., x_n)$ and $(y_1, ..., y_m)$ are equivalent if $n = m$, and there exists an integer k such that $x_{i+k} = y_i$ (where $i + k$ means $i + k \bmod n$) for all $i = 1, ..., n$.

A **trip** of π with respect to S is an equivalence class of pretrips. We denote the set of all trips by $\mathcal{T}(\pi, S)$. If the set $\mathcal{T}(\pi, S)$ admits more than one element, these elements are called **short trips**, and if it admits only one element, this element is the **long trip**. We refer to the statement "for all switchings S, the set $\mathcal{T}(\pi, S)$ contains exactly one element" as the **long trip condition**.

A **short pretrip** is a choice of representative for a short trip, and a **long pretrip** is a choice of representatitive of a long trip.

Given a proof structure π satisfying the long trip condition and a tensor link l with premises A, B say, let S be a switching of π and $t := (x_1, ..., x_n)$ be the long pretrip of π satisfying $x_1 = A \downarrow$. Since π satisfies the long trip condition, it must be the case that $\uparrow (A \otimes B)$ and $B \downarrow$ occur somewhere in t. Can we determine which occurs earlier? Let $m, l > 0$ be such that $x_m = \uparrow (A \otimes B), x_l = B \downarrow$ and assume $l < m$. Say $S(\tau) = L$, then t has the shape

$$(A \downarrow, (A \otimes B) \downarrow, ..., B \downarrow, \uparrow A, ..., \uparrow (A \otimes B), \uparrow B, ..., A \downarrow) \tag{49}$$

Now consider the switching given by

$$\hat{S}(\sigma) = \begin{cases} S(\sigma), & \sigma \neq \tau \\ R, & \sigma = \tau \end{cases}$$

Then (49) becomes:

$$(A \downarrow, \uparrow B, ..., A \downarrow) \tag{50}$$

which is a short pretrip, contradicting the assumption that π satisfies the long trip condition. Thus $m < l$. We have proven (the first half) of the following.

Lemma 4.1.4. *Let π be a proof structure satisfying the long trip condition, l be a tensor link with premises A, B say, S be a switching of π and $(x_1, ..., x_n)$ the long pretrip satisfying $x_1 = A \downarrow$. If $m, l > 0$ are such that $x_m = \uparrow (A \otimes B), x_l = B \downarrow$, then:*

- *if $S(\tau) = L$ then $m < l$,*
- *if $S(\tau) = R$ then $l < m$.*

The proof of the other half is similar to what has already been written, however since Lemma 4.1.4 contradicts [1, Lemma 2.9.1] we write out the details here:

Proof. Say $m < l$, then t has the shape

$$(A \downarrow, \uparrow B, ..., \uparrow (A \otimes B), \uparrow A, ..., B \downarrow, (A \otimes B) \downarrow, ..., A \downarrow) \tag{51}$$

Now consider the switching given by

$$S'(\sigma) = \begin{cases} S(\sigma), & \sigma \neq \tau \\ L, & \sigma = \tau \end{cases}$$

Then (51) becomes:

$$(A \downarrow, (A \otimes B) \downarrow, ..., A \downarrow) \tag{52}$$

which is a short pretrip. □

Lemma 4.1.5. *Let π be a proof structure satisfying the long trip condition, l be a par link with premises A, B say, S be a switching of π and $(x_1, ..., x_n)$ be the long pretrip satisfying $x_1 = A \downarrow$. If $m, l > 0$ are such that $x_m =\uparrow (A \parr B), x_l = B \downarrow$, then*

- *if $S(\tau) = L$ then $m < l$,*
- *if $S(\tau) = R$ then $l < m$*

Remark 4.1.6. Lemma 4.1.4 gives a nice interpretation of Lemma 4.1.4 that long trips *return to where they left* at each tensor link.

The situation is a bit different for par links; the relevant slogan is long trips *visit the premises before returning to the conclusion.*

Say π satisfies the long trip condition and moreover π admits a tensor link l (with premises A, B say) such that if l is removed, the resulting proof structure consists of two disjoint proof structures π_1, π_2 each satisfying the long trip condition. It is necessarily the case that any pretrip ρ of π starting at $\uparrow A$ visits the entirety of $\mathcal{U}(\pi_1)$ before returning to the tensor link l, lest π_1 admit a short trip. Moreover, it must be the case that σ admits no occurrence of formulas in π_2 lest the result of removing the tensor link l not result in disjoint proof structures. Thus, if such a link l exists, it is *maximal* in the sense that there is no other tensor link l' where a pretrip starting at a premise of l' contains the entirety of any pretrip starting at A. Most of the remainder of this Section will amount to proving the converse, that any such maximal tensor link "splits" π. This is the *splitting lemma* of [1]. We then conclude with the Sequentialisation Theorem (Theorem 4.1.17).

Definition 4.1.7. Let π be a proof structure satisfying the long trip condition, S a switching of π, and A an occurrence of a formula in π. Consider the long pretrip $(x_1, ..., x_n)$ satisfying $x_1 =\uparrow A$. We denote by

$$\mathrm{PTrip}(\pi, S, A, \uparrow) \tag{53}$$

the subsequence $(x_1, ..., x_m)$ of $(x_1, ..., x_n)$ satisfying $x_m = A \downarrow$. We define

$$\mathrm{PTrip}(\pi, S, A, \downarrow) \tag{54}$$

similarly.

Also, for $a \in \{\uparrow, \downarrow\}$ we define the following set

$$\mathrm{Visit}_S(A, a) := \{C \in \mathcal{O}(\pi) \mid \uparrow C, C \downarrow \text{ occur in } \mathrm{PTrip}(\pi, S, A, a)\} \tag{55}$$

The **up empire of** A is the following set:

$$\mathrm{Emp}_{\uparrow} A := \{C \in \mathcal{O}(\pi) \mid \text{For all switchings } S \text{ we have } \uparrow C, C \downarrow \text{ occur in } \mathrm{PTrip}(\pi, S, A, \uparrow)\} \tag{56}$$

The **down empire of** A is defined symmetrically.

One point of difference between the proof presented here and the original proof [1] is that Girard did *not* consider *down* empires, and instead only considered up empires. At the time of writing, the current author does *not* see how to avoid down empires, and believes the proof in [1] is too turse to extract a rigorous proof which avoids them.

With the new terminology, we now have some corollaries of Lemmas 4.1.4 and 4.1.5:

Corollary 4.1.8. *Let π be a proof structure satisfying the long trip condition, and let S be a switching of π, for a formula A and $a \in \{\uparrow, \downarrow\}$, denote* $\mathrm{PTrip}(\pi, S, A, a)$ *by* $\mathrm{PTrip}(A, a)$*:*

1. *if A is part of an axiom link then*

$$\mathrm{PTrip}(A,\uparrow) = \uparrow A, \mathrm{PTrip}(\neg A,\downarrow), A\downarrow \tag{57}$$

2. *if l is a tensor link with conclusion $A \otimes B$:*

   (a) *if $S(l) = L$:*

$$\mathrm{Ptrip}(A,\downarrow) = A\downarrow, \mathrm{PTrip}(A\otimes B,\downarrow), \mathrm{PTrip}(B,\uparrow), \uparrow A \tag{58}$$

$$\mathrm{PTrip}(B,\downarrow) = B\downarrow, \mathrm{PTrip}(A,\uparrow), \mathrm{PTrip}(A\otimes B,\downarrow), \uparrow B \tag{59}$$

$$\mathrm{PTrip}(A\otimes B,\uparrow) = \uparrow A\otimes B, \mathrm{PTrip}(B,\uparrow), \mathrm{PTrip}(A,\uparrow), A\otimes B\downarrow \tag{60}$$

   (b) *if $S(l) = R$:*

$$\mathrm{PTrip}(A,\downarrow) = A\downarrow, \mathrm{PTrip}(B,\uparrow), \mathrm{PTrip}(A\otimes B,\downarrow), \uparrow A \tag{61}$$

$$\mathrm{PTrip}(B,\downarrow) = B\downarrow, \mathrm{PTrip}(A\otimes B,\downarrow), \mathrm{PTrip}(A,\uparrow), \uparrow B \tag{62}$$

$$\mathrm{PTrip}(A\otimes B,\uparrow) = \uparrow A\otimes B, \mathrm{PTrip}(A,\uparrow), \mathrm{PTrip}(B,\uparrow), A\otimes B\downarrow \tag{63}$$

3. *if A is a premise of a par link l with conclusion $A \parr B$:*

   (a) *if $S(l) = L$:*

$$\mathrm{PTrip}(A,\downarrow) = A\downarrow, \mathrm{PTrip}(A\parr B,\downarrow), \uparrow A \tag{64}$$

$$\mathrm{PTrip}(B,\downarrow) = B\downarrow, \uparrow B \tag{65}$$

$$\mathrm{PTrip}(A\parr B,\uparrow) = \uparrow A\parr B, \mathrm{PTrip}(A,\uparrow), A\parr B\downarrow \tag{66}$$

   (b) *if $S(l) = R$:*

$$\mathrm{PTrip}(A,\downarrow) = A\downarrow, \uparrow A \tag{67}$$

$$\mathrm{PTrip}(B,\downarrow) = B\downarrow, \mathrm{PTrip}(A\parr B,\downarrow), \uparrow B \tag{68}$$

$$\mathrm{PTrip}(A\parr B,\uparrow) = \uparrow A\parr B, \mathrm{PTrip}(B,\uparrow), A\parr B\downarrow \tag{69}$$

In particular:

Corollary 4.1.9. *For any formula A which is a premise to either a tensor or par link, and any $a \in \{\uparrow, \downarrow\}$, we have:*

$\uparrow C$ *occurs in* $\mathrm{PTrip}(\pi, S, A, \uparrow)$ *if and only if* $C \downarrow$ *occurs in* $\mathrm{PTrip}(\pi, S, A, \downarrow)$

and similarly for $\mathrm{PTrip}(\pi, S, A, \downarrow)$.

Proof. By induction on the length of the sequence $\mathrm{PTrip}(\pi, S, A, a)$ and appealing to Corollary 4.1.8. □

Corollary 4.1.10. *Let π be a proof structure satisfying the long trip condition, we have the following.*

1. *For any axiom link with conclusions $A, \neg A$:*

$$\mathrm{Emp}_{\uparrow} A = \mathrm{Emp}_{\downarrow}(\neg A) \cup \{A\} \tag{70}$$

2. *For any cut link with premises $A, \neg A$:*

$$\mathrm{Emp}_{\downarrow} A = \mathrm{Emp}_{\uparrow}(\neg A) \cup \{A\} \tag{71}$$

3. *For any tensor link with premises A, B:*

$$\mathrm{Emp}_{\uparrow} A \cap \mathrm{Emp}_{\uparrow} B = \varnothing \tag{72}$$

4. *For any tensor or par link with premises A, B and conclusion C:*

$$\mathrm{Emp}_{\uparrow} C = \mathrm{Emp}_{\uparrow} A \cup \mathrm{Emp}_{\uparrow} B \cup \{C\} \tag{73}$$

5. *For any tensor link with premises A, B:*

$$\mathrm{Emp}_{\downarrow} B = \mathrm{Emp}_{\uparrow} A \cup \mathrm{Emp}_{\downarrow}(A \otimes B) \cup \{B\} \tag{74}$$

and similarly:

$$\mathrm{Emp}_{\downarrow} A = \mathrm{Emp}_{\uparrow} B \cup \mathrm{Emp}_{\downarrow}(A \otimes B) \cup \{A\} \tag{75}$$

Definition 4.1.11. Given any link l we write $B \in l$ if B occurs as either a premise or a conclusion of l.

Let π be a proof structure satisfying the long trip condition, and $a \in \{\uparrow, \downarrow\}$. The set of **links of A with respect to S** is the set

$$\mathrm{Link}_a A := \{ l \in \mathrm{Link}\, \pi \mid \forall B \in l, B \in \mathrm{Emp}_a A \} \tag{76}$$

Definition 4.1.12. Let π be a proof structure satisfying the long trip condition and let $a \in \{\uparrow, \downarrow\}$. Define the set

$$\mathrm{Link}^0_{\parr, a} A := \{ l \in \mathrm{Link}\, \pi \mid \text{Exactly one premise of } l \text{ is in } \mathrm{Emp}_a A \} \tag{77}$$

Lemma 4.1.13 (Realisation Lemma)**.** *Let π be a cut-free proof structure satisfying the long trip condition, let $a \in \{\uparrow, \downarrow\}$ and A an occurrence of a formula in π. Define the following function:*

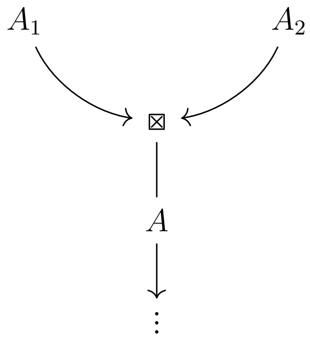
$$\begin{aligned} S : \operatorname{Link}^0_{⅋,a} A &\longrightarrow \{L, R\} \\ l &\longmapsto \begin{cases} L, & \textit{if the right premise of } l \textit{ is in } \operatorname{Emp}_a A \\ R, & \textit{if the left premise of } l \textit{ is in } \operatorname{Emp}_a A \end{cases} \end{aligned}$$

and extend this to a switching $\hat{S} : \operatorname{Link} \pi \longrightarrow \{L, R\}$ arbitrarily. Then

$$\operatorname{Emp}_a A = \operatorname{Visit}_{\hat{S}}(A, a) \tag{78}$$

Proof. We proceed by induction on the size $|\operatorname{Link}_a(A)|$ of the set $\operatorname{Link}_a(A)$. For the base case, assume $|\operatorname{Link}_a(A)| = 0$. The formula A is part of an axiom link and so $\operatorname{Emp}_\uparrow A = A, \sim A$ and $\operatorname{Emp}_\downarrow A = A$, the result follows easily.

Now assume that $|\operatorname{Link}_a A| = n > 0$ and the result holds for any formula B such that $|\operatorname{Link}_a B| < n$. First say $a =\uparrow$, and A is a conclusion of either a tensor or a par link



where $⊠ \in \{\otimes, ⅋\}$ and $A = A_1 \otimes A_2$ or $A = A_1 ⅋ A_2$. By (4) we have

$$\begin{aligned} \operatorname{Emp}_\uparrow A &= \operatorname{Emp}_\uparrow A_1 \cup \operatorname{Emp}_\uparrow A_2 \cup \{A\} \\ &= \operatorname{Visit}_{\hat{S}}(A_1, \uparrow) \cup \operatorname{Visit}_S(A_2, \uparrow) \cup \{A\} \\ &= \operatorname{Visit}_{\hat{S}}(A, \uparrow) \end{aligned}$$

where the second equality follows from the inductive hypothesis.

Assume A is part of an axiom link. By (1)

$$\operatorname{Emp}_\uparrow A = \operatorname{Emp}_\downarrow(\neg A) \cup \{A\} \tag{79}$$

with

$$|\operatorname{Link}_\uparrow A| = |\operatorname{Link}_\downarrow(\neg A)| \tag{80}$$

Since $|\operatorname{Link}_\downarrow(\sim A)| > 0$ we necessarily have that $\sim A$ is not a conclusion. Thus, since π is cut-free, A is connected to an occurrence $\sim A$ which is a premise to either a tensor link or a par link. In the case of the former, we have:

$$\begin{tikzcd}
C \arrow[dr, bend right] & & \neg A \arrow[dl, bend left] \\
& \otimes \arrow[d, dash] & \\
& C \otimes \neg A \arrow[d] & \\
& \vdots &
\end{tikzcd}$$

then by (5):

$$\begin{aligned}
\mathrm{Emp}_{\downarrow}(\neg A) &= \mathrm{Emp}_{\uparrow} C \cup \mathrm{Emp}_{\downarrow}(C \otimes \neg A) \cup \{\neg A\} \\
&= \mathrm{Visit}_{\hat{S}}(C, \uparrow) \cup \mathrm{Visit}_{\hat{S}}(C \otimes \neg A, \downarrow) \cup \{\neg A\} \\
&= \mathrm{Visit}_{\hat{S}}(\neg A, \downarrow)
\end{aligned}$$

where the second equality follows from the inductive hypothesis.

If ~ A is a premise of a par link

$$\begin{tikzcd}
C \arrow[dr, bend right] & & \neg A \arrow[dl, bend left] \\
& \parr \arrow[d, dash] & \\
& C \parr \neg A \arrow[d] & \\
& \vdots &
\end{tikzcd}$$

then by construction of $\hat{S}$, where we use the specific definition of S for the first time,

$$\begin{aligned}
\mathrm{Emp}_{\downarrow}(\neg A) &= \{\neg A\} \\
&= \mathrm{Visit}_{\hat{S}}(\neg A, \downarrow)
\end{aligned}$$

The case when $a =\downarrow$ is exactly similar and so we omit the proof. □

Definition 4.1.14. A tensor or par link is **terminal** if it is a conclusion.

Corollary 4.1.15. *Let π be a cut-free proof structure satisfying the long trip condition. Let*

$$l = \begin{tikzcd}
A \arrow[dr, bend right] & & B \arrow[dl, bend left] \\
& \otimes \arrow[d, dash] & \\
& A \otimes B \arrow[d] & \\
& \mathrm{c} &
\end{tikzcd}$$

be a terminal tensor link of π. Then π admits a par link

$$l' := \begin{tikzcd} C \arrow[dr, bend right] & & D \arrow[dl, bend left] \\ & \otimes \arrow[d, dash] & \\ & C \parr D \arrow[d] & \\ & \vdots & \end{tikzcd}$$

such that either $C \in \mathrm{Emp}_{\uparrow} A$ and $D \in \mathrm{Emp}_{\uparrow} B$ or $C \in \mathrm{Emp}_{\uparrow} B$ and $D \in \mathrm{Emp}_{\uparrow} A$ if and only if for any switching S of π we have that either

$$\mathrm{Emp}_{\uparrow} A \subsetneq \mathrm{Visit}_S(A, \uparrow) \qquad \textit{or} \qquad \mathrm{Emp}_{\uparrow} B \subsetneq \mathrm{Visit}_S(B, \uparrow)$$

Proof. Say π admitted l' and $C \in \mathrm{Emp}_{\uparrow} A$ and $D \in \mathrm{Emp}_{\uparrow} B$. If the switching S is such that $S(l) = L$ then $C \parr D \in \mathrm{Visit}_S(B) \smallsetminus \mathrm{Emp}_{\uparrow} B$ and if $S(\tau) = R$ then $C \parr D \in \mathrm{Visit}_S(A) \smallsetminus \mathrm{Emp}_{\uparrow} A$. The other case is similar.

Conversely, say π admits no such par link l', that is, assume

$$\mathrm{Link}^0_{\parr,\uparrow}(A) \cap \mathrm{Link}^0_{\parr,\uparrow}(B) = \varnothing \tag{81}$$

Then there is by Lemma 4.1.13 a well defined function

$$S : \mathrm{Link}^0_{\parr,\uparrow}(A) \cup \mathrm{Link}^0_{\parr,\uparrow}(B) \longrightarrow \{L, R\}$$

which extends to a switching $\hat{S}$ such that

$$\mathrm{Emp}_{\uparrow} A = \mathrm{Visit}_{\hat{S}}(A, \uparrow) \qquad \text{and} \qquad \mathrm{Emp}_{\uparrow} B = \mathrm{Visit}_{\hat{S}}(B, \uparrow) \tag{82}$$

□

Lemma 4.1.16 (Separation Lemma)**.** *A cut-free proof structure π satisfying the long trip condition, with only tensor links amongst its conclusions admits a tensor link*

$$l := \begin{tikzcd} A \arrow[dr, bend right] & & B \arrow[dl, bend left] \\ & \otimes \arrow[d, dash] & \\ & A \otimes B \arrow[d] & \\ & \mathrm{c} & \end{tikzcd}$$

satisfying

$$\mathcal{O}(\pi) = \mathrm{Emp}_{\uparrow} A \cup \mathrm{Emp}_{\uparrow} B \cup \{A \otimes B\} \tag{83}$$

Moreover, removing $A \otimes B$ results in a disconnected graph with each component a proof structure satisfying the long trip condition.

Proof. Consider the set of tensor links $\mathrm{Link}_{\otimes}(\pi)$ of π. We endow this with the following partial order $\leq$: a pair of links:

$$l' := \begin{tikzcd}[column sep=small] A \arrow[dr, bend right] & & B \arrow[dl, bend left] \\ & \otimes \arrow[d, dash] & \\ & A \otimes B \arrow[d] & \\ & \vdots & \end{tikzcd} \qquad l'' := \begin{tikzcd}[column sep=small] C \arrow[dr, bend right] & & D \arrow[dl, bend left] \\ & \otimes \arrow[d, dash] & \\ & C \otimes D \arrow[d] & \\ & \vdots & \end{tikzcd}$$

are such that $l' \leq l''$ if $\mathrm{Emp}_{\uparrow} A \cup \mathrm{Emp}_{\uparrow} B \subseteq \mathrm{Emp}_{\uparrow} C \cup \mathrm{Emp}_{\uparrow} D$. Let l (with conclusion $A \otimes B$ say) be a tensor link maximal with respect to $\leq$. We show that l satisfies the required property.

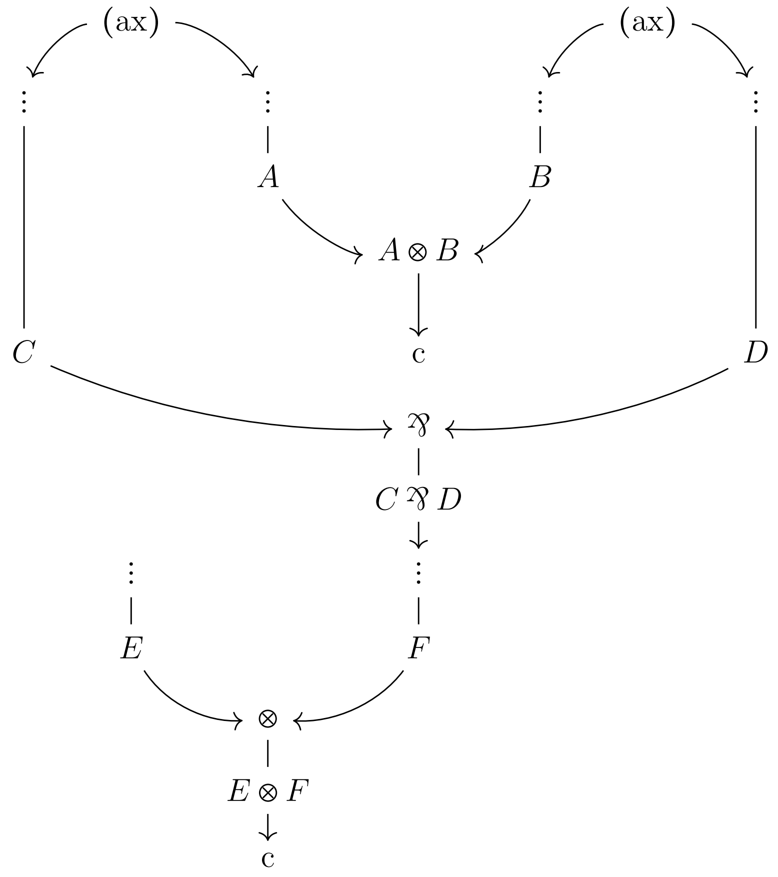
Say $\mathcal{O}(\pi) \neq \mathrm{Emp}_{\uparrow} A \cup \mathrm{Emp}_{\uparrow} B \cup \{A \otimes B\}$. Then by Lemma 4.1.15 there exists a par link

$$l' = \begin{tikzcd}[column sep=small] C \arrow[dr, bend right] & & D \arrow[dl, bend left] \\ & \parr \arrow[d, dash] & \\ & C \parr D \arrow[d] & \\ & \vdots & \end{tikzcd}$$

such that either $C \in \mathrm{Emp}_{\uparrow} A$ and $D \in \mathrm{Emp}_{\uparrow} B$ or $C \in \mathrm{Emp}_{\uparrow} B$ and $D \in \mathrm{Emp}_{\uparrow} A$. We show the proof in the case of the former. Since π admits no terminal par links, the unique maximal length directed path of π beginning at the node $\parr$ of l' terminates at an edge labelled $E \otimes F$, for some E, F.

$$l'' := \begin{tikzcd}[column sep=small] E \arrow[dr, bend right] & & F \arrow[dl, bend left] \\ & \otimes \arrow[d, dash] & \\ & E \otimes F \arrow[d] & \\ & \vdots & \end{tikzcd}$$

Notice that if $l'' = l$, then either $C \parr D \in \mathrm{Emp}_{\uparrow} A$ or $C \parr D \in \mathrm{Emp}_{\uparrow} B$ which in either case implies $\mathrm{Emp}_{\uparrow} A \cap \mathrm{Emp}_{\uparrow} B \neq \varnothing$, contradicting Corollary 4.1.10, 3, and so $l'' \neq l$. Without any loss of generality, assume that l' sits above F. The situation looks as follows.



Let S be a switching of π so that $\mathrm{Emp}_{\uparrow} F = \mathrm{Visit}_S(F, \uparrow)$ and so that $S(l') = L$, which exists by Lemma 4.1.15. Let $t = (x_1, ..., x_n)$ be the long pretrip of π with respect to S satisfying $x_1 = F\uparrow$. We have by Lemma 4.1.5 that t takes the following shape:

$$\uparrow F, ..., \uparrow (C \parr D), \uparrow C, ..., D\downarrow, \uparrow D, ..., C\downarrow, (C \parr D)\downarrow, ..., F\downarrow, ... \tag{84}$$

We have that $D \in \mathrm{Emp}_{\uparrow} B$ so for simplicity, rewrite (84) as $t' = (x_{1+k}, ..., x_{n+k})$ for some $k > 0$ (where $i + k$ means $i + k \bmod n$) so that $\uparrow B$ occurs to the left of $D\downarrow$ and $B\downarrow$ occurring to the right of $\uparrow D$. We have that $C \notin \mathrm{Emp}_{\uparrow} B$ and so by Corollary 4.1.9:

$$\uparrow B \text{ occurs in } \uparrow C, ..., D\downarrow \text{ and } B\downarrow \text{ occurrs in } \uparrow D, ..., C\downarrow \tag{85}$$

However, this implies that $B \in \mathrm{Visit}_S(F, \uparrow)$ which by Lemma 4.1.13 implies $B \in \mathrm{Emp}_{\uparrow} F$.

By reversing the switching of l' we can similarly show that $A \in \mathrm{Emp}_{\uparrow} F$, contradicting the maximality of l. This proves the first claim.

For the second claim, since $\mathcal{O}(\pi) = \mathrm{Emp}_{\uparrow} A \cup \mathrm{Emp}_{\uparrow} B \cup \{A \otimes B\}$ we have by Lemma 4.1.15 that

$$\mathrm{Link}^0_{\parr,\uparrow}(A \otimes B) = \varnothing \tag{86}$$

and we saw in the proof of Lemma 4.1.13 that a switching S which realises $\mathrm{Emp}_{\uparrow} A$ is given by setting all switchings arbitrarily except for those in $\mathrm{Link}^{0}_{\parr,\uparrow}(A \otimes B)$. This means that for any switching S of π:

$$\mathrm{Visit}_S(A, \uparrow) = \mathrm{Emp}_{\uparrow} A \qquad \text{and} \qquad \mathrm{Visit}_S(B, \uparrow) = \mathrm{Emp}_{\uparrow} B \tag{87}$$

which is to say the two subproof structures given by removing $A \otimes B$ never admit a short trip, that is, they each satisfy the long trip condition. □

Theorem 4.1.17 (The Sequentialisation Theorem). *A proof structure π (possibly with cuts) satisfies the long trip condition if and only π is a proof net.*

Proof. First assume that π is cut-free.

We proceed by induction on the size $|\mathrm{Link}\,\pi|$ of the set $\mathrm{Link}\,\pi$. If there this is zero then π consists of a single axiom link and so the result is clear.

For the inductive step, we consider two cases, first say π admits a par link for a conclusion. Then removing this par link clearly results in two cut-free subproof structures satsifying the long trip condition and so the result follows from the inductive hypothesis. If no such terminal par link exists, then by the Separation Lemma there exists some tensor link in the conclusion for which we can remove and apply the inductive hypothesis.

Now say that π contained cuts. We replace each cut with a tensor link to create a new proof ζ. That there exists a proof Ξ which maps to ζ follows from the part of the result proved already as ζ is cut-free. We adapt Ξ appropriately by replacing $\otimes$-rules by cut-rules and we are done. □

4.2 Modelling the dynamics of MLL

The distinction between *sense* and *reference*, due to Frege [21], can crudely be explained as the *means of description* of an object vs the object itself. From this angle, it makes sense to ignore the distinction between two proofs which differ only by a series of cut-reduction steps (either forwards or backwards ones), as surely these two proofs do not differ in their reference. This is the *denotational semantics* program, in which two proofs π, π' which are cut-equivalent to each other are given the same interpretation $[\![\pi]\!] = [\![\pi']\!]$.

On the other hand, the Curry-Howard correspondence [22] and the Gentzen-Mints-Zucker Duality [18] relate the cut-elimination process to the dynamics of a system of computation (β-reduction in the simply typed λ-calculus, in both cases). Thus, it makes sense also to look for models of logical systems where two cut equivalent proofs π, π' are *not* given the same interpretation, but instead there exists some relationship between the two $[\![\pi]\!] \longrightarrow [\![\pi']\!]$. This is the *geometry of interaction* [2], [3], [4], [5], [6], [7], due to Girard. In this section, we introduce the first two of these models which he created. The reference for Geometry of Interaction Zero is [2] and the reference for Geometry of Interaction One is [3].

See the Introduction of [12] for more on the distinction between denotation semantics and Geometry of Interaction.

Definition 4.2.1. Let $\mathcal{F}$ denote the set of formulas (Definition 3.0.1), $\mathcal{A}$ the set of oriented atoms, and $\mathcal{A}^* = \bigcup_{n\geq 0} \mathcal{A}^n$ the set of sequences of oriented atoms of length ≥ 0. We define an involution r on $\mathcal{A}^*$ as follows:

$$r : \mathcal{A}^* \longrightarrow \mathcal{A}^* \tag{88}$$

$$\big((X_1, x_1), ..., (X_n, x_n)\big) \longmapsto \big((X_n, \bar{x}_n), ..., (X_1, \bar{x}_1)\big) \tag{89}$$

where $\overline{+} = -$ and $\overline{-} = +$.

For the empty string $\varnothing \in \mathcal{A}^*$ we define $r(\varnothing) = \varnothing$.

The set $\mathcal{A}^*$ is a monoid under concatenation $c : \mathcal{A}^* \times \mathcal{A}^* \longrightarrow \mathcal{A}^*$ with identity $\varnothing$.

Definition 4.2.2. We denote by $\otimes : \mathcal{F} \times \mathcal{F} \longrightarrow \mathcal{F}$ the function which maps a pair of formulas (A, B) to the formula $A \otimes B$. Similarly, $\parr : \mathcal{F} \times \mathcal{F} \longrightarrow \mathcal{F}$ denotes the function such that $\parr(A, B) = A \parr B$ and $\neg : \mathcal{F} \longrightarrow \mathcal{F}$ denotes the function such that $\neg(A) = \neg A$. We denote by $\mathrm{inc} : \mathcal{A} \longrightarrow \mathcal{F}$ the map which sends an oriented atom (X, x) to itself (X, x), and lastly we denote by $\iota : \mathcal{A} \longrightarrow \mathcal{A}^*$ the function which maps an oriented atom (X, x) to the sequence consisting only of (X, x).

Lemma 4.2.3. *There is a unique map $a : \mathcal{F} \longrightarrow \mathcal{A}^*$ making the following diagrams commute*

$$\begin{tikzcd}
\mathcal{F} \times \mathcal{F} \arrow[r, "a \times a"] \arrow[d, "\otimes"'] & \mathcal{A}^* \times \mathcal{A}^* \arrow[d, "c"] & \mathcal{F} \times \mathcal{F} \arrow[r, "a \times a"] \arrow[d, "\parr"'] & \mathcal{A}^* \times \mathcal{A}^* \arrow[d, "c"] \\
\mathcal{F} \arrow[r, "a"] & \mathcal{A}^* & \mathcal{F} \arrow[r, "a"] & \mathcal{A}^*
\end{tikzcd} \tag{90}$$

$$\begin{tikzcd}
\mathcal{F} \arrow[r, "a"] \arrow[d, "\sim"'] & \mathcal{A}^* \arrow[d, "r"'] & \mathcal{A} \arrow[r, "\mathrm{inc}"] \arrow[dr, "\iota"'] & \mathcal{F} \arrow[d, "a"] \\
\mathcal{F} \arrow[r, "a"] & \mathcal{A}^* & & \mathcal{A}^*
\end{tikzcd} \tag{91}$$

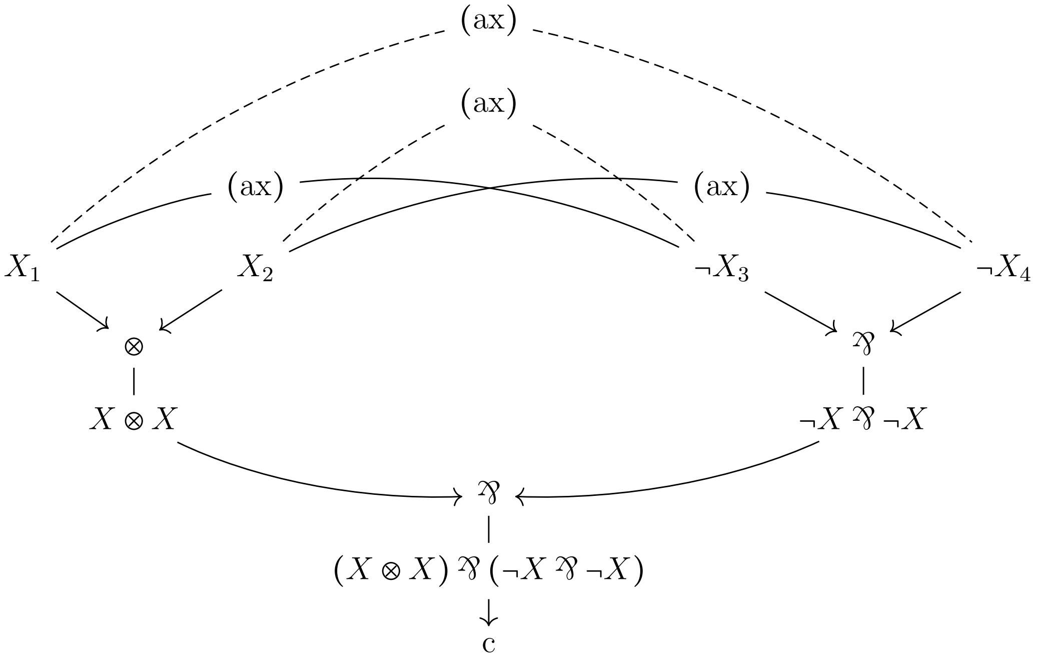
Proof. Left to the reader. □

Definition 4.2.4. Let A be a formula. The **sequence of oriented atoms** of A is $a(A) = (X_1, x_1), \ldots, (X_n, x_n)$ as defined by the previous lemma. The **sequence of unoriented atoms** of A is $X_1, ..., X_n$ and the **set of unoriented atoms** of A is the disjoint union $U_A = \{X_1\} \coprod \ldots \coprod \{X_n\}$. The **set of unoriented atoms** of a proof structure π is the disjoint union $U_\pi = \coprod_{e \in E} U_{A_e}$ where E is the set of edges of π, and A_e is the formula labelling e.

4.3 Proofs as permutations (Geometry of Interaction Zero)

A proof π in MLL with a single conclusion A is determined by A up to the axiom links of π. For instance, when the following proof net is read with dashed Axiom links ignored, we obtain a proof net π, and similarly if we read the dashed Axiom links and with the solid arrow Axiom links ignored.

Example 4.3.1.



(92)

Assuming that π satisfies the property that all the conclusions of its axiom links are atomic, then in fact these two possibilities completely exhaust the proof nets with conclusion $(X \otimes X) \parr (\neg X \parr \neg X)$. This example is generic, in the sense that the "trunk" of any proof net is completely determined by its conclusion.

A compact way of describing the axiom links of a proof in MLL is to read each axiom link as a transposition, and to give the product of these as a permutation. This translation of proofs into permutations was first given in [2] and was expounded upon in [3]. Due to the popularity of the latter paper, the former is often overlooked.

In [2], it is also shown how to relate the permutations of a proof with cuts to the permutations of the associated normal form. The most important difference between the current presentation and that of [2] is that we use *unoriented atoms* (Definition 4.2.4).

Definition 4.3.2. Let π be a proof net. Let $\mathcal{P}(\pi)$ denote the disjoint union of all the unoriented axioms of all formulas which are conclusions to axiom links in π.

Definition 4.3.3. Let π be a proof net with axiom links $l_1, ..., l_n$ say. For each $i = 1, ..., n$ the link l_i defines a permutation τ_{l_i} on the set $\mathcal{P}(\pi)$ in the following way: if l_i has conclusions $\neg A, A$ then the j^{th} element of the sequence of unoriented atoms of A is mapped via τ_{l_i} to the j^{th} element of the sequence of unoriented atoms of $\neg A$. We define α_π to be the product of all these permutations.

$$\alpha_\pi := \tau_{l_1} \cdots \tau_{l_n} \tag{93}$$

We call this permutation the **axiom link permutation associated to** π.

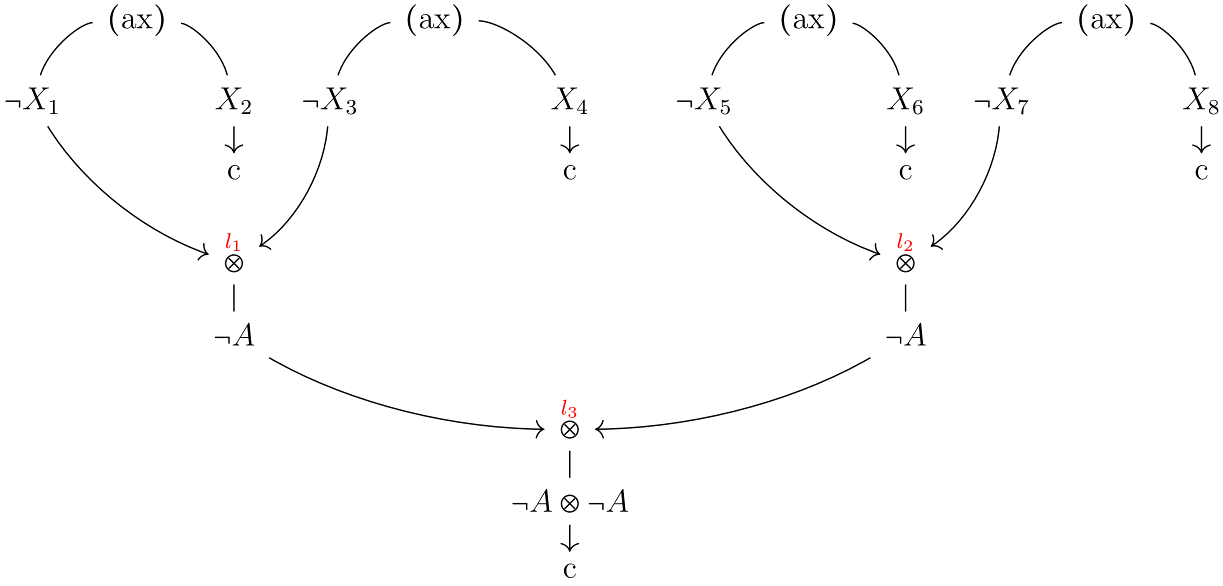
We define more permutations on $\mathcal{P}(\pi)$. Recall the definitions of pretrips (Definition 4.1.7) and switchings (Definition 4.1.1). Let S be a switching of π. For each unoriented axiom $X \in \mathcal{P}(\pi)$, corresponding to a formula A say, let $\beta_\pi^S(X)$ denote the unoriented axiom corresponding to the first occurrence in $\mathrm{PTrip}(\pi, S, A, \downarrow)$ of the form $\uparrow B$ where B is a formula labelling a conclusion of an axiom link in π.

The set of all permutations of the second form is denoted:

$$\Sigma(\pi) := \{\beta_\pi^S \mid S \text{ is a switching of } \pi\} \tag{94}$$

We will often denote elements of $\beta_\pi^S \in \Sigma(\pi)$ simply by β.

Example 4.3.4. Let π denote the following proof structure with tensor links labelled l_1, l_2, l_3 as displayed. The formula A denotes $\neg X \otimes \neg X$.



(95)

Consider first the switching $S(l_1) = S(l_2) = S(l_3) = L$. Then we have

$$\beta_\pi^S : X_1 \mapsto X_7 \mapsto X_5 \mapsto X_3 \mapsto X_1, \quad X_i \mapsto X_i, i = 2,4,6,8 \tag{96}$$

The other permutations are as follows.

$$X_1 \mapsto X_3 \mapsto X_7 \mapsto X_5 \mapsto X_1, \quad X_i \mapsto X_i, i = 2,4,6,8$$
$$X_1 \mapsto X_3 \mapsto X_5 \mapsto X_7 \mapsto X_1, \quad X_i \mapsto X_i, i = 2,4,6,8$$
$$X_1 \mapsto X_5 \mapsto X_7 \mapsto X_3 \mapsto X_1, \quad X_i \mapsto X_i, i = 2,4,6,8$$

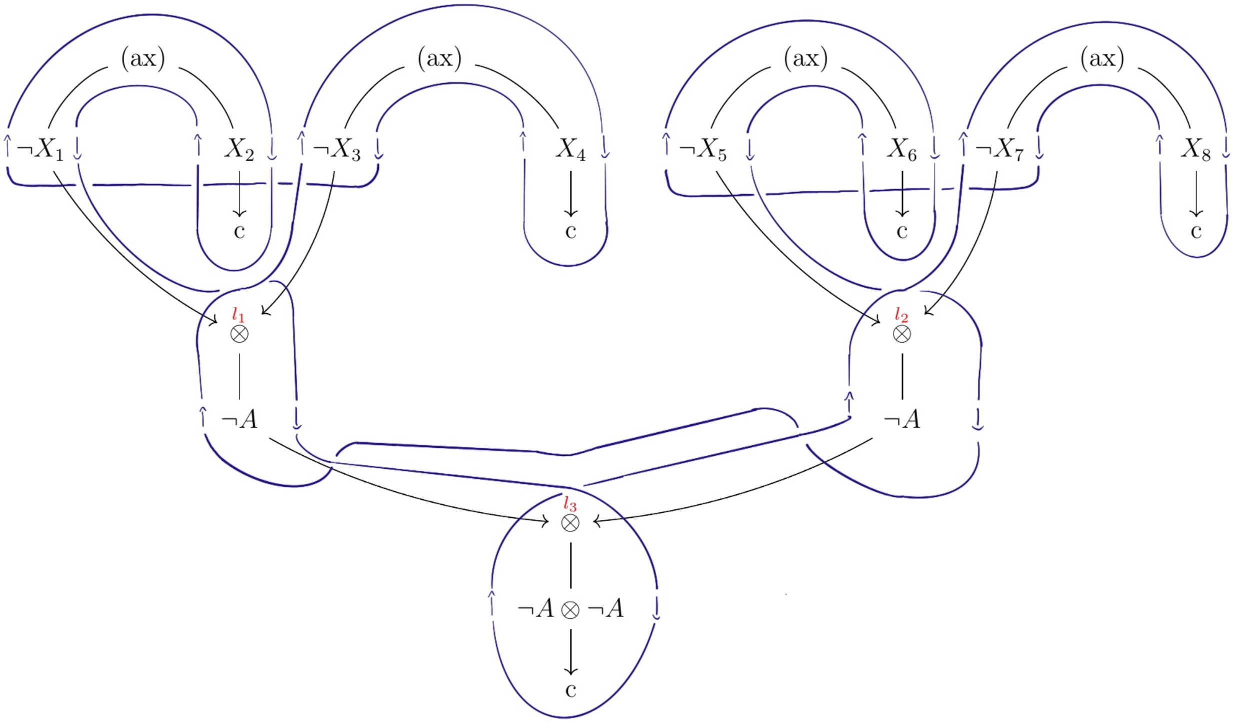


Figure 3: The switching S of Example 4.3.4

We can now rephrase the longtrip condition of Section 4.1 in terms of permutations.

Proposition 4.3.5. *Let π be a proof structure, then π is a proof net if and only if for all $\beta \in \Sigma(\pi)$ the permutation $\alpha_\pi \beta$ is cyclic.*

Proposition 4.3.6. *Let π be a cut-free proof net with only one conclusion, assume also that all conclusions of all axiom links are atomic. Then π is determined uniquely by α_π and the conclusion A.*

Proof. Simple proof by induction on the structure of A. □

Corollary 4.3.7. *Let π be a cut-free proof net with conclusions $A_1, ..., A_n$, assume also that all conclusions of all axiom links are atomic. Then π is determined uniquely by α_π and the conclusions $A_1, ..., A_n$.*

Proof. Let π_1, π_2 be two such proof nets. Construct a new proof net π_1' from π_1 by creating par links (in any order) so that π_1' has a unique conclusion $A_1 \parr \cdots \parr A_n$.

Construct a new proof net π_2' in a similar way and make the same choices of par links made when π_1' was constructed. No axiom links were altered in this process, and so $\alpha_{\pi_1} = \alpha_{\pi_1'} = \alpha_{\pi_2'} = \alpha_{\pi_2}$. It follows from Proposition 4.3.6 that $\pi_1 = \pi_2$. □

The proof net given by ignoring the dashed lines in (92) corresponds to the permutation

$$X_1 \leftrightarrow X_2, X_3 \leftrightarrow X_4 \tag{97}$$

and that given by ignoring the axiom links and including the dashed lines is

$$X_1 \leftrightarrow X_4, X_2 \leftrightarrow X_3 \tag{98}$$

Say π contains cuts and has corresponding normal form π'. Then π corresponds to a permutation α and π' to a permutation α'. We now describe the relationship between α and α'.

Lemma 4.3.8. *Let π be a proof structure such that every conclusion of every atom link is atomic. Assume there is a cut in π with premises $A, \neg A$. Write*

$$A := X_1 \boxtimes_1 \cdots \boxtimes_{n-1} X_n \tag{99}$$

where for each $i = 1, \dots, n-1$ we have $\boxtimes_i \in \{\otimes, ⅋\}$ and for each $i = 1, \dots, n$ we have that X_i is atomic. Let ζ be a proof structure equivalent to π under cut-reduction which is obtained by reducing all m-redexes (Definition 3.2.1). Then in ζ, there exists for each i a cut link l_i with premises $X_i, \neg X_i$.

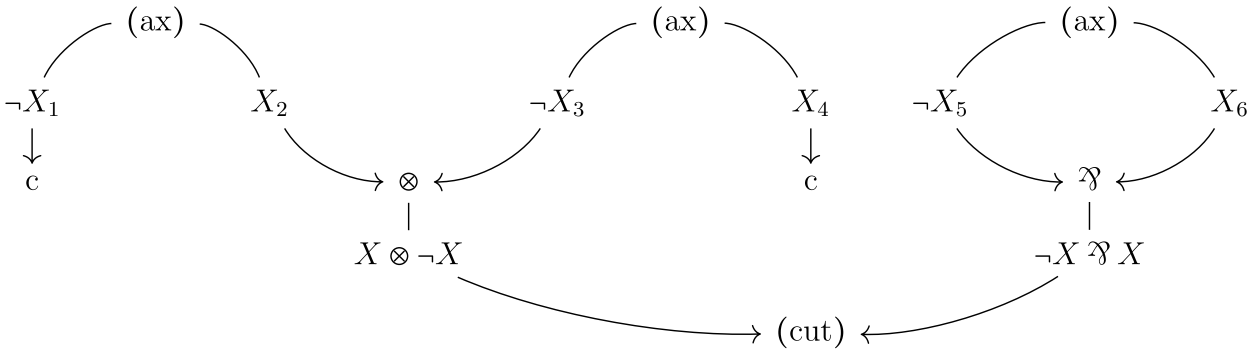
Proof. By induction on n. □

Using Lemma 4.3.8, if π is a cut-free proof structure with all conclusions to all axiom links atomic, then we can identify the atoms in the premises of the cut links with the atoms in the conclusions of the axiom links. We will do this throughout this section.

Definition 4.3.9. We define a permutation γ_π on $\mathcal{P}(\pi)$ (Definition 4.3.2). Let l be a cut link in π with premises $\neg A, A$, say. Let $\neg A, A$ have corresponding unoriented atoms $X_1, \dots, X_n$ and $Y_1, \dots, Y_n$. Let γ_l be the permutation which swaps X_j and Y_j. Ranging over all cut links $l_1, \dots, l_n$ we define

$$\gamma_\pi := \gamma_{l_1} \dots \gamma_{l_n} \tag{100}$$

Example 4.3.10. We denote by π the following proof net with artificial labels on the formulas. Assume X_i for $i = 1, \ldots, 6$ is atomic.



(101)

We have

$$\gamma_\pi : X_2 \leftrightarrow X_5, \quad X_3 \leftrightarrow X_6, \quad X_i \leftrightarrow X_i, i = 1, 4 \tag{102}$$

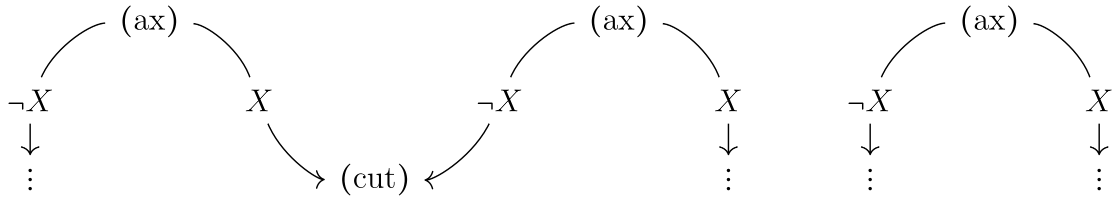
Lemma 4.3.11. *The set $\mathcal{P}(\pi)$ is invariant under reduction of m-redexes and η-expansion. More precisely, we have the following two statements.*

- *Say π' is produced by reducing an m-redex (**??**) in π, then $\mathcal{P}(\pi) = \mathcal{P}(\pi')$.*
- *Say $\pi \longrightarrow_\eta \pi'$ (see Definition **??**), then $\mathcal{P}(\pi) = \mathcal{P}(\pi')$.*

Proof. For the first claim we simply notice that rule (**??**) has no effect on the axiom links of π. For the second we see that the order of the sequence of unoriented atoms of A, B is explicated by the axiom links produced by an η-expansion. □

Hence, when considering $\mathcal{P}(\pi)$, we can always assume without loss of generality that π contains no m-redexes and that all conclusions of all axiom links of π are atomic.

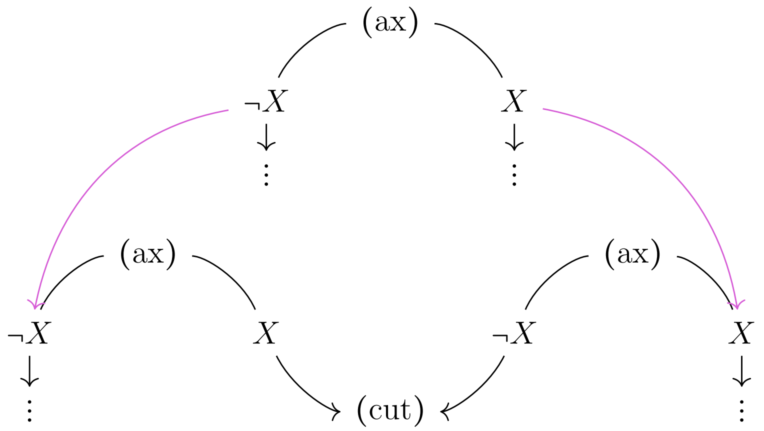
Lemma 4.3.12. *Let π be a proof net admitting no m-redexes and assume that all conclusions of all axiom links of π are atomic. All redexes $\pi \longrightarrow_{(\mathrm{cut})} \pi'$ are necessarily of the following form, with X atomic.*



(103)

Proof. All redexes of π are a-redexes, so all redexes of π are of the form (**??**) or (**??**), but since all the axiom links have atoms as conclusions, it must be the case that the cut link in (**??**), (**??**) have premises which are also atoms. These atoms can only possibly exist if they are conclusions to an axiom link, and so we obtain the form given in the statement. □

Definition 4.3.13. Say π is a proof net with no m-redexes and all conclusions of all axiom links are atomic. Moreover, say there is a reduction $\pi \longrightarrow \pi'$ which by Lemma 4.3.11 is of the form (103). We define a function $\iota : \mathcal{P}(\pi') \rightarrowtail \mathcal{P}(\pi)$ given by the following schema:



(104)

Definition 4.3.14. Let π be a proof net and consider $\mathcal{P}(\pi)$, in light of Lemma 4.3.11 we can assume without loss of generality that π admits no m-redexes and that all conclusions of all axiom links in π are atomic. Let ζ be the corresponding super normal form established by Corollary 4.3.1. Let $(\pi = \pi_1, \cdots, \pi_n = \zeta)$ be a sequence of cut reductions. These induce a family of functions:

$$\mathcal{P}(\zeta) = \mathcal{P}(\pi_n) \rightarrowtail \mathcal{P}(\pi_{n-1}) \longrightarrow \cdots \longrightarrow \mathcal{P}(\pi_2) \longrightarrow \mathcal{P}(\pi_1) = \mathcal{P}(\pi) \tag{105}$$

Composing these determines a function $\iota_\pi : \mathcal{P}(\zeta) \rightarrowtail \mathcal{P}(\pi)$.

Remark 4.3.15. It follows from Proposition **??** that the function ι_π is independent of the choice of reduction path used to define it.

We give an alternate characterisation of the image of ι_π.

Lemma 4.3.16. *Let π be a proof net admitting no m-redexes and assume all conclusions of all axiom links are atomic. A formula A in π is in $\operatorname{im} \iota_\pi$ if and only if it is the conclusion to an axiom link.*

Proof. Say A is premise to a cut link. Since $A \in \mathcal{P}(\pi)$ it is also the case that A is conclusion to an axiom link. Hence there exists a cut reduction which removes A, and so A is not in the image of ι_π.

Now say A is *not* premise to a cut link and so A is necessarily *not* part of an a-redex. There are no m-redexes in π and so all cut reductions reduce a-redexes. Hence A survives the cut reduction process. In other words, $A \in \operatorname{im} \iota_\pi$. □

Corollary 4.3.17. *Let π be a proof net and assume all conclusions of all axiom links are atomic. A formula A in π is in $\operatorname{im} \iota_\pi$ if an only if the unique maximal length directed path in π starting at the edge labelled A ends at the premise to a cut link.*

Definition 4.3.18. Let π be a proof net. We describe a final permutation δ_π on $\mathcal{P}(\pi)$. Recall the injective function ι_π of Definition 4.3.14. For each $X \in \mathcal{P}(\pi)$ let d_i denote the least integer such that this shouldn't use im

$$(\alpha_\pi \circ \gamma_\pi)^{d_i}(X) \in \operatorname{im} \iota_\pi \tag{106}$$

Notice that such an integer d_i always exists as π is a proof net (as π satisfies the longtrip condition, see Section 4.1).

We then define the following permutation on $\mathcal{P}(\pi)$, the permutations α_π, γ_π Definition 4.3.3, 4.3.9 respectively:

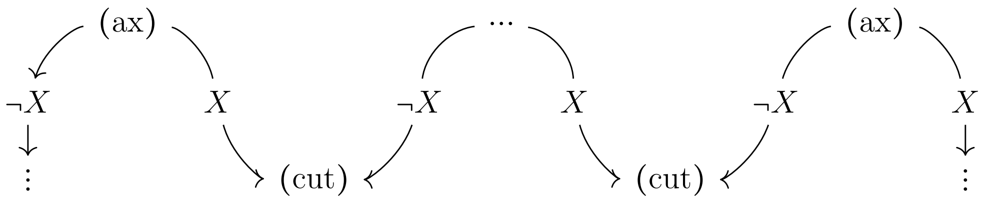
$$\delta_\pi(X) = (\alpha_\pi \circ \gamma_\pi)^{d_i}(X) \tag{107}$$

Theorem 4.3.19. *[Geometry of Interaction zero] Let π be a proof net possibly with cuts and let ζ be the normal form of π (Definition **??**). Then*

$$\delta_\pi = \iota_\pi \alpha_\zeta \tag{108}$$

Proof. By inspection of (**??**) we have that γ_π is invariant under reduction of m-redexes. Also, α_π is clearly invariant under reduction of m-redexes, thus we can assume that π admits no m-redex. Furthermore, by inspection of (**??**) we see that α_π is invariant under η-expansion, it is also clear that γ_π is invariant under η-expansion. Thus we can also assume that all conclusions of all axiom links of π are atomic.

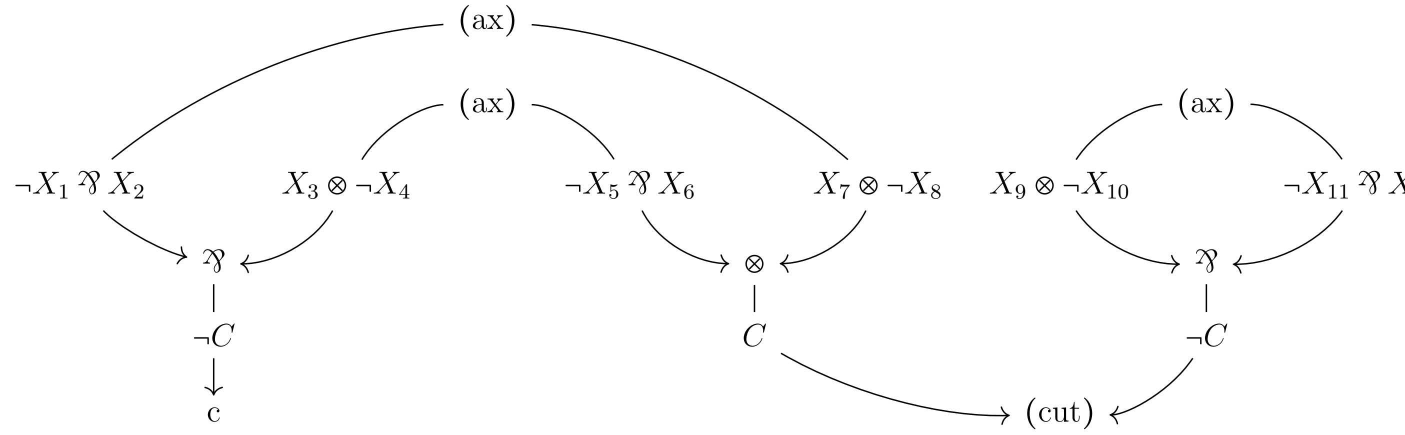
All cut links appear inside "chains" of axiom and cut links, such as in the following Diagram.



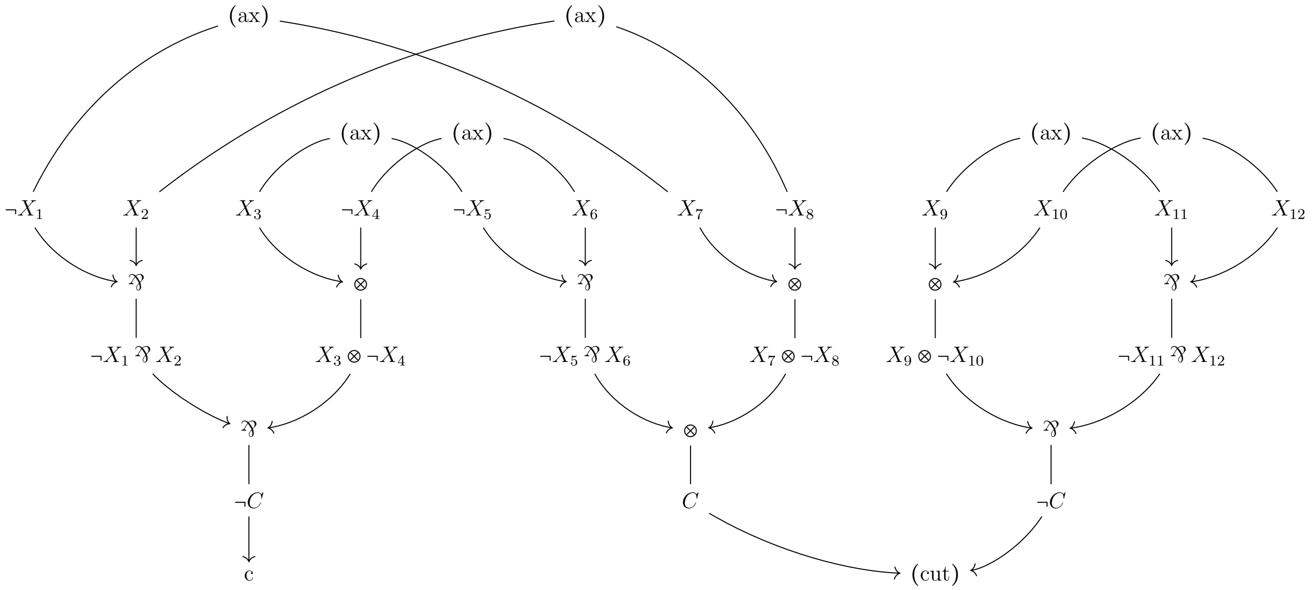
By Lemma 4.3.16, all formulas in the "interior" of these chains are not in $\operatorname{im} \iota_\pi$. Hence, δ_π is a product of transposes where the formulas on the two extreme ends of these chains are swapped. By considering the cut elimination rules (**??**), (**??**) we see that this is exactly the behaviour of α_ζ, and the that these two formulas are the images of the corresponding formulas in ζ. □

In [20, Proposition A.1] the relationship between the permutation δ of Definition 4.3.18 and another permutation coming from the model of Multiplicative Linear Logic as coordinate rings presented there. Here, we show a detailed example of this connection.

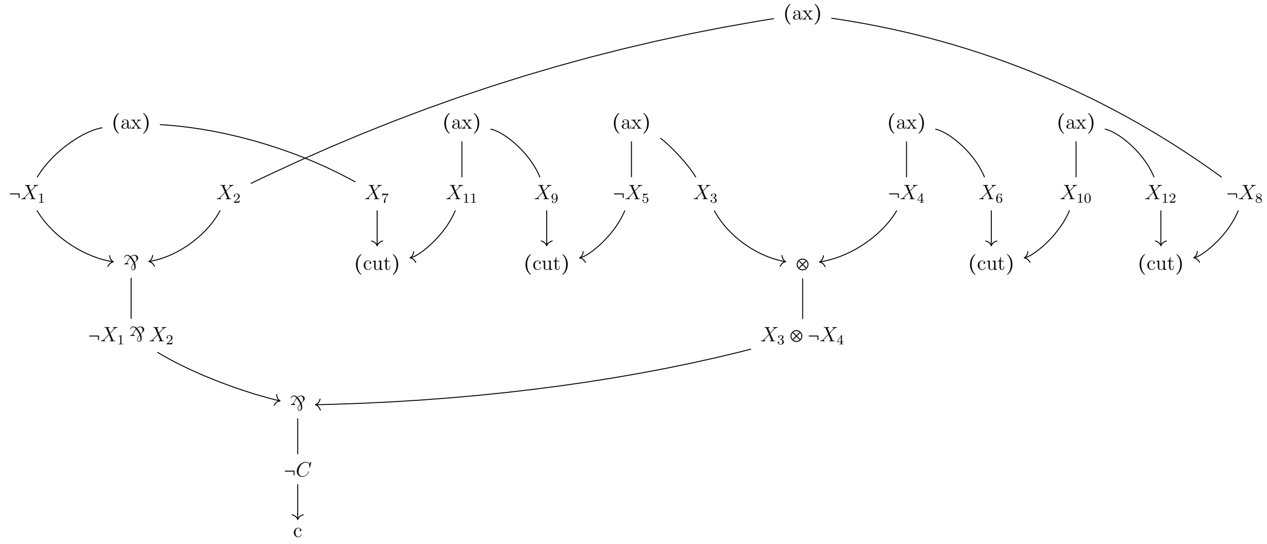
Example 4.3.20. Let π denote the following proof net, we let $(X, +)$ be atomic and denote it by X, the formula C denotes $(\neg X \parr X) \otimes (X \otimes \neg X)$. For convenience, we have artificially labelled the atomic propositions, but throughout, for any i the notation X_i means X.



First we describe δ_π. The first observation is that π is mapped under η-expansion to the following proof net, which we denote by π'.



The proof net π' admits m-redexes, we reduce these to obtain the following proof net which we denote by π''.



(109)

As was explained in the proof of Theorem [20, Proposition A.1] we have that $\delta_\pi = \delta_{\pi''}$. It was also explained in the same proof that $\delta_{\pi''}$ is a product of transpositions which swaps two formulas which are at the extreme ends of a common "chain". Hence, we read off (109) that

$$\delta_\pi : X_1 \leftrightarrow X_3, X_2 \leftrightarrow X_4 \tag{110}$$

On the other hand, we have that $\neg C = (\neg X_1 \parr X_2) \parr (X_3 \otimes \neg X_4)$, and so in the notation of Proposition [20, Proposition 3.9] we have a sequence $(i_1, i_2) = (2, 3)$ with complement $(j_1, j_2) = (1, 4)$, and so the polynomial denoted $k[X_1, X_2]$ in the statement of Proposition [20, Proposition 3.9] here is the polynomial $k[X_2, X_3]$ and the polynomial denoted $k[Y_1, Y_2]$ in Proposition [20, Proposition 3.9] here is the polynomial $k[X_1, X_4]$. The following are elements of the defining ideal I_π of π.

$$X_2 - X_8, \quad X_8'' - X_{12}'', \quad X_{12} - X_{10}, \quad X_{10}'' - X_6'', \quad X_6 - X_4 \tag{111}$$

and so are $X_i - X_i', X_i' - X_i''$ for $i = 2, 4, 6, 10, 12$. Hence we see that $\beta_-^{-1}\beta_+(X_2) = X_4$, so $\sigma(2) = 4$.

Similarly, the following are also elements of the defining ideal I_π of π.

$$X_1 - X_7, \quad X_7'' - X_{11}'', \quad X_{11} - X_9, \quad X_9'' - X_5'', \quad X_5 - X_3 \tag{112}$$

and so are $X_i - X_i', X_i' - X_i''$ for $i = 1, 3, 5, 7$. Hence, $\sigma(1) = 3$. Thus, the following holds for all $i = 1, 2, 3, 4$, as anticipated by Proposition [20, Proposition A.1].

$$\delta_\pi(X_i) = X_{\sigma(i)} \tag{113}$$

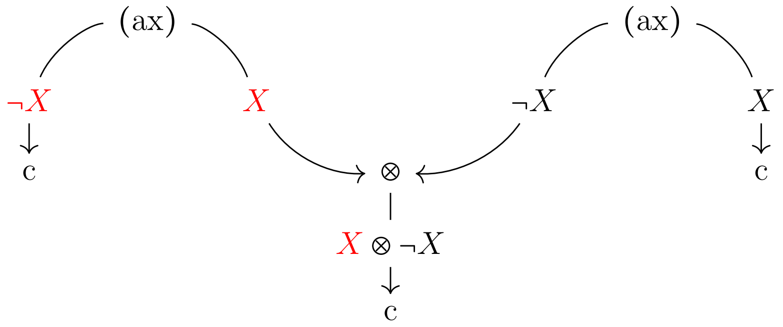
4.4 Persistent paths

It is somewhat remarkable that Girard's original presentation of Geometry of Interaction [3] never mentioned persistent paths, as this concept makes the ideas significantly more transparent. Persistent Paths were first defined by Regnier [8]. What is new here is the equivalence relation of Definition 4.4.1 used to define Persistent Paths (Definition 4.4.2). This provides an *intrinsic* definition which does not require knowledge of the result of any cut-reduction in order to define (unlike the definition given in [8]).

An axiom link with conclusions $\neg X, X$ is the translation of an axiom rule, here we assume X is atomic

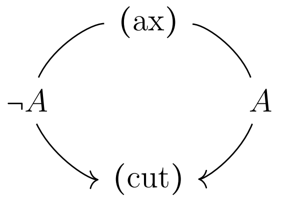
$$\frac{}{X \vdash X}\ (\text{ax})$$

and so we think of $\neg X$ as the *hypothesis* and X as the *conclusion*. The role of the edges in a proof net are then to keep track of the occurrences of formulae which are logically related, that is, they represent "the same" hypothesis or conclusion. For instance, the formulas coloured red in what follows are logically related.



More precisely, axiom/cut links induce a bijection between the unoriented atoms of each conclusion, and tensor/par links induce injective functions from the unoriented atoms of the premises to the conclusions. In the tensor/par case, the pair of injective functions is moreover a surjective family.

Thus, a choice of unoriented atom in a proof structure has a set of edges associated to it according to the previously mentioned functions. We will show that if the chosen unoriented atom is part of a conclusion to a proof structure, then the induced set of edges induces a path which both begins and ends at a conclusion edge. If the chosen unoriented atom is *not* part of a conclusion, then the induced path may not include *any* conclusions, as is the case for any choice of unoriented atom in the following proof structure.



In fact, this can only happen in a proof *structure*, whereas *any* choice of unoriented atom inside a proof net induces a conclusion-conclusion path. This is Lemma 4.4.5.

Definition 4.4.1. Let π be a proof structure. We define an equivalence relation $\sim$ on the set U_π of unoriented atoms of π. We do this by considering each non-conclusion link l of π.

If l is an axiom (respectively cut) link, with conclusions (premises) $\neg A, A$, where $U_{\neg A} = \{X_1, \dots, X_n\}$ and $U_A = \{X'_1, \dots, X'_n\}$ then we define

$$X_i \sim X'_i, \quad \forall i = 1, \dots, n \tag{114}$$

If l is a tensor or par link with premises A, B and conclusions $A \boxtimes B$ (where $\boxtimes \in \{\otimes, \parr\}$) then if we write $U_A = \{X_1, \dots, X_n\}, U_B = \{Y_1, \dots, Y_m\}$ and $U_{A \boxtimes B} = \{X'_1, \dots, X'_n, Y'_1, \dots, Y'_m\}$ then we define

$$X_i \sim X'_i, \forall i = 1, \dots, n \quad Y_i \sim Y'_i, \forall j = 1, \dots, m \tag{115}$$

Definition 4.4.2. Each equivalence class $[X_i]$ of formulas in U_π is the underlying set of a sequence

$$(Z_1, \dots, Z_n) \tag{116}$$

where $Z_i \sim Z_{i+1}, \forall i = 1, \dots, n-1$. Such a sequence is called a **persistent path**. Notice that the reverse sequence $(Z_n, \dots, Z_1)$ of any persistent path $(Z_1, \dots, Z_n)$ is itself a persistent path. If Z_1 is positive, then the persistent path $(Z_1, \dots, Z_n)$ is **positively oriented**.

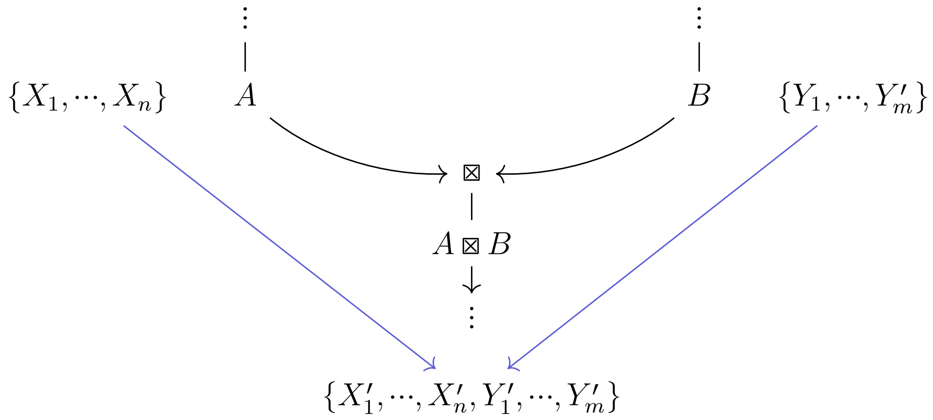
Remark 4.4.3. The equivalence relation of Definition 4.4.1 gives a visual conceptualisation of the links as "plugging" wires together. The phrase "plugging" is used informally throughout the literature ([3], [1], [2]). In what follows, $U_{\neg A} = \{X_1, \dots, X_n\}$ and $U_A = \{X'_1, \dots, X'_n\}$.

$$\begin{tikzcd}
 & (\mathrm{ax}) \arrow[dl, dash, bend right] \arrow[dr, dash, bend left] & \\
A \arrow[d] & & \neg A \arrow[d] \\
\vdots & & \vdots \\
\{X_1, \dots, X_n\} \arrow[rr, leftrightarrow] & & \{X'_1, \dots, X'_n\}
\end{tikzcd}$$

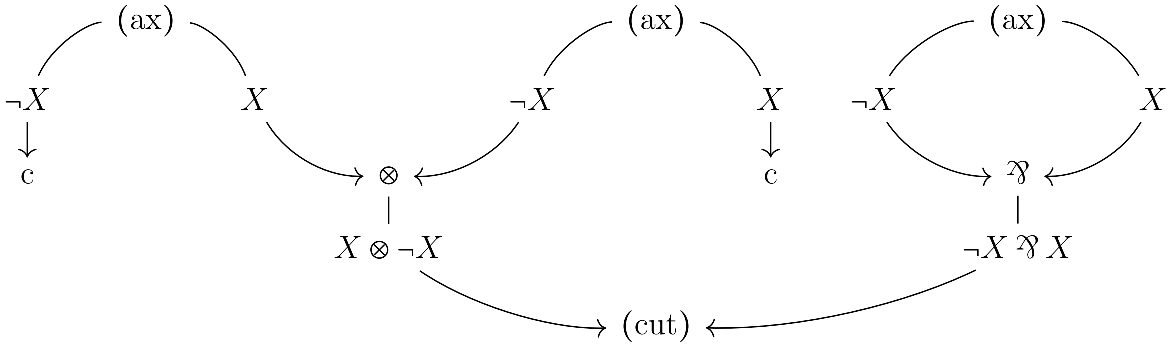
$$\begin{tikzcd}
\{X_1, \dots, X_n\} \arrow[rr, leftrightarrow] & & \{X'_1, \dots, X'_n\} \\
\vdots & & \vdots \\
A \arrow[u] & & \neg A \arrow[u] \\
 & (\mathrm{cut}) \arrow[ul, dash, bend left] \arrow[ur, dash, bend right] &
\end{tikzcd}$$

For this following diagram, we have $U_A = \{X_1, \dots, X_n\}, U_B = \{Y_1, \dots, Y_m\}, U_{A \boxtimes B} =$

$\{X_1', \dots, X_n', Y_1', \dots, Y_m'\}$, where $\boxtimes \in \{\otimes, \parr\}$.

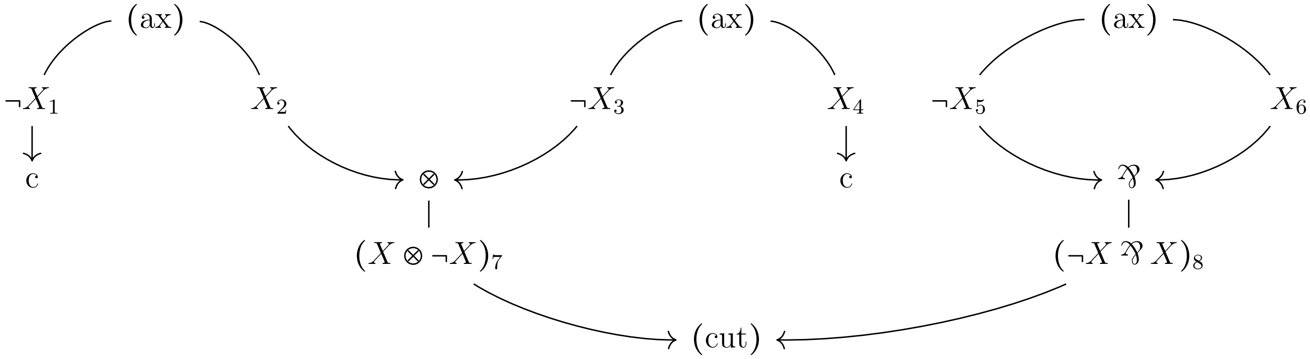


Example 4.4.4. Let π denote the following proof structure.



(117)

For clarity, we artificially place labels on the formulas so that we can refer to particular edges, but for all $i = 1, \dots, 8$ the notation Z_i, where $Z = X, \neg X, X \otimes \neg X, \neg X \parr X$, denotes the formula Z.



(118)

The only positively oriented persistent path π is

$$\neg X_1, X_2 (X \otimes \neg X)_7, (\neg X \parr X)_8, \neg X_5, X_6, (\neg X \parr X)_8, (X \otimes \neg X)_7, \neg X_3, X_4 \tag{119}$$

Question 4.4.5. Is the following true? If a proof structure π admits a looping persistent path then π is not a proof net.

An obvious first attempt to answer this question is to attempt to extract a short-trip from the looping persistent path by "traversing the interior of the loop". Does this proof technique work though?

4.5 Proofs as operators

A permutation σ on a finite set X induces a bounded linear operator on the Hilbert space FX freely generated by X, which is defined by $x \longmapsto \sigma x$ for each $x \in X$. Writing this linear operator as a matrix with respect to the basis X of FX we obtain an $n \times n$ matrix M_σ, where n is the number of elements of X, where each entry is either 0 of 1.

In Section **??** we will consider a particular choice of infinite dimensional Hilbert space $\mathbb{H}$ and then consider the space of bounded linear operators $\mathcal{B}(\mathbb{H})$ on $\mathbb{H}$. Since $\mathcal{B}(\mathbb{H})$ is infinite dimensional, we have that $\mathcal{B}(\mathbb{H})^n \cong \mathcal{B}(\mathbb{H})$ for every $n > 0$. Thus, if we read each entry 1 of M_σ as the identity operator, and each entry 0 as the zero operator, then each M_σ induces an operator $\mathbb{H} \longrightarrow \mathbb{H}$ (in other words, an element of $\mathcal{B}(\mathcal{H})$) allowing for each such matrix to be compared on the same footing. More precisely, each matrix is an element of *the same* Hilbert space, even though they differ in size.

We focus on the specific Hilbert space $\mathbb{H} = \ell^2$ of sequences $\underline{z} = (z_0, z_1, ...)$ of complex numbers which are square summable, ie, $\sum_{n=0}^{\infty} |z_n|^2$ converges. The idea of modelling proofs inside this Hilbert space is due to Girard [3] and the mathematics behind this model has been expounded upon by Hines [15].

The space $\mathbb{H} = \ell^2$ has an inner product defined as follows.

$$\left\langle \underline{z}, \underline{w} \right\rangle = \sum_{n=0}^{\infty} z_n \overline{w}_n \tag{120}$$

In fact, the sum $\mathbb{H}^m$ of m copies of $\mathbb{H}$ also has an inner product structure, defined by

$$\left\langle \left(\underline{z}^1, ..., \underline{z}^m\right), \left(\underline{w}^1, ..., \underline{w}^m\right) \right\rangle_{\mathbb{H}^m} = \sum_{j=1}^{m} \langle \left(\underline{z}^j, \underline{w}^j\right) \rangle_{\mathbb{H}} \tag{121}$$

We fix the standard basis for ℓ^2 consisting of sequences $\underline{e}^i$ such that all entries are equal to 0 except for the i^{th} which is equal to 1. We note that this basis is countably infinite. A basis for $\ell^2 \oplus \ell^2$ is given by all $(\underline{e}^i, 0)$ and $(0, \underline{e}^i)$ which is also countable, thus, bijections $\alpha : \mathbb{N} \coprod \mathbb{N} \longrightarrow \mathbb{N}$ induce isomorphisms $\ell^2 \longrightarrow \ell^2 \oplus \ell^2$. More explicitly, if $\alpha : \mathbb{N} \coprod \mathbb{N} \longrightarrow \mathbb{N}$ is such a bijection then there exists injective functions $\alpha_1, \alpha_2 : \mathbb{N} \longrightarrow \mathbb{N}$ which make the following diagram commute.

$$\begin{tikzcd}
\mathbb{N} \arrow[d, tail] \arrow[dr, tail, "\alpha_1"] & \\
\mathbb{N} \coprod \mathbb{N} \arrow[r, tail, "\alpha"] & \mathbb{N} \\
\mathbb{N} \arrow[u, tail] \arrow[ur, tail, "\alpha_2"'] &
\end{tikzcd} \tag{122}$$

The induced isomorphism $\hat{\alpha} : \ell^2 \longrightarrow \ell^2 \oplus \ell^2$ is then given by the following explicit formula, where $z = \sum_{i=0}^{\infty} z_i \underline{e}^i$:

$$\hat{\alpha}(z) = \sum_{i=0}^{\infty} \Big(z_{\alpha_1(i)} \underline{e}^i, z_{\alpha_2(i)} \underline{e}^i \Big) \tag{123}$$

The following calculation shows that $\hat{\alpha}$ is an isometry:

$$\begin{aligned}
\Big\langle \hat{\alpha}(\underline{z}), \hat{\alpha}(\underline{w}) \Big\rangle &= \Big\langle \sum_{i=0}^{\infty} \big(z_{\alpha_1(i)} \underline{e}^i, z_{\alpha_2(i)} \underline{e}^i \big), \sum_{i=0}^{\infty} \big(w_{\alpha_1(i)} \underline{e}^i, w_{\alpha_2(i)} \underline{e}^i \big) \Big\rangle \\
&= \Big\langle \sum_{i=0}^{\infty} z_{\alpha_1(i)} \underline{e}^i, \sum_{i=0}^{\infty} w_{\alpha_1(i)} \underline{e}^i \Big\rangle + \Big\langle \sum_{i=0}^{\infty} z_{\alpha_2(i)} \underline{e}^i, \sum_{i=0}^{\infty} w_{\alpha_2(i)} \underline{e}^i \Big\rangle \\
&= \sum_{i=0}^{\infty} z_{\alpha_1(i)} \overline{w}_{\alpha_i(i)} + \sum_{i=0}^{\infty} z_{\alpha_2(i)} \overline{w}_{\alpha_2(i)} \\
&= \sum_{i=0}^{\infty} z_i \overline{w}_i \\
&= \langle \underline{z}, \underline{w} \rangle
\end{aligned}$$

We claim that (123) can also be written as $\hat{\alpha}(z) = \big(p^*(z), q^*(z) \big)$ for operators $p, q : \ell^2 \longrightarrow \ell^2$ determined by continuity and the following conditions.

$$p(\underline{e}^i) = \underline{e}^{\alpha_1(i)}, \qquad q(\underline{e}^i) = \underline{e}^{\alpha_2(i)} \tag{124}$$

These maps are norm preserving and so are clearly bounded, thus we have well defined bounded, linear operators. It can be established by a direct calculation that these have adjoints respectively determined by continuity and the following conditions.

$$p^*(\underline{e}^i) = \underline{e}^{\alpha_1^{-1}(i)} \text{ if } \alpha_1^{-1}(i) \text{ exists, otherwise } p^*(\underline{e}^i) = 0 \tag{125}$$

$$q^*(\underline{e}^i) = \underline{e}^{\alpha_2^{-1}(i)} \text{ if } \alpha_2^{-1}(i) \text{ exists, otherwise } p^*(\underline{e}^i) = 0 \tag{126}$$

For example: let $w = \sum_{i=0}^{\infty} w_i \underline{e}^i$, then

$$\Big\langle p(z), w \Big\rangle = \sum_{i=0}^{\infty} z_i \overline{w}_{\alpha_1(i)} = \Big\langle z, p^*(w) \Big\rangle$$

we thus have the following formula.

$$\hat{\alpha} = p^* \oplus q^* \tag{127}$$

In a similar way, given any $n > 0$ along with a bijection $\alpha : \mathbb{N} \longrightarrow \coprod_{i=1}^{n} \mathbb{N}$, there is a corresponding induced isometric isomorphism $\hat{\alpha} : \mathbb{H} \longrightarrow \mathbb{H}^n$ which has an explicit formula, where $z = \sum_{i=0}^{\infty} z_i \underline{e}^i$:

$$\hat{\alpha}(z) = \sum_{i=0}^{\infty} \Big(z_{\alpha_1(i)} \underline{e}^i, ..., z_{\alpha_n(i)} \underline{e}^i \Big) \tag{128}$$

Example 4.5.1. A simple example is given by the following:

$$\begin{aligned} \alpha_1 : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto 2n \end{aligned} \qquad\qquad \begin{aligned} \alpha_2 : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto 2n+1 \end{aligned}$$

which induces $\alpha : \mathbb{N} \coprod \mathbb{N} \longrightarrow \mathbb{N}$, defined by $\alpha(n,1) = 2n$ and $\alpha(n,2) = 2n+1$. The functions $\alpha_1, \alpha_2, \alpha$ make the following a coproduct diagram:

$$\begin{tikzcd}
\mathbb{N} \arrow[d, tail] \arrow[dr, "\alpha_1"] & \\
\mathbb{N} \coprod \mathbb{N} \arrow[r, "\alpha"] & \mathbb{N} \\
\mathbb{N} \arrow[u, tail] \arrow[ur, "\alpha_2"'] &
\end{tikzcd} \tag{129}$$

and indeed α is a bijection. We thus have two functions:

$$\begin{aligned} p : \ell^2 &\longrightarrow \ell^2 \\ (z_0, z_1, ...) &\longmapsto (z_0, 0, z_1, 0, z_2, ...) \end{aligned} \qquad\qquad \begin{aligned} q : \ell^2 &\longrightarrow \ell^2 \\ (z_1, z_2, ...) &\longmapsto (0, z_0, 0, z_1, 0, ...) \end{aligned}$$

which have the following adjoints:

$$\begin{aligned} p^* : \ell^2 &\longmapsto \ell^2 \\ (z_0, z_1, ...) &\longmapsto (z_0, z_2, ...) \end{aligned} \qquad\qquad \begin{aligned} q^* : \ell^2 &\longrightarrow \ell^2 \\ (z_0, z_1, ...) &\longmapsto (z_1, z_3, ...) \end{aligned}$$

Aside 4.5.2. The following calculation shows that p^* is adjoint to p, the corresponding calculation for q is similar:

$$\begin{aligned} \big\langle p(z_0, z_1, ...), (w_0, w_1, ...) \big\rangle &= \big\langle (z_0, 0, z_1, 0, ...), (w_1, w_2, ...) \big\rangle \\ &= \big\langle (z_0, z_1, ...), (w_0, w_2, ...) \big\rangle \\ &= \big\langle (z_0, z_1, ...), p^*(w_0, w_1, ...) \big\rangle \end{aligned}$$

The function p^*, q^* induce $\hat{\alpha} = p^* \oplus q^* : \ell^2 \longrightarrow \ell^2 \oplus \ell^2$ defined by

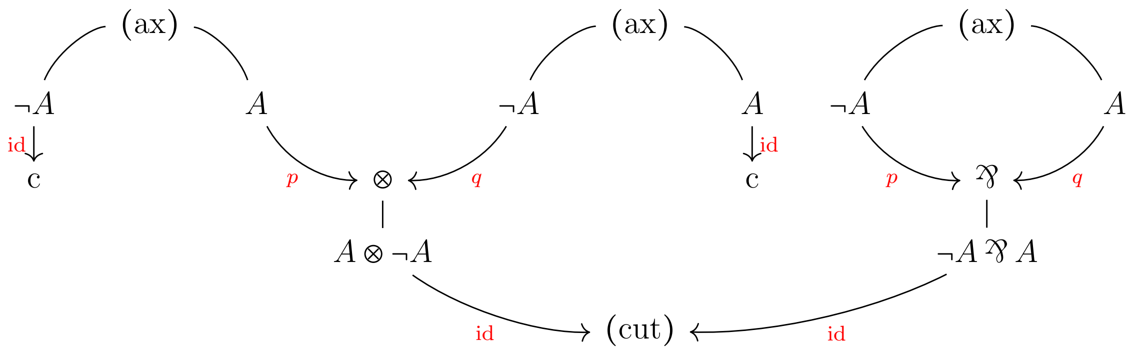
$$\hat{\alpha}(z_0, z_1, ...) = \big((z_0, z_2, ...), (z_1, z_3, ...) \big) \tag{130}$$

We make a few observations:

Lemma 4.5.3. *The functions p, q, p^*, q^* satisfy the following:*

- $p^* p = \mathrm{id}_{\ell^2} = q^* q$,
- $pp^* + qq^* = \mathrm{id}_{\ell^2}$,
- $p^* q = 0 = q^* p$.

Definition 4.5.4. Let π be a proof structure. We decorate the edges of π with the symbols p, q, id which will later be interpreted as the operators with the same name described in Section **??**. The labelling is done in the following way: the left premise of each tensor and each par link is labelled p and the right premise of each tensor and each par link is labelled q, the remaining edges are labelled id. An example is given as follows.



Each persistent path $\rho = (e_1, \dots, e_n)$ of π consists of edges e_i traversed π either forwards, or backwards. If the e_i is traversed forwards then we associate the symbol $w_i \in \{p, q, \mathrm{id}\}$ to e_i as determined by the label of e_i. If e_i is traversed backwards then we augment the label with an astrix $*$ and consider the symbol $w_i \in \{p^*, q^*, \mathrm{id}^*\}$. For example, the unique (assuming A is atomic), positively oriented persistent path in the above example has associated word

$$\mathrm{id}^*\, q\, \mathrm{id}\, \mathrm{id}^*\, q^* p\, \mathrm{id}\, \mathrm{id}^*\, p^*\, \mathrm{id} \tag{131}$$

Denote the operator of the same name as $w \in \{p, q, \mathrm{id}, p^*, q^*, \mathrm{id}^*\}$ by $\overline{w}$. The **operator associated to** ρ is

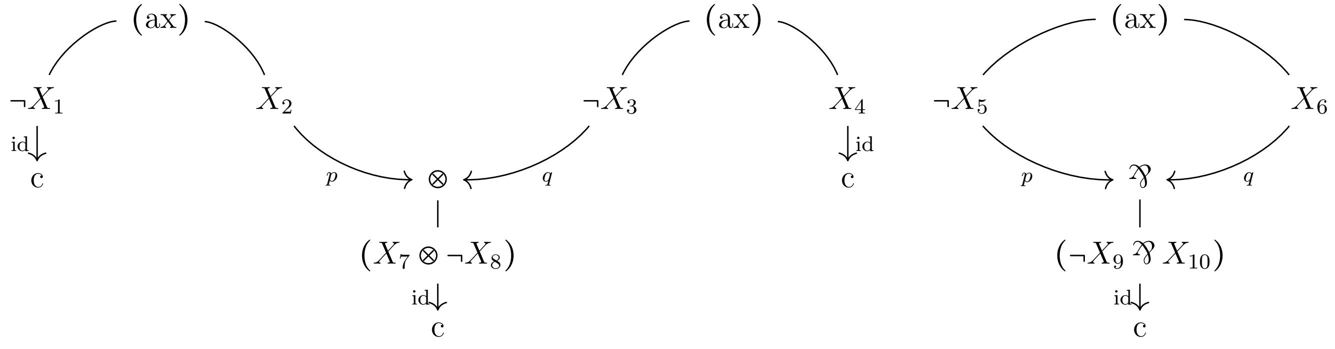
$$o_\rho := \overline{w_n} \circ \dots \circ \overline{w_1} \tag{132}$$

So, in the above example, the associated operator is $qq^*pp^* = \mathrm{id}$. We will see that since we obtained id, the above proof net is equivalent under cut reduction to a proof net consisting of a single axiom link.

Definition 4.5.5. Let π be a proof structure and ζ the proof structure obtained by removing all the cut links of π (and appending conclusion links to the premises of the cut links removed). Consider all the unoriented atoms of all premises to conclusion links of ζ, say there are n of these. We construct an $n \times n$ matrix $[\![\pi]\!]$, we will use these unoriented atoms as the indices for the rows and columns of $[\![\pi]\!]$. For each persistent path ρ of ζ, form o_ρ of Definition 4.5.4 and let this be entry BA of $[\![\pi]\!]$ where ρ begins at B and ends at A. The remaining entries are 0.

Example 4.5.6. Consider π of Example 4.4.4. We remove the cut link to obtain a proof-structure π'. Label the left premise of each tensor and each par link by p and the right premise of each tensor and each par link by q (indeed these are the same p and q

as in Section **??**). Label the remaining edges by the identity map id (this is the identity on the space ℓ^2). For convenience, we have added artificial labels to the formulas.



(133)

Now we calculate the persistent paths in π' along with their associated linear operators. These are as follows.

$$\nu_1 = (\neg X_1, X_2, (X_7 \otimes \neg X)_8) \qquad o_{\nu_1} = \mathrm{id}\, p\, \mathrm{id}^* = p \tag{134}$$
$$\nu_2 = ((X_7 \otimes \neg X_8), X_2, \neg X_1) \qquad o_{\nu_2} = \mathrm{id}\, p^*\, \mathrm{id}^* = p^* \tag{135}$$
$$\nu_3 = (X_4, \neg X_3, (X_7 \otimes \neg X_8)) \qquad o_{\nu_3} = \mathrm{id}\, q\, \mathrm{id}^* = q \tag{136}$$
$$\nu_4 = ((X_7 \otimes \neg X_8), \neg X_3, X_4) \qquad o_{\nu_4} = \mathrm{id}\, q^*\, \mathrm{id}^* = q^* \tag{137}$$
$$\nu_5 = ((\neg X_9 ⅋ X_{10}), \neg X_5, X_6, (\neg X_9 ⅋ X_{10})) \qquad o_{\nu_5} = \mathrm{id}\, qp^*\, \mathrm{id}^* = qp^* \tag{138}$$
$$\nu_6 = ((\neg X_9 ⅋ X_{10}), X_6, \neg X_5, (\neg X_9 ⅋ X_{10})) \qquad o_{\nu_6} = \mathrm{id}\, pq^*\, \mathrm{id}^* = pq^* \tag{139}$$

Hence $[\![\pi]\!]$ is the following matrix 4×4 matrix, where we assume respectively that index $1, 2, 3, 4, 5, 6$ corresponds to conclusion $\neg X_1, X_7, \neg X_8, X_4, \neg X_9, X_{10}$.

$$[\![\pi]\!] = \begin{array}{c|cccccc} & \neg X_1 & X_7 & \neg X_8 & X_4 & \neg X_9 & X_{10} \\ \hline \neg X_1 & 0 & p^* & 0 & 0 & 0 & 0 \\ X_7 & p & 0 & 0 & 0 & 0 & 0 \\ \neg X_8 & 0 & 0 & 0 & q^* & 0 & 0 \\ X_4 & 0 & 0 & q & 0 & 0 & 0 \\ \neg X_9 & 0 & 0 & 0 & 0 & 0 & pq^* \\ X_{10} & 0 & 0 & 0 & 0 & qp^* & 0 \end{array} \tag{140}$$

Remark 4.5.7. There are more paths which begin and end at conclusions in π' than the persistent paths $\nu_1, ..., \nu_6$. For example, there is the following path.

$$\rho := (\neg X_1, X_2, \neg X_3, X_4) \tag{141}$$

The path ρ has corresponding operator $o_\rho = q^* p$. We notice that this is the zero operator. This reflects the fact that ρ is not a persistent path.

4.6 Geometry of Interaction One

Definition 4.6.1. Let π be a proof structure and ζ the proof structure obtained by removing all cut-links in π (and appending conclusion links to the premises of the cut links removed). Say π has atomic atoms $X_1, \ldots, X_m$ amongst the premises to its conclusion links, and say it has atomic atoms $Y_1, \ldots, Y_n$ amongst the premises of the cut links. We will construct a $(2n+m) \times (2n+m)$ matrix σ and use $X_1, \ldots, X_m, Y_1, Y_1', \ldots, Y_n, Y_n'$ as labels for the indices of this matrix.

For each $i = 1, \ldots, n$ consider the minor with rows and columns Y_i, Y_i'. Set this to be the matrix

$$\begin{array}{c|cc} & Y_i & Y_i' \\ \hline Y_i & 0 & 1 \\ Y_i' & 1 & 0 \end{array} \tag{142}$$

The remaining entries are 0.

The point is that $[\![\pi]\!]$ contains the information of the persistent paths of π once the cut links have been removed, and σ contains the information of the cut links. This allows us to talk about persistent paths of π which traverse cuts some chosen amount of times in a way made precise by the following Proposition.

Proposition 4.6.2. *Let X, Y be amongst the unoriented atoms of all premises to all conclusion links of some proof structure π. The operator given by the persistent path from X to Y and whic traverses cut links exactly m times is the YX entry of the matrix $[\![\pi]\!](\sigma[\![\pi]\!])^m$. Moreover, if no such path exists then this entry is equal to 0.*

Proof. Both $[\![\pi]\!]$ and σ can be thought of as weighted incidence matrices of the graph π. This makes the first claim clear. For the second, first notice the YX entry of $[\![\pi]\!](\sigma[\![\pi]\!])^m$ is the composition of some sequence of operators which in turn are given by persistent paths in ζ, the proof structure given by removing the cut links of π. Since the incidences described by σ are exactly the ones given by the way persistent paths connect at cut links, we must have some corresponding persistent path in π as claimed. □

Corollary 4.6.3. *If π is a proof net and σ_m is as defined in Definition 4.6.1 then there exists an integer $n > 0$ such that $[\![\pi]\!](\sigma_m[\![\pi]\!])^n = 0$.*

Proof. Follows from Proposition 4.6.2 along with the fact that persistent paths in proof nets are finite (Lemma 4.4.5). □

Definition 4.6.4. We define

$$\mathrm{Ex}([\![\pi]\!]) = (I - \sigma^2)([\![\pi]\!] + [\![\pi]\!]\sigma[\![\pi]\!] + [\![\pi]\!]\sigma[\![\pi]\!]\sigma[\![\pi]\!] + \cdots)(I - \sigma^2) \tag{143}$$

which by Corollary 4.6.3 is a well defined matrix. This is the **execution formula**.

The Execution Formula (143) is due to Girard [3]. The proof here that $\mathrm{Ex}([\![\pi]\!])$ is well defined (Corollary 4.6.3) is new though, and differs significantly to that given in [3] (recall, Girard *never* used persistent paths in his paper). The same comment holds for Theorem 4.6.7 below.

Example 4.6.5. We continue with π from Examples 4.4.4 and 4.5.6. Using the same indexing as Example 4.5.6 we have that σ is the following matrix.

$$\sigma = \begin{array}{c} \\ \neg X \\ X_7 \\ \neg X_8 \\ X_4 \\ \neg X_9 \\ X_{10} \end{array} \begin{array}{c} \begin{array}{cccccc} \neg X_1 & X_7 & \neg X_8 & X_4 & \neg X_9 & X_{10} \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

This matrix reflects the "plugging" in the unique positively oriented persistent path of π of X_7 into $\neg X_9$ and of $\neg X_8$ into X_{10}. Notice that this matrix satisfies the following.

$$I - \sigma^2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{144}$$

Consider also $\llbracket\pi\rrbracket\sigma\llbracket\pi\rrbracket$, which is a matrix whose ij^{th} entry corresponds to the sum of operators corresponding to the paths in π' which traverse the cut once, where the start of the path is the conclusion in π' with label corresponding to column j, and whose end point is the conclusion with label corresponding to row i. In our current example this is given as follows:

$$\llbracket\pi\rrbracket\sigma\llbracket\pi\rrbracket = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & p^*pq^* \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & q^*qp^* & 0 \\ 0 & 0 & 0 & pq^*q & 0 & 0 \\ qp^*p & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & q^* \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & p^* & 0 \\ 0 & 0 & 0 & p & 0 & 0 \\ q & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{145}$$

Multiplying by $\sigma\llbracket\pi\rrbracket$ yields:

$$\llbracket\pi\rrbracket\sigma\llbracket\pi\rrbracket\sigma\llbracket\pi\rrbracket = \begin{bmatrix} 0 & 0 & 0 & p^*pq^*q & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ q^*qp^*p & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{146}$$

The matrix $\llbracket\pi\rrbracket\sigma\llbracket\pi\rrbracket\sigma\llbracket\pi\rrbracket\sigma\llbracket\pi\rrbracket$ is the zero matrix and therefore $\llbracket\pi\rrbracket(\sigma\llbracket\pi\rrbracket)^n = 0$ for $n > 2$.

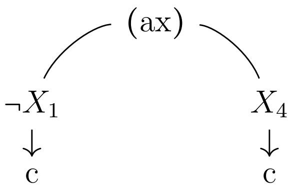
Thus

$$[\![\pi]\!] + [\![\pi]\!]\sigma[\![\pi]\!] + [\![\pi]\!]\sigma[\![\pi]\!]\sigma[\![\pi]\!] + \cdots = \begin{array}{c|cccccc} & \neg X_1 & X_7 & \neg X_8 & X_4 & \neg X_9 & X_{10} \\ \hline \neg X_1 & 0 & 0 & 0 & 1 & 0 & q^* \\ X_7 & 0 & 0 & 0 & 0 & 1 & 0 \\ \neg X_8 & 0 & 0 & 0 & 0 & 0 & 1 \\ X_4 & 1 & 0 & 0 & 0 & p^* & 0 \\ \neg X_9 & 0 & 1 & 0 & p & 0 & 0 \\ X_{10} & q & 0 & 1 & 0 & 0 & 0 \end{array} \tag{147}$$

The execution formula is thus

$$\mathrm{Ex}([\![\pi]\!]) = \begin{array}{c|cccccc} & \neg X_1 & X_7 & \neg X_8 & X_4 & \neg X_9 & X_{10} \\ \hline \neg X_1 & 0 & 0 & 0 & 1 & 0 & 0 \\ X_7 & 0 & 0 & 0 & 0 & 0 & 0 \\ \neg X_8 & 0 & 0 & 0 & 0 & 0 & 0 \\ X_4 & 1 & 0 & 0 & 0 & 0 & 0 \\ \neg X_9 & 0 & 0 & 0 & 0 & 0 & 0 \\ X_{10} & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \tag{148}$$

What happens if we perform the same process to π after we have performed cut-elimination? Under this process, π corresponds to the proof consisting of a single axiom link:



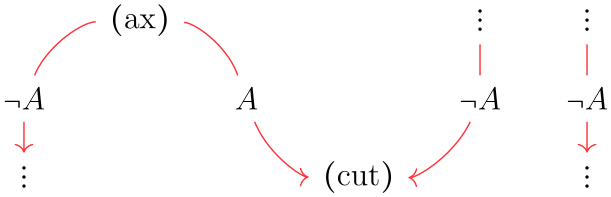
(149)

which corresponds to the matrix

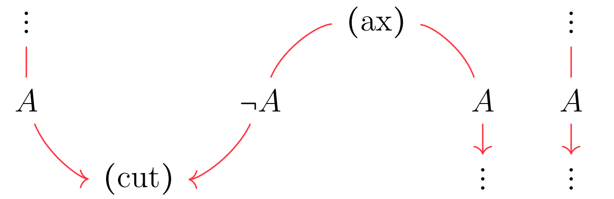
$$\begin{array}{c|cc} & \neg X_1 & X_4 \\ \hline \neg X_1 & 0 & 1 \\ X_4 & 1 & 0 \end{array} \tag{150}$$

which appears as a minor in (146). Theorem 4.6.7 states that this is not a coincidence.

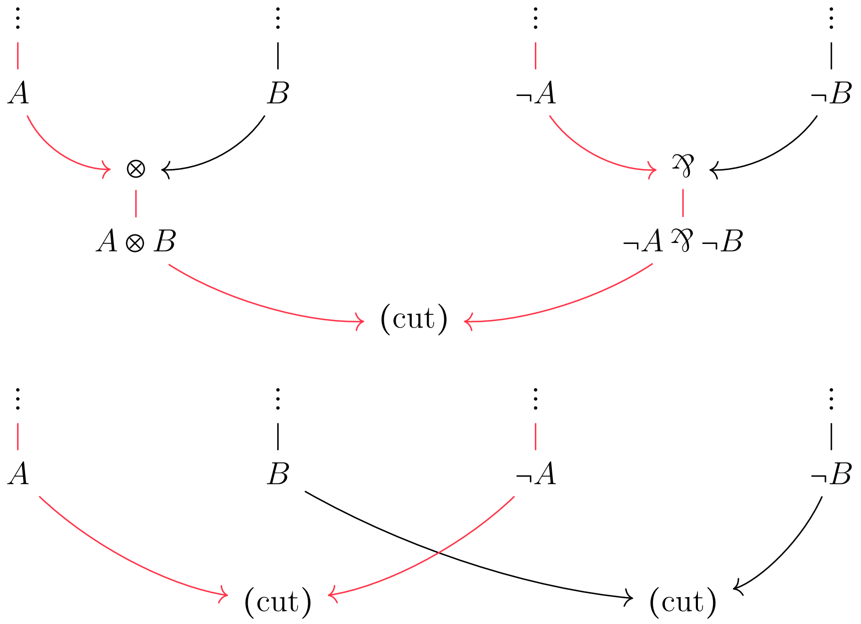
Definition 4.6.6. Let $\gamma : \pi \longrightarrow \pi'$ be a reduction, then there is a bijection between the set of persistent paths of π and the set of persistent path on π' (hence, *persistent* paths). This is according the following schema:



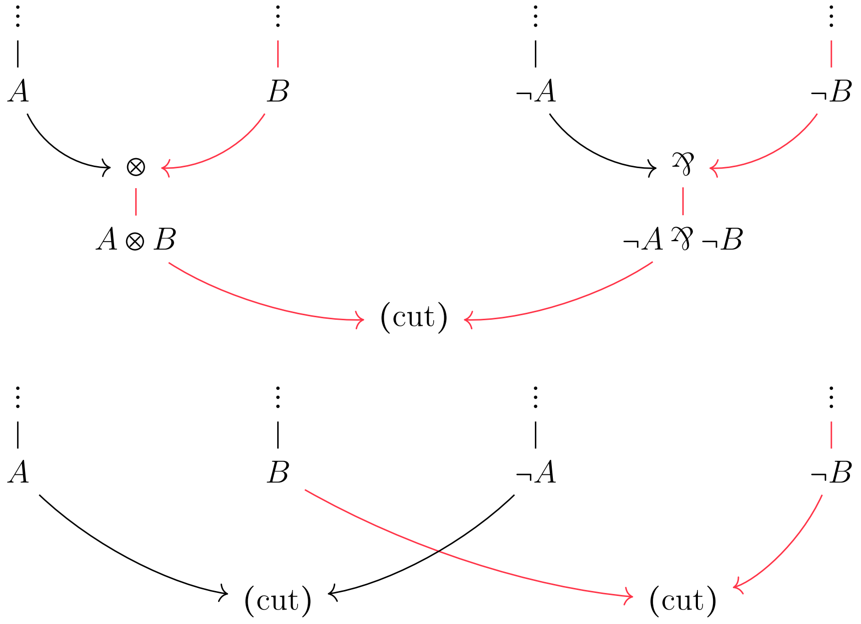
(151)



(152)



(153)



(154)

Theorem 4.6.7 (Geometry of Interaction One)**.** *Let π be a proof net and ζ the cut-free proof equivalent under cut elimination to π. Then the matrix $[\![\zeta]\!]$ exists as a minor in*

$\mathrm{Ex}(\llbracket\pi\rrbracket)$ *and any entry in* $\mathrm{Ex}(\llbracket\pi\rrbracket)$ *which is not in the minor corresponding to* $\llbracket\zeta\rrbracket$ *is equal to 0.*

Proof. It is clear by inspection of the rules in Definition 4.6.6 that the transformations preserve persistency of paths. This establishes the first claim.

On the level of words, the rules in Definition 4.6.6 replace instances of p^*p and q^*q with 1. That this is observed by the execution formula follows from the fact that as operators $p^*p = q^*q = 1$ (Lemma 4.5.3).

There are also entries in $\llbracket\pi\rrbracket + \llbracket\pi\rrbracket\sigma\llbracket\pi\rrbracket + \llbracket\pi\rrbracket\sigma\llbracket\pi\rrbracket\sigma\llbracket\pi\rrbracket + \dots$ which do not correspond to persistent paths in π, but instead correspond to persistent paths in ζ, the proof structure obtained by removing the cut links in π. However, these are sent to 0 by the presence of the matrices $(I - \sigma^2)$ in the execution formula. □

5 Algebra

5.1 Graded rings, modules, and algebras

Let $\Bbbk$ be a commutative ring. A polynomial ring $\Bbbk[x_1, \dots, x_n]$ can be decomposed as a direct sum of elements according to their degrees: $\Bbbk[x_1, \dots, x_n] = \bigoplus_{d\geq 0} \Bbbk[x_1, \dots, x_n]_d$ where $\Bbbk[x_1, \dots, x_n]_d$ is the abelian group of polynomials of degree d. Graded rings/modules generalise this structure.

Definition 5.1.1. Let G be a totally ordered group. A G**-graded ring** is a ring A along with a G**-grading**, ie, a group isomorphism

$$A \cong \bigoplus_{g\in G} A_g \tag{155}$$

for some collection of subgroups $\{A_g \subseteq A\}_{g\in G}$. Furthermore, A is required to be such that $A_g A_h \subseteq A_{g+h}$ for all $g, h \in G$.

An element $a \in A$ such that $a \in A_g$ is **homogeneous of degree** g. An ideal which can be generated by homogeneous elements is a **homogeneous ideal**.

Let A be a G-graded ring, a G**-graded** A**-module** M is an A-module along with a G**-grading**, ie a group isomorphism

$$M \cong \bigoplus_{g\in G} M_g \tag{156}$$

for some collection of subgroups $\{M_g \subseteq M\}_{g\in G}$. Furthermore, M is required to be such that $A_g M_h \subseteq M_{g+h}$ for all $g, h \in G$.

Lemma 5.1.2. *An ideal* I *is homogeneous if and only if* $I = \bigoplus_{g\in G}(A_g \cap I)$.

Example 5.1.3. If $A \cong \bigoplus_{g\in G} A_g$ is a graded algebra and $I \subseteq A$ is a homogeneous ideal, then A/I is graded as per:

$$A/I \cong \bigoplus_{g\in G} A_g / \bigoplus_{g\in G}(A_g \cap I) \cong \bigoplus_{g\in G} A_g / A_g \cap I \tag{157}$$

The most important case will be when $G = \mathbb{Z}$, we now focus on this case, though most of what follows holds in greater generality.

Definition 5.1.4. Let A be a $\mathbb{Z}$-graded ring and M, N two $\mathbb{Z}$-graded A-modules. A **morphism of $\mathbb{Z}$-graded A-modules of degree** $i \in \mathbb{Z}$ is an A-module homomorphism $\varphi : A \longrightarrow B$ subject to $\forall j \in \mathbb{Z}, f(A_j) \subseteq B_{j+i}$ we denote the A-module of such morphisms by $\operatorname{Hom}(A, B)$.

This gives rise to a $\mathbb{Z}$-graded module

$$\operatorname{Hom}(A, B) \coloneqq \bigoplus_{i \in \mathbb{Z}} \operatorname{Hom}(A, B)_i \tag{158}$$

Moreover, the tensor product is naturally a $\mathbb{Z}$-graded module with grading:

$$A \otimes B \cong \bigoplus_{\substack{i \in \mathbb{Z} \\ n+m=i}} A_n \otimes B_m \tag{159}$$

What if A, B are $\mathbb{Z}$-graded *algebras*? All the definitions go through as expected except for the tensor product which has multiplication defined by

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = (-1)^{\deg a_2 \deg b_1}(a_1 a_2 \otimes b_1 b_2) \tag{160}$$

This multiplication law is necessary for the differential cases in order to make $\operatorname{Hom}(A, B) \otimes A \longrightarrow B$ given on pure tensors by $f \otimes a \longmapsto f(a)$ a morphism of chain complexes.

Definition 5.1.5. Let A be a ring, a **differential, $\mathbb{Z}$-graded A-module** is a $\mathbb{Z}$-graded A-module M along with a **differential**, ie, a linear map $d : A \longrightarrow A$ such that for all $m \in M$ we have $\deg f(m) = \deg m - 1$. A **morphism of differential, $\mathbb{Z}$-graded A-modules** M, N is a morphism of $\mathbb{Z}$-graded modules $\varphi : M \longrightarrow N$ such that for all $i \in \mathbb{Z}$ the following diagram commutes:

$$\begin{tikzcd} M_i \arrow[r, "\varphi"] \arrow[d, "d_M"] & N_i \arrow[d, "d_N"] \\ M_{i-1} \arrow[r, "\varphi"] & N_{i-1} \end{tikzcd} \tag{161}$$

We often say “graded” in place of $\mathbb{Z}$-graded.

Every differential, graded module is naturally a chain complex.

Definition 5.1.6. Let $(A, d_A), (B, d_B)$ be differential, graded k-algebras (for some commutative ring k), the tensor product is naturally equipped with the following differential:

$$d_{A \otimes B}(a \otimes b) = d_A(a) \otimes b + (-1)^{\deg a} a \otimes d_B(b) \tag{162}$$

Similarly, $\operatorname{Hom}(A, B)$ is naturally equipped with the following differential:

$$d_H(f) = d_B(f) - (-1)^{\deg f} f(d_A) \tag{163}$$

Remark 5.1.7. Let $\psi : \mathrm{Hom}(A,B) \otimes A \longrightarrow B$ be the evaluation map, ie, the map given on pure tensors by $\psi(f \otimes a) = f(a)$. We claim this is a chain map. We require commutativity of the following diagram:

$$\begin{tikzcd}
(\mathrm{Hom}(A,B) \otimes A)_n \arrow[r, "\psi"] \arrow[d, "d_{H\otimes A}"] & B_n \arrow[d, "d_B"] \\
(\mathrm{Hom}(A,B) \otimes A)_{n-1} \arrow[r, "\psi"] & B_{n-1}
\end{tikzcd} \tag{164}$$

Unpacking definitions, for all pure tensors $f \otimes a \in (\mathrm{Hom}(A,B) \otimes A)_n$ we have

$$d_B(\psi)(f \otimes a) = d_B(f(a)) \tag{165}$$

and

$$\begin{aligned}
\psi d_{H\otimes A}(f \otimes a) &= \psi(d_H f \otimes a + (-1)^{\deg f} f \otimes d_A(a)) \\
&= d_H f(a) + (-1)^{\deg f} f(d_A(a)) \\
&= d_B(f(a)) - (-1)^{\deg f} f(d_A(a)) + (-1)^{\deg f} f(d_A(a)) \\
&= d_B(f(a))
\end{aligned}$$

so indeed we have a morphism of differential, graded algebras.

Consider the $\mathbb{Z}$-graded ring $S := k[x_0, ..., x_n]$. We can define a ring homomorphism $\varphi : S \longrightarrow S$ given by multiplication by x_0, strictly speaking though this fails to be a morphism of $\mathbb{Z}$-graded rings as, for example, the degree 0 element 1 is mapped to the degree 1 element x_0.

There is an obvious fix to this, we simply shift the grading of the first copy of S.

Definition 5.1.8. Let A be a G-graded ring. We denote by $A(g)$ the graded ring which is identical as a ring to A, but with the grading shifted by g, more concretely, if for an arbitrary G-graded ring B we denote by B_g the subgroup generated by the degree g elements, then we have

$$A(g)_h = A_{g+h} \tag{166}$$

In the special case where $G = \mathbb{Z}$, the differential denoted $d_{A(n)}$ is given by $d_{A(n)}(a) = (-1)^n d_A(a)$.

Example 5.1.9. We have a well defined morphism of graded rings

$$S(-1) \xrightarrow{(x_0)} S \tag{167}$$

We conclude this Section with one last chain complex constructor: let M be an R-module and $y \in R$ an arbitrary element of R. Let $\mathscr{G}$ be a chain complex, we denote by $K(y)$ (see Definition B.0.6 for a justification of this choice of notation) the following chain complex:

$$0 \longrightarrow R \xrightarrow{y} R \longrightarrow 0 \tag{168}$$

5.2 Exterior algebra

Throughout, R is a commutative ring with unit and M a left R-module.

Definition 5.2.1. The **exterior algebra** associated to M is the pair $(\bigwedge M, \iota : M \longrightarrow \bigwedge M)$ satisfying the following universal property: if N is an R-algebra, and $f : M \longrightarrow N$ is an R-module homomorphism such that for all $m \in M, f(m)^2 = 0$ then there exists a unique R-algebra homomorphism $g : \bigwedge M \longrightarrow N$ making the following diagram commute:

$$\begin{tikzcd}
M \arrow[r, "\iota"] \arrow[dr, "f"'] & \bigwedge M \arrow[d, "g"] \\
& N
\end{tikzcd} \tag{169}$$

Moreover, if N is graded and $f(M) \subseteq N_1$ then g is a morphism of graded modules.

Remark 5.2.2. Existence of the exterior algebra is given by taking $\bigwedge M$ to be, where m ranges over all $m \in M$:

$$\bigwedge M := \bigotimes M / m \otimes m \tag{170}$$

Remark 5.2.3. If M is free and of finite rank, and $v_1, ..., v_n$ is a basis for M, then a basis for $\bigwedge M$ as a vector space is given by

$$\{v_{i_1} \wedge \cdots \wedge v_{i_d} \mid 1 \leq d \leq n, 1 \leq i_1 < \cdots < i_d \leq n\} \tag{171}$$

which is a set of size 2^n.

Proposition 5.2.4. *Let $\varphi : M \longrightarrow N$ be an R-module homomorphism. Then there exists a unique morphism $\wedge\varphi : \wedge M \longrightarrow \wedge N$ such that the following diagram commutes:*

$$\begin{tikzcd}
M \arrow[r, "\varphi"] \arrow[d] & N \arrow[d] \\
\wedge M \arrow[r, "\wedge\varphi"] & \wedge N
\end{tikzcd} \tag{172}$$

Definition 5.2.5. As per Example 5.1.3 we have that the exterior algebra is $\mathbb{Z}$-graded. We denote the degree d elements of $\bigwedge M$ by $\bigwedge^d M$.

There are two canonical operators on the exterior algebra, which we now explain.

Definition 5.2.6. Let $x \in \bigwedge M$ be an arbitrary element. We define

$$\begin{aligned} x \wedge \_ : \bigwedge M &\longrightarrow \bigwedge M \\ x_1 \wedge \cdots \wedge x_n &\longmapsto x \wedge x_1 \wedge \cdots \wedge x_n \end{aligned}$$

The second map is a bit harder to explain. We begin with some preliminary observations.

Lemma 5.2.7. *Let M be free and of finite rank. Then*

$$\bigwedge^d M^* \cong (\bigwedge^d M)^* \tag{173}$$

Proof. Let $\lambda_1, ..., \lambda_n$ be elements of M^*. Define the following functional:

$$\begin{aligned} M^d &\longrightarrow R \\ (m_1, ..., m_d) &\longmapsto \det\big((\lambda_i m_j)_{ij}\big) \end{aligned}$$

This indeed is bilinear and so induces a map $M^{\otimes d} \longrightarrow R$ and moreover is such that any pure tensor with repeated elements maps to 0, thus we obtain a map

$$\bigwedge M \longrightarrow R \tag{174}$$

We have thus described a homomorphism $M^{*d} \longrightarrow R$ which indeed is bilinear and maps tuples with repeated elements to 0, thus we have described a function

$$\varphi : \bigwedge^d M^* \longrightarrow \big(\bigwedge^d M\big)^* \tag{175}$$

It remains to show that this is an isomorphism, and for this we use for the first time that M is free of finite rank. Let $v_{i_1}, ..., v_{i_d} \in M$ be a basis. One can show

$$\varphi(v_{i_1} \wedge \cdots \wedge v_{i_d}) = (v_{i_1} \wedge \cdots \wedge v_{i_d})^* \tag{176}$$

and so φ maps onto a basis for $\big(\bigwedge^d M\big)^*$ so in particular φ is surjective. Since φ is a surjective map between vector spaces of the same, finite dimension, it must therefore also be injective. □

Remark 5.2.8. Another simple but important observation is that $\bigwedge^d \_$ is a functor.

We can now define the second canonical map.

Definition 5.2.9. Assume that M is free of finite rank. Let $\eta \in M^*$. There is the following sequence of compositions

$$\begin{tikzcd}
\bigwedge^d M \arrow[r] & \bigwedge^d M^{**} \arrow[r] & \big(\bigwedge^d M^*\big)^* \arrow[d, "(\eta\wedge\_)^*"] \\
\bigwedge^{d-1} M & \bigwedge^{d-1} M^{**} \arrow[l] & \big(\bigwedge^{d-1} M^*\big)^* \arrow[l]
\end{tikzcd} \tag{177}$$

The resulting map $\bigwedge^d M \longrightarrow \bigwedge^{d-1} M$ is **contraction** and is denoted by $\eta\lrcorner$.

For an element $x \in M$ we often denote $x \wedge \_$ by x and $x^*\lrcorner$ by x^*.

Remark 5.2.10. We can follow the sequence of homomorphism (177) to obtain an explicit formula for the contraction map. To this end, let $v_1, ..., v_n$ be a basis for M and observe the following calculation:

$$\begin{aligned} v_{i_1} \wedge \cdots \wedge v_{i_d} &\longmapsto v_{i_1}^{**} \wedge \cdots \wedge v_{i_d}^{**} \\ &\longmapsto (v_{i_1}^{*} \wedge \cdots \wedge v_{i_d}^{*})^* \\ &\longmapsto (v_{i_1}^{*} \wedge \cdots \wedge v_{i_d}^{*})^* \circ (\eta \wedge \_) \end{aligned}$$

We then have for any basis vector $(v_{j_1}^* \wedge \cdots \wedge v_{j_{d-1}}^*)^* \in (\bigwedge^{d-1} M^*)^*$ that

$$\begin{aligned} &(v_{i_1}^{*} \wedge \cdots \wedge v_{i_d}^{*})^* \circ (\eta \wedge \_)(v_{j_1}^* \wedge \cdots \wedge v_{j_{d-1}}^*) && (178) \\ &\qquad = (v_{i_1}^{*} \wedge \cdots \wedge v_{i_d}^{*})^* (\eta \wedge v_{j_1}^* \wedge \cdots \wedge v_{j_{d-1}}^*) && (179) \end{aligned}$$

By writing $\eta = \eta(v_1)v_1^* + \cdots + \eta(v_n)v_n^*$ we have

$$\begin{aligned} \eta \wedge v_{j_1}^* \wedge \cdots \wedge v_{j_{d-1}}^* &= (\eta(v_1)v_1^* + \cdots + \eta(v_n)v_n^*) \wedge v_{j_1}^* \wedge \cdots \wedge v_{j_{d-1}}^* \\ &= \sum_{k=1}^n \eta(v_k) v_k^* \wedge v_{j_1}^* \wedge \cdots \wedge v_{j_{d-1}}^* \end{aligned}$$

so returning to (179), we have

$$(v_{i_1}^{*} \wedge \cdots \wedge v_{i_d}^{*})^* (\sum_{k=1}^n \eta(v_k) v_k^* \wedge v_{j_1}^* \wedge \cdots \wedge v_{j_{d-1}}^*)$$

which, if there exists $l \in \{1, ..., d\}$ such that $(i_1, ..., i_{\hat{l}}, ..., i_d) = (j_1, ..., j_{d-1})$ is equal to $(-1)^{l-1}\eta(v_{i_l})$. Hence, traversing the other direction of (177) we see that this corresponds to the element

$$\eta \lrcorner (v_{i_1} \wedge \cdots \wedge v_{i_d}) = \sum_{j=1}^d (-1)^{j-1} \eta(v_{i_j}) v_{i_1} \wedge \cdots \wedge \hat{v_{i_j}} \wedge \cdots \wedge v_{i_d} \qquad (180)$$

Remark 5.2.11. Notice that from (177) and the fact that $\eta \wedge \eta \wedge \_ = 0$ it follows that contraction is a differential. Thus there is a chain complex

$$L(M) := \cdots \wedge^2 M \xrightarrow{\eta \lrcorner} M \xrightarrow{\eta} R \longrightarrow 0 \qquad (181)$$

In fact, more can be said, we return to this after considering some category theoretic facts about the exterior algebra.

5.2.1 Category theoretic properties of the exterior algebra

The exterior algebra admits some properties which are described well using the language of category theory.

Definition 5.2.12. A **super algebra** is a graded, commutative algebra A with the following properties:

- for all $a, b \in A$ we have $ab = (-1)^{\deg a \deg b} ba$,
- if $a \in A$ is homogeneous of odd degree, then $a^2 = 0$.

Example 5.2.13. The exterior algebra $\bigwedge M$ of a module M is a super algebra.

Lemma 5.2.14. *The wedge product $\wedge(\_) : mod_R \longrightarrow sAlg_R$ is a functor. This follows from Remark 5.2.2 and Proposition 5.2.4.*

Definition 5.2.15. We let mod_R denote the category of commutative, left R-modules, and sAlg_R the category of R-super algebras.

We denote by $(\_)_1 : \mathrm{sAlg}_R \longrightarrow \mathrm{mod}_R$ the functor which takes a super algebra to its degree 1 component.

Remark 5.2.16. The functor $\wedge(\_)$ is left adjoint to $(\_)_1$. This follows from Proposition 5.2.4.

We now use these observations to prove that there is a canonical isomorphism $\wedge(M) \otimes \wedge(N) \longrightarrow \wedge(M \oplus N)$.

Proposition 5.2.17. *For any pair of R-algebras M, N there is an isomorphism*

$$\Psi : \wedge(M \oplus N) \longrightarrow \wedge M \otimes \wedge N$$
$$\psi(m, n) = m \otimes 1 + 1 \otimes n$$

Proof. By Observation 5.2.16 and that the tensor product acts as a coproduct in the category of Alg_R of commutative R-algebras, we have the following commutative diagram, where the horizontal arrows are composition and all vertical arrows are natural isomorphisms, note also we simply write H in place of Hom:

$$\begin{tikzcd}
H(\wedge(M \oplus N), \wedge M \otimes \wedge N) \times H(\wedge M \otimes \wedge N, \wedge(M \oplus N)) \arrow[r] \arrow[d] & H(\wedge(M \oplus N), \wedge(M \oplus N)) \arrow[ddd] \\
H(M \oplus N, (\wedge M \otimes \wedge N)_1) \times H(\wedge M, \wedge(M \oplus N)) \times H(\wedge N, \wedge(M \oplus N)) \arrow[d] & \\
H(M \oplus N, M \oplus N) \times H(M, M \oplus N) \times H(N, M \oplus N) \arrow[d] & \\
H(M \oplus N, M \oplus N) \times H(M \oplus N, M \oplus N) \arrow[r] & H(M \oplus N, M \oplus N)
\end{tikzcd}$$

Since the image of $\mathrm{id}_{M \oplus N}$ under

$$H(M \oplus N, M \oplus N) \times H(M \oplus N, M \oplus N) \longrightarrow H(M \oplus N, M \oplus N) \longrightarrow H(\wedge(M \oplus N), \wedge(M \oplus N))$$

is $\mathrm{id}_{\wedge(M \oplus N)}$ it follows that there are canonical morphisms $\psi : \wedge(M \oplus N) \longrightarrow \wedge M \otimes \wedge N$ and $\psi' : \wedge M \otimes \wedge N \longrightarrow \wedge(M \oplus N)$ such that $\psi'\psi = \mathrm{id}_{\wedge(M \oplus N)}$. A similar argument shows $\psi\psi' = \mathrm{id}_{\wedge M \otimes \wedge N}$. □

5.2.2 Completion and quasi-regularity

Let R be a ring and $(f_1, \dots, f_n)$ a sequence of elements in R. Let I denote the ideal generated by $f_1, \dots, f_n$ and $\hat{R}$ the I-adic completion of R. We recall that elements of $\hat{R}$ can be identified with elements in the following limit

$$\hat{R} = \operatorname{Lim}\Big\{R/I \leftarrow R/I^2 \leftarrow R/I^3 \leftarrow R/I^4 \leftarrow \dots\Big\} \tag{182}$$

For an element $r \in R$ we write $[r]_i$ for the equivalence class represented by r modulo I^i.

Any element $r \in \hat{R}$ can be written as a sequence $([r_1]_1, [r_2]_2, \dots)$ for some elements $r_1, r_2, \dots \in R$ and where for $j < i$ we have $r_j = r_i \operatorname{mod} I^j$.

If $r = ([r_1]_1, [r_2]_2, \dots)$ is such an element, then for all $i > 0$ we have $r_i - r_{i-1} \in I^{i-1}$ and so there exists $t_{i-1} \in I^{i-1}$ such that $r_i = r_{i-1} + t_{i-1}$. This allows us to rewrite r:

$$r = (r_1, r_2, \dots) = (r_1', r_1' + r_2', r_1' + r_2' + r_3', \dots) \tag{183}$$

where $r_1 = r_1'$ and $r_i' = r_i - r_{i-1}$ for $i > 1$. Since each $r_i' \in I^{i-1}$ we can write $r_i' = r_i'' t_i$ for some $t_{i-1} \in I^{i-1}, r_i'' \in R$. Taking $r_1'' := r_1'$, this second representation can be written more compactly as

$$r_1' + \sum_{i=2}^{\infty} r_i'' t_{i-1} \tag{184}$$

With a change of index labelling, we have proven:

Lemma 5.2.18. *For any element $r \in \hat{R}$ there exists $\alpha_0, \alpha_1, \dots \in R$ and $t_i \in I^i$ such that*

$$r = \sum_{i=0}^{\infty} \alpha_i t_i \tag{185}$$

Now, given any $M = (m_1, \dots, m_n) \in \mathbb{N}^n$ we denote by f^M the element $f_1^{m_1} \dots f_n^{m_n} \in R$. Since I is generated by $f_1, \dots, f_n$ we have that each $t_i = \sum_{M \in \mathbb{N}^n} \beta_{iM} f^M$ for some collection $\{\beta_{iM}\}_{i \in I, M \in \mathbb{N}^n} \subseteq R$ where for each $M \in \mathbb{N}^n$ all but finitely many $\{\beta_{iM}\}_{i \in I}$ are equal to 0. So (184) becomes

$$\sum_{M \in \mathbb{N}^n} \Big(\sum_{i=0}^{\infty} \alpha_i \beta_{iM} \Big) f^M \tag{186}$$

We can then set $\gamma_M := \sum_{i=0}^{\infty} \alpha_i \beta_{iM}$ (note this sum is finite). For any $g \in I$ we have

$$\sum_{M \in \mathbb{N}^n} (\gamma_M + g) f^M = \sum_{M \in \mathbb{N}^n} \gamma_M f^M \tag{187}$$

Thus, if $\sigma : R/I \longrightarrow R$ is a section (ie, a function $\sigma : R/I \longrightarrow R$ of *sets* such that $\sigma\pi = \mathrm{id}_R$) to the projection $R \longrightarrow R/I$ then

$$\sum_{M \in \mathbb{N}^n} \gamma_M f^M = \sum_{M \in \mathbb{N}^n} \sigma(\gamma_M) f^M \tag{188}$$

where on the right hand side (188) we think of $\hat{R}$ as an R/I-algebra. The final remark to make is that if $(f_1, \dots, f_n)$ is quasi-regular, then the coefficients $\sigma(\gamma_M)$ are uniquely determined by r. We have proven:

Lemma 5.2.19. *If R is a ring,$(f_1,\dots,f_n)$ a sequence of elements in R and I is the ideal generated by $f_1,\dots,f_n$. Let $\sigma : R/I \longrightarrow R$ be a section to the projection $\pi : R \longrightarrow R/I$. Then for any $r \in \hat{R}$ (the I-adic completion of R) there exists a set $\{\sigma_M\}_{M\in\mathbb{N}^n} \subseteq R$ such that*

$$r = \sum_{M\in\mathbb{N}^n} \sigma(\gamma_M) f^M \tag{189}$$

Moreover, the coefficients $\sigma(\gamma_M)$ are uniquely determined by r if and only if $(f_1,\dots,f_n)$ is a quasi-regular sequence.

5.3 Clifford algebras

5.3.1 Bilinear/Quadratic forms

Throughout V is a finite dimensional k-vector space.

This Section considers vector spaces equipped with either a bilinear form or a quadratic form (which due to 5.3.3 amounts, in the case where k is of characteristic not equal to 2, to the same thing).

Definition 5.3.1. A bilinear map $B : V \times V \longrightarrow k$ is sometimes called a **bilinear form**. If $v_1,...,v_n$ is a basis for V then for any $u = u_1v_1 + \cdots u_nv_n, w = w_1v_1 + \cdots w_nv_n \in V$ the value $B(u,w)$ can be calculated by

$$\begin{bmatrix} w_1 & \cdots & w_n \end{bmatrix} \begin{bmatrix} B(v_1,v_1) & \cdots & B(v_1,v_n) \\ \vdots & \ddots & \vdots \\ B(v_n,v_1) & \cdots & B(v_n,v_n) \end{bmatrix} \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} \tag{190}$$

and so given a choice of basis for V there exists an isomorphism between the vector space of bilinear forms and the vector space of $n \times n$ matrices with entries in k. If $\mathscr{B}$ is a basis for V, the matrix corresponding to B is denoted $[B]_{\mathscr{B}}$.

A bilinear form $B : V \times V \longrightarrow k$ is **symmetric** if for all $v,u \in V$ we have $B(v,u) = B(u,v)$.

Definition 5.3.2. A **quadratic form** is a function $Q : V \longrightarrow k$ satisfying the following properties:

- for all $a \in k$ and $v \in V$, we have $Q(av) = a^2Q(v)$,
- the function $B : V \times V \longrightarrow k$ given by $B(v,u) = Q(v+u) - Q(v) - Q(u)$ is bilinear.

Proposition 5.3.3. *Let $B : V \times V \longrightarrow k$ be a symmetric bilinear form and k a field of characteristic not equal to 2. Then the function $Q_B : V \longrightarrow k$ given by $Q_B(v) = B(v,v)$ is a quadratic form.*

Also, given a quadratic form $Q : V \longrightarrow k$, the function $B_Q : V \times V \longrightarrow k$ given by $B_Q(v,u) = \frac{1}{2}\big(Q(v+u) - Q(v) - Q(u)\big)$ is a bilinear form.

Proof. Easy. □

Definition 5.3.4. In the notation of Proposition 5.3.3, B_Q is the **bilinear form associated to** Q and Q_B is the **quadratic form associated to** B. Notice that B_Q is symmetric.

We say that a bilinear form B is **diagonalisable** if there exists a basis $\mathscr{B}$ for V rendering $[B]_{\mathscr{B}}$ diagonal, similarly, we say that Q is **diagonalisable**.

Proposition 5.3.5. *A finite dimensional bilinear form* $B : V \times V \longrightarrow k$ *is diagonalisable if and only if it is symmetric.*

Proof. The bilinear form B is symmetric if and only if there exists a basis with respect to which the matrix representation of B is symmetric (which would imply the matrix representation with respect to *any* basis is symmetric). So since B is diagonalisable we have that B is symmetric.

Now we prove the converse. If B maps everything to zero then the result is obvious so assume this is not the case. We first prove that there exists a vector v such that $Q_B(v) = B(v,v) \neq 0$. Let $u_1, u_2 \in V$ be such that $B(u_1,u_2) \neq 0$. If $B(u_1,u_1) \neq 0$ or $B(u_2,u_2) \neq 0$ then we could take v to be one of u_1, u_2, so assume $B(u_1,u_1) = B(u_2,u_2) = 0$. We have

$$Q(u_1+u_2) = B(u_1+u_2, u_1+u_2) = B(u_1,u_2) + B(u_2,u_1) = 2B(u_1,u_2) \neq 0 \tag{191}$$

where we have used both the assumptions that B is symmetric and that the characteristic of k is not 2. We can thus take v to be $u_1 + u_2$.

We proceed by induction on the dimension of V, with the base case $\dim V = 1$ being trivial.

Say $\dim V = n > 1$. Consider the map $\varphi_v : V \longrightarrow k$ given by $\varphi_v(u) = B(u,v)$. Since $B(v,v) \neq 0$ we have that $\operatorname{im}\varphi_v = k$ and so $\ker\varphi_v = \dim_k V - 1$. Since we are working with finite dimensional vector spaces that there exists implies a decomposition $V = \ker\varphi_v \oplus \operatorname{im}\varphi_v$. We have by the inductive hypothesis that $B \upharpoonright_{\ker\varphi_v \times \ker\varphi_v}$ is diagonalisable. Fix a basis $\mathscr{B} := \{v_1, ..., v_{n-1}\}$ of $\ker\varphi_v \times \ker\varphi_v$ so that the top left $n-1 \times n-1$ minor of the matrix representation of B with respect to this basis is diagonal. We extend $\mathscr{B}$ to a basis $\mathscr{B}'$ for V by taking $\mathscr{B} := \mathscr{B} \bigcup \{v_n\}$ with v and notice that $B(v_i, v) = B(v, v_i) = 0$ for all $i = 1, ..., n-1$ (using the decomposition $V = \ker\varphi_v \oplus \operatorname{im}\varphi_v$ from earlier). We thus have a basis $\{v_1, ..., v_{n-1}, v\}$ with respect to which the matrix representation of V is diagonal. □

Remark 5.3.6. In the proof of Propsition 5.3.5 we used the fact that a linear transformation $\varphi : V \longrightarrow W$ between two finite dimensional k-vector spaces induces a decomposition

$$V \cong \ker\varphi \oplus \operatorname{im}\varphi \tag{192}$$

for some subspace W. To see this, we use the splitting lemma. There is always a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \ker\varphi \arrow[r, tail] & V \arrow[r, "\varphi"] & \operatorname{im}\varphi \arrow[r] & 0 \end{tikzcd} \tag{193}$$

Now pick a basis $\mathscr{B}$ for $\operatorname{im}\varphi$ and make a choice of lifts $\mathscr{C} := \{v_b \mid \varphi(v_b) = b\}_{b\in\mathscr{B}}$. There is thus a linear transformation $\psi : \operatorname{im}\varphi \longrightarrow V$ which is given on basis vectors by $\psi(b) = v_b$. Clearly, $\varphi\psi = \mathrm{id}_{\operatorname{im}\varphi}$, and so the Splitting Lemma may be applied.

Proposition 5.3.7. *Say V is finite dimensional of dimension n. By Proposition 5.3.5 the quadratic form Q is diagonalisable, in fact, more can be said:*

- *if $k = \mathbb{R}$ then there exists a basis for V and $0 \le r \le n$ such that Q with respect to this basis has diagonal entries*
$$\lambda_1 = \cdots = \lambda_r = 1, \qquad \lambda_{r+1} = \cdots = \lambda_n = -1 \tag{194}$$
- *if $k = \mathbb{C}$ then there exists a basis for V such that Q with respect to this basis has diagonal entries*
$$\lambda_1 = \cdots = \lambda_n = 1 \tag{195}$$

Proof. Let $v_1, \cdots, v_n$ be a basis with respect to which Q is diagonal with diagonal entries $\lambda_1, \cdots, \lambda_n$. We proceed by induction on n. Say $n = 1$ and let e be the chosen basis vector of V,and say $k = \mathbb{R}$, we have

$$B_Q(v_1, v_2) = v_2 e \cdot \lambda_1 \cdot v_1 e = \begin{cases} v_2\sqrt{\lambda_1}e \cdot 1 \cdot v_1\sqrt{\lambda_1}e, & \lambda_1 \ge 0, \\ v_2\sqrt{-\lambda_1}e \cdot -1 \cdot v_1\sqrt{-\lambda_1}e, & \lambda_1 < 0 \end{cases} \tag{196}$$

so we can replace the basis e by either $\sqrt{\lambda_1}e$ or $\sqrt{-\lambda_1}e$ and we are done. In the case when $k = \mathbb{C}$, there always exists a square root of λ_1.

The logic of the inductive step is exactly similar. □

Proposition 5.3.8. *Say V is a real vector space of dimension n. By Proposition 5.3.7 there exists a basis of V for which $[B]_{\mathscr{B}}$ is diagonal with all entries equal to either 1 or -1. The triple (n_+, n_-, n_0) consisting of the number n_+ of positive entries, the number n_- of negative entries, and the number n_0 of entries equal to zero in a $[B]_{\mathscr{B}}$ is independent of the choice of diagonalising basis $\mathscr{B}$.*

Proof. Write

$$[B]_{\mathscr{B}} = \begin{bmatrix} I_p & & \\ & -I_q & \\ & & 0_r \end{bmatrix} \tag{197}$$

Denote by $W \subseteq V$ the largest subspace such that $B \restriction_{W\times W}$ is positive definite, ie, $B(w, w) > 0$ for all $w \in W$. Letting $w = w_1 v_1 + \cdots w_n v_n$ and calculating $B(w, w)$ using $[B]_{\mathscr{B}}$ we have

$$w^T [B]_{\mathscr{B}} w = w_1^2 + \cdots w_p^2 - w_{p+1}^2 - \cdots - w_{p+q}^2 \tag{198}$$

and so $w^t [B]_{\mathscr{B}} w > 0$ if and only if $w_{p+1} = \cdots = w_{p+q} = 0$. We thus have

$$W \subseteq \operatorname{Span}(v_1, ..., v_p)$$

Letting W' denote this span, we clearly also have $W' \subseteq W$, implying $p = \dim W$. Thus p has been related to a value which is basis independent and so p is an invariant. The remaining invariances follow from the rank-nullity Theorem. □

Definition 5.3.9. In the notation of Proposition 5.3.8, the triple (n_+, n_-, n_0) is the **signature** of B.

If $n_0 = 0$ then the bilinear form is **nondegenerate**.

Remark 5.3.10. The number of entries equal to 1 in a matrix representation of a symmetric bilinear form on a finite dimensional complex vector space is also an invariant, this follows directly from the rank-nullity Theorem.

5.3.2 Clifford algebras

Throughout, we denote by (V, Q) a quadratic form, consisting of a finite dimensional k-vector space V and a quadratic form $Q : V \longrightarrow k$ on V. The field k is assumed to have characteristic not equal to 2.

Definition 5.3.11. A pair (C_Q, j) consisting of a k-algebra C_Q and a linear transformation $j : V \longrightarrow C_Q$ such that

$$\forall v \in V, j(v)^2 = Q(v) \cdot 1 \tag{199}$$

is a **clifford algebra for** (V, Q) if it is universal amongst such maps. That is, for every pair (D, k) consisting of a k-algebra D and a linear transformation $k : V \longrightarrow D$ satisfying

$$\forall v \in V, k(v)^2 = Q(v) \cdot 1 \tag{200}$$

there exists a unique k-algebra homomorphism $m : C_Q \longrightarrow D$ such that the following diagram commutes

$$\begin{tikzcd}
V \arrow[r, "j"] \arrow[dr, "k"'] & C_Q \arrow[d, "m"] \\
& D
\end{tikzcd} \tag{201}$$

Proposition 5.3.12. *A Clifford algebra for (V, Q) always exists and is essentially unique (unique up to unique isomorphism) amongst those algebras satisfying the unversal property given in Definition 5.3.11.*

Proof (sketch). We construct the tensor algebra

$$T(V) := \bigoplus_{i \geq 0} V^{\otimes i} \tag{202}$$

(where $V^{\otimes 0} := k$) quotiented by the ideal I generated by the set $\{v \otimes v - Q(v) \cdot 1\}_{v \in V}$. The map $j : V \longrightarrow C_Q$ is the inclusion $V \longrightarrow T(V)$ composed with the projection $T(V) \longrightarrow T(V)/I$. □

Notice that j given in the proof of Proposition 5.3.12 is injective.

Proposition 5.3.13. *The underlying vector spaces of C_Q and $\bigwedge V$ are isomorphic.*

Proposition 5.3.13 will follow from a series of observations which cover a broader scope of theory, which we now present.

Consider the linear map $k : V \longrightarrow C_Q$ given by $k(v) = -j(v)$ which clearly satisfies $k(v)^2 = Q(v) \cdot 1$. There is thus an induced morphism $\beta : C_Q \longrightarrow C_Q$ rendering the following diagram commutative:

$$\begin{tikzcd}
V \arrow[r, "j"] \arrow[dr, "k"'] & C_Q \arrow[d, "\beta"] \\
& C_Q
\end{tikzcd} \tag{203}$$

We have that $\beta^2 = \mathrm{id}_{C_Q}$.

Definition 5.3.14. The involution β is the **involution associated with the Clifford Algebra** (C_Q, j).

Recall that for an arbitrary involution $f : V \longrightarrow V$ (where V is a vector space over a field of characteristic not equal to 2) we have

$$\begin{aligned}\forall v \in V, v &= 1/2(f(v) + v) + v - 1/2(f(v) + v) \\ &= 1/2(f(v) + v) + 1/2(v - f(v))\end{aligned}$$

where we notice

$$f(1/2(f(v) + v)) = 1/2(f(v) + v), \quad \text{and} \quad f(1/2(v - f(v))) = 1/2(f(v) - v) \tag{204}$$

and so

$$V = E_1 + E_{-1} \tag{205}$$

where E_i is the i^{th} Eigenspace of f.

Applying this observation to the situation of Clifford algebras, we have:

$$C_Q^0 := \{v \in C_Q^0 \mid \beta(v) = v\}, \qquad C_Q^1 := \{v \in C_Q^1 \mid \beta(v) = -v\} \tag{206}$$

and

$$C_Q = C_Q^0 \oplus C_Q^1 \tag{207}$$

Thus the Clifford algebra (C_Q, j) associated to a quadratic form $Q : V \longrightarrow k$ is naturally a $\mathbb{Z}_2$-graded algebra.

Proposition 5.3.15. *For quadratic forms $Q_1 : V_1 \longrightarrow k, Q_2 : V_2 \longrightarrow k$ we have*

$$C_{Q_1 \oplus Q_2} \cong C_{Q_1} \otimes C_{Q_2} \tag{208}$$

Proof. Consider the linear transformation

$$\begin{aligned}T : V_1 \oplus V_2 &\longrightarrow C_{Q_1} \otimes C_{Q_2} \\ (v_1, v_2) &\longmapsto v_1 \otimes 1 + 1 \otimes v_2\end{aligned}$$

We have:

$$\begin{aligned}T(v_1,v_2)^2 &= (v_1\otimes 1+1\otimes v_2)^2\\ &= (v_1\otimes 1+1\otimes v_2)(v_1\otimes 1+1\otimes v_2)\\ &= v_1^2\otimes 1+v_1\otimes v_2-v_1\otimes v_2+1\otimes v_2^2\\ &= Q_{V_1}(v_1)\otimes 1+1\otimes Q_{V_2}(v_2)\\ &= (Q_{V_1}(v_1)+Q_{V_2}(v_2))(1\otimes 1)\\ &= Q_{V_1\oplus V_2}(v_1,v_2)(1\otimes 1)\end{aligned}$$

So by the universal property of the Clifford algebra (C_Q,j) there exists a k-algebra homomorphism $\hat{T}:C_{Q_1\oplus Q_2}\longrightarrow C_{Q_1}\otimes C_{Q_2}$. First we prove surjectivity, it is sufficient to prove that every pure tensor $x\otimes y\in C_{Q_1}\otimes C_{Q_2}$ is mapped onto by some element by $\hat{T}$. Write $x\otimes y=v_1\cdots v_n\otimes u_1\cdots u_m$ for some $u_1,\ldots,u_n\in C_{Q_1},v_1,\ldots,v_m\in C_{Q_2}$. Since

$$v_1\cdots v_n\otimes u_1\cdots u_m=(v_1\otimes 1)\cdots(v_n\otimes 1)(1\otimes u_1)\cdots(1\otimes u_m)\tag{209}$$

it suffices to show that for all pairs $(v,u)\in V_1\times V_2$ that $v\otimes u\in C_{Q_1}\otimes C_{Q_2}$ is mapped onto by some element by $\hat{T}$. Indeed:

$$\begin{aligned}T\big((v,0)(0,u)\big) &= (v\otimes 1+1\otimes 0)(0\otimes 1+1\otimes u)\\ &= v\otimes u\end{aligned}$$

Surjectivity follows.

Injectivity? □

Definition 5.3.16. A bilinear form or a quadratic form is **finite dimensional** if V is.

For the next result, recall that a finite dimensional bilinear form is diagonalisable if and only if it is symmetric (Proposition 5.3.5):

We are now in a position to describe a basis for C_Q given one for V:

Proposition 5.3.17. *Let $v_1,\ldots,v_n$ be a basis for V. The set:*

$$\mathscr{B}:=\{v_{i_1}\ldots v_{i_m}\mid m\leq n,v_j\in V,0\leq i_1<\cdots<i_m\leq n\}\tag{210}$$

forms a basis for C_Q. In particular,

$$\dim_k C_Q=2^{\dim_k V}\tag{211}$$

Proof. This set clearly linearly generates C_Q and so it suffices to show that (211) holds.

By Proposition 5.3.5 we have that $Q=Q_1\oplus\cdots\oplus Q_n$ and by Proposition 5.3.15 it follows that $C_{Q_1\oplus\cdots\oplus Q_n}\cong C_{Q_1}\otimes\cdots\otimes C_{Q_n}$. Thus it suffices to prove the case when $\dim_k V=1$. This can be directly analysed; we know

$$C_Q\cong C_Q^0\oplus C_Q^1\tag{212}$$

and $C_Q^0=k,C_Q^1=k\cdot e$, where $e\neq 0$. Thus the dimension of C_Q in this case is 2. □

Proposition 5.3.18. *Say V is finite dimensional and $v_1, ..., v_n$ is a basis such that $B(v_i, v_j) = 0$ for all $i \neq j$. Then the Clifford algebra C_Q is multiplicatively generated by $v_1, ..., v_n$ which satisfy the relations*

$$v_i^2 = Q(v_i), \qquad v_iv_j + v_jv_i = 0, i \neq j \tag{213}$$

Proof. The only non-obvious part follows from the calculation

$$\begin{aligned}(v_i + v_j)^2 &= Q(v_i + v_j)\\ &= B(v_i + v_j, v_i + v_j)\\ &= B(v_i, v_i) + 2B(v_i, v_j) + B(v_j, v_j)\\ &= Q(v_i) + Q(v_j)\\ &= v_i^2 + v_j^2\end{aligned}$$

which implies

$$v_iv_j + v_jv_i = 0, i \neq j \tag{214}$$

□

Thus we may think of a Clifford algebra with respect to a finite quadratic form as the free algebra on $\dim_k V$ elements subject to the relations (213).

5.3.3 Clifford algebras of real or complex bilinear forms

In this Section we sometimes will think of the Clifford algebra as associated to a symmetric bilinear form, rather than a quadratic form. There is no difficult difference, but we note that the correct universal property of (C_B, j) is:

$$\forall v_1, v_2 \in V, j(v_1)j(v_2) + j(v_2)j(v_1) = 2B(v_1, v_2) \cdot 1 \tag{215}$$

We also introduce new notation; the Clifford algebra associated to a bilinear form $B : V \times V \longrightarrow k$ is denoted $C(V, B)$.

We can restate Remark 5.3.10 in terms of Clifford algebras:

Corollary 5.3.19. *Let $k \in \{\mathbb{R}, \mathbb{C}\}$. All Clifford algebras of quadratic forms over finite dimensional, k-vector spaces which admit the same signature are isomorphic.*

Notation 5.3.20. We denote:

- the Clifford algebra associated to the quadratic form $(\mathbb{R}^n, -x_1^2 - \cdots - x_n^2)$ by C_n,
- the Clifford algebra associated to the quadratic form $(\mathbb{R}^n, x_1^2 + \cdots + x_n^2)$ by C_n',
- the Clifford algebra associated to the quadratic form $(\mathbb{C}^n, z_1^2 + \cdots + z_n^2)$ by $C_n^{\mathbb{C}}$.

where these quadratic forms are written with respect to the respective standard bases.

Throughout this Section, V is assumed to be a vector space over k with $k \in \{\mathbb{R}, \mathbb{C}\}$, and $B : V \times V \longrightarrow k$ is a bilinear form. Given a real algebra A, the *complexification* is the $\mathbb{C}$-algebra $A \otimes_{\mathbb{R}} \mathbb{C}$ with multiplication given by

$$\big((x \otimes z), (y \otimes w)\big) \longmapsto (xy \otimes zw) \tag{216}$$

Also, given a bilinear form $B : V \times V \longrightarrow k$ where V is a real vector space, we define the *complexification* of B as $B_{\mathbb{C}} : V \otimes_{\mathbb{R}} \mathbb{C} \longrightarrow \mathbb{C}$ given by

$$B_{\mathbb{C}}\big((v_1 \otimes z_1), (v_2 \otimes z_2)\big) = B(v_1, v_2) z_1 z_2 \tag{217}$$

The following Proposition shows that the Clifford algebra of a complexification behaves well:

Proposition 5.3.21. *We have*

$$C(V \otimes_{\mathbb{R}} \mathbb{C}, B_{\mathbb{C}}) \cong C(V, B) \otimes_{\mathbb{R}} \mathbb{C} \tag{218}$$

Proof. Consider the map $\varphi : V \otimes_{\mathbb{R}} \mathbb{C} \longrightarrow C(V, B) \otimes_{\mathbb{R}} \mathbb{C}$ given by $\varphi(v \otimes z) = v \otimes z$. This is such that

$$\varphi(v \otimes z)^2 = (v \otimes z)^2 = v^2 \otimes z^2 = B(v, v) z^2 \cdot 1 \otimes 1 = B_{\mathbb{C}}\big((v \otimes z), (v \otimes z)\big) \cdot 1 \tag{219}$$

So φ induces a map $\hat{\varphi} : C(V \otimes_{\mathbb{R}} \mathbb{C}) \longrightarrow C(V, B) \otimes_{\mathbb{R}} \mathbb{C}$ which is an isomorphism with inverse induced by the bilinear map $C(V, B) \times \mathbb{C} \longrightarrow C(V \otimes_{\mathbb{R}} \mathbb{C}, B_{\mathbb{C}})$ given by $(x, z) \longmapsto x \otimes z$. □

Lemma 5.3.22. *We have*

$$C_n^{\mathbb{C}} \cong C_n \otimes_{\mathbb{R}} \mathbb{C} \cong C_n' \otimes_{\mathbb{R}} \mathbb{C} \tag{220}$$

Proof. For $i = 1, \dots, n$ let $\varphi_i : \mathbb{C} \longrightarrow \mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{C}$ denote the map defined by linearity and the rule $z \longmapsto e_i \otimes z$. These induce a map $\varphi : \mathbb{C}^n \longrightarrow \mathbb{R}^n \otimes \mathbb{C}$ which is the unique such that for all $i = 1, \dots, n$ we have $\varphi \iota_i = \varphi_i$ where $\iota_i : \mathbb{C} \longrightarrow \mathbb{C}^n$ is the i^{th} canonical inclusion.

The map φ has an inverse ψ which is given by linearity and the rule $e_i \otimes z \longmapsto (0, \dots, z, \dots, 0)$ where every entry is 0 other than the i^{th} slot which is occupied by z.

To see that this is indeed an inverse, notice

$$\varphi\psi(e_i \otimes z) = \varphi(0, \dots, z, \dots, 0) = e_i \otimes z \tag{221}$$

and

$$\psi\varphi(z_1, \dots, z_n) = \psi(\sum_{i=1}^n e_i \otimes z_i) = \sum_{i=1}^n (0, \dots, z_i, \dots, 0) = (z_1, \dots, z_n) \tag{222}$$

Next, given $(z_1, \dots, z_n), (w_1, \dots, w_n) \in \mathbb{C}^n$ we have

$$\begin{aligned} B_{C_n' \otimes \mathbb{C}}\big(\varphi(z_1, \dots, z_n), \varphi(w_1, \dots, w_n)\big) &= B_{C_n' \otimes \mathbb{C}}(\sum_{i=1}^n e_i \otimes z_i, \sum_{j=1}^n e_j \otimes w_j) \\ &= \sum_{i,j=1}^n B_{C_n'}(e_i, e_j) z_i w_j \\ &= \sum_{i=1}^n z_i w_i \end{aligned}$$

This implies that φ induces an isomorphism $C_n^{\mathbb{C}} \cong C'_n$.

To obtain an isomorphism $C_n^{\mathbb{C}^n} \cong C_n \otimes \mathbb{R}$ we compose φ with the map $\mathbb{R}^n \otimes \mathbb{C} \longrightarrow \mathbb{R}^n \otimes \mathbb{C}$ defined by linear and the rule $e_i \otimes z \longmapsto e_i \otimes iz$ and proceed similarly to before. □

Example 5.3.23. We have $C_2^{\mathbb{C}} \cong C_2 \otimes_{\mathbb{R}} \mathbb{C}$, and the latter algebra is generated by e_1, e_2 satisfying

$$e_1^2 = e_2^2 = -1, \qquad e_1 e_2 + e_2 e_1 = 0 \tag{223}$$

On the other hand, the underlying vector space of the complex algebra $M_2(\mathbb{C})$ has a basis

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, g_1 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, g_2 = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, T = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{224}$$

satisfying:

$$g_1^2 = g_2^2 = -I, \qquad g_1 g_2 + g_2 g_1 = 0, \tag{225}$$

which implies $C_2^{\mathbb{C}} \cong M_2(\mathbb{C})$.

A final isomorphism (Proposition 5.3.24) allows for a structure Theorem (Theorem 5.3.28)

Proposition 5.3.24. *We have*

$$C_{n+2} \cong C'_n \otimes_{\mathbb{R}} C_2, \qquad C'_{n+2} \cong C_n \otimes_{\mathbb{R}} C'_2 \tag{226}$$

Here the tensor product is the usual one for algebras.

Proof. We satisfy ourselves with a proof sketch. The key Definition is the following:

$$u : \mathbb{R}^2 \longrightarrow C'_n \otimes_{\mathbb{R}} C_2 \tag{227}$$

defined on basis vectors $e_1, e_2 \in \mathbb{R}^{n+2}$ as:

$$u(e_1) = 1 \otimes e_1, \quad u(e_2) = 1 \otimes e_2, \quad u(e_j) = e_{j-2} \otimes e_1 e_2, j = 3, ..., n+2 \tag{228}$$

and the key calculation is

$$\begin{aligned} u(e_j)^2 &= (e_{j-2} \otimes e_1 e_2)^2 \\ &= e_{j-2}^2 \otimes e_1 e_2 e_1 e_2 \\ &= 1 \otimes -e_1^2 e_2^2 \\ &= -1 \otimes 1 \end{aligned}$$

In the penultimate step we have used the fact that $e_{j-2}^2 = 1$ in C'_n and that $e_1 e_2 + e_2 e_1 = 0$ in C_2. □

Remark 5.3.25. Notice that had we mapped u into $C_n \otimes_{\mathbb{R}} C_2$ instead of into $C'_n \otimes_{\mathbb{R}} C_2$ then $u(e_j)^2 = 1$ which would not induce a map $C_{n+2} \longrightarrow C_n \otimes_{\mathbb{R}} C_2$.

Remark 5.3.26. In Proposition 5.3.24, one might suggest (incorrectly) defining $u : C_{n+2} \longrightarrow C_n \otimes_{\mathbb{R}} C_2$ by

$$u(e_1) = 1 \otimes e_1, \quad u(e_2) = 1 \otimes e_2, \quad u(e_j) = e_{j-2} \otimes 1, j = 3, ..., n+2 \tag{229}$$

but this does not work as then (for example)

$$\begin{aligned} u(e_1)u(e_3) + u(e_3)u(e_1) &= (1 \otimes e_1)(e_1 \otimes 1) + (e_1 \otimes 1)(1 \otimes e_1) \\ &= 2e_1 \otimes e_1 \neq 0 \end{aligned}$$

Corollary 5.3.27. *We have*

$$C^{\mathbb{C}}_{n+2} \cong C^{\mathbb{C}}_n \otimes_{\mathbb{C}} M_2(\mathbb{C}) \tag{230}$$

given explicitly by the following (g_1, g_2 are as in Example 5.3.23)

$$e_1 \longmapsto 1 \otimes e_1, \quad e_2 \longmapsto 1 \otimes e_2, \quad e_j \longmapsto ie_{j-2} \otimes g_1g_2, j = 3, ..., n+2 \tag{231}$$

Proof. This follows from an algebraic manipulation:

$$\begin{aligned} C^{\mathbb{C}}_{n+2} &\cong C_{n+2} \otimes_{\mathbb{R}} \mathbb{C} \\ &\cong (C'_n \otimes_{\mathbb{R}} C_2) \otimes_{\mathbb{R}} \mathbb{C} \\ &\cong (C'_n \otimes_{\mathbb{R}} \mathbb{C}) \otimes_{\mathbb{C}} (C_2 \otimes_{\mathbb{R}} \mathbb{C}) \\ &\cong C^{\mathbb{C}}_n \otimes_{\mathbb{C}} C^{\mathbb{C}}_2 \\ &\cong C^{\mathbb{C}}_n \otimes_{\mathbb{C}} M_2(\mathbb{C}) \end{aligned}$$

We note that for $j > 2$, the element e_j is mapped along these isomorphisms in the following way:

$$\begin{aligned} e_j &\longmapsto e_j \otimes_{\mathbb{R}} 1 && (232) \\ &\longmapsto (e_{j-2} \otimes_{\mathbb{R}} e_1e_2) \otimes_{\mathbb{R}} 1 && (233) \\ &\longmapsto (e_{j-2} \otimes_{\mathbb{R}} 1) \otimes_{\mathbb{C}} (e_1e_2 \otimes_{\mathbb{R}} 1) && (234) \\ &\longmapsto e_{j-2} \otimes_{\mathbb{C}} ie_1e_2 && (235) \\ &\longmapsto ie_{j-2} \otimes_{\mathbb{C}} g_1g_2 && (236) \end{aligned}$$

□

Theorem 5.3.28. *There is the following decomposition:*

- *If $n = 2k$ is even,*

$$C^{\mathbb{C}}_n \cong M_2(\mathbb{C}) \otimes \cdots \otimes M_2(\mathbb{C}) \cong \mathrm{End}(\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2) \cong \mathrm{End}((\mathbb{C}^2)^{\otimes k}) \tag{237}$$

given explicitly by the following, we make use of the function

$$\alpha(j) = \begin{cases} 1, & j \text{ odd}, \\ 2, & j \text{ even} \end{cases}$$

$$e_j \longmapsto I \otimes \cdots \otimes I \otimes g_{\alpha(j)} \otimes T \otimes \cdots \otimes T \tag{238}$$

- *if $n = 2k + 1$ is odd,*
$$C_n^{\mathbb{C}} \cong \mathrm{End}(\mathbb{C}^{2^k}) \oplus \mathrm{End}(\mathbb{C}^{2^k}) \tag{239}$$

Consider a finitely generated, free complex vector space $F_n = \mathbb{C}\theta_1 \oplus \ldots \oplus \mathbb{C}\theta_n$ along with its dual F^*. We look at the special case of the above theory when $V = F \oplus F^*$. We begin by defining the following bilinear form on V.

$$\begin{aligned} B : V \times V &\longrightarrow \mathbb{C} \\ \big((x,\nu),(y,\mu)\big) &\longmapsto \frac{1}{2}\big(\nu(y) + \mu(x)\big) \end{aligned}$$

The Clifford algebra $C_n(V,B)$ with respect to this bilinear form is the associative $\mathbb{Z}_2$-graded commutative $\mathbb{C}$-algebra generated by elements $\gamma_1, \ldots, \gamma_n, \gamma^\dagger, \ldots, \gamma_n^\dagger$ subject to the following conditions, where $[a,b] = ab - (-1)^{|a||b|}ba$ and $|\gamma_i| = |\gamma_i^\dagger| = 1, \forall i$.

$$[\gamma_i, \gamma_j] = 0 \quad [\gamma_i^\dagger, \gamma_j^\dagger] = 0 \quad [\gamma_i, \gamma_j^\dagger] = \delta_{ij} \tag{240}$$

Let S_n denote the exterior algebra of F_n.

$$S_n := \bigwedge F_n = \bigwedge(\mathbb{C}\theta_1 \oplus \ldots \oplus \mathbb{C}\theta_n) \tag{241}$$

Lemma 5.3.29. *There is an isomorphism of $\mathbb{C}$-algebras*

$$\begin{aligned} \psi : C_n(V,B) &\longrightarrow \mathrm{End}_{\mathbb{C}}(S_n) \\ \gamma^\dagger &\longmapsto \theta_i \wedge (\_) \\ \gamma &\longmapsto \theta_i\lrcorner(\_) \end{aligned}$$

Proof. It is clear that $\mathrm{End}_{\mathbb{C}}(S_n)$ is a free vector space and that the set $\{\theta_i \wedge (\_), \theta_i\lrcorner(\_)\}$ is linearly independent.

Consider the Clifford algebra $C_{2n}^{\mathbb{C}}$. Consider the map $\varphi : C_{2n}^{\mathbb{C}} \longrightarrow C_n(V,B)$ defined by linearity and the rule

$$e_i \longmapsto \begin{cases} i(\gamma_i^\dagger\gamma_i - \gamma_i\gamma_i^\dagger), & i = 1, \ldots, n \\ i(\gamma_i + \gamma_i^\dagger), & i = n+1, \ldots, 2n \end{cases} \tag{242}$$

We notice that $(\gamma_i^\dagger\gamma_i - \gamma_i\gamma_i^\dagger)(\gamma_i + \gamma_i^\dagger) = \gamma_i^\dagger - \gamma_i$ and so the set $\{i(\gamma_i^\dagger\gamma_i - \gamma_i\gamma_i^\dagger), i(\gamma_i + \gamma_i^\dagger)\}_{i=1,\ldots,n}$ is a generating set for $C_n(V,B)$. Moreover, this set is linearly independent and so indeed is a basis. This implies that φ is an isomorphism of the underlying vector spaces, and one checks that it respects the Bilinear form and so is an isomorphism of Clifford algebras.

Under the isomorphism $C_{2n}^{\mathbb{C}} \cong \mathrm{End}((\mathbb{C}^2)^{\otimes n})$ we have $i(\gamma_i^\dagger\gamma_i - \gamma_i\gamma_i^\dagger) \longmapsto I \otimes \ldots \otimes I \otimes g_2 \otimes T \otimes \ldots \otimes T$ and $i(\gamma_i + \gamma_i^\dagger) \longmapsto I \otimes \ldots \otimes I \otimes g_1 \otimes T \otimes \ldots \otimes T$. Thus the result follows from Theorem 5.3.28. □

Definition 5.3.30. Let $Q_i : V_i \longrightarrow k$ be quadratic forms for $i = 1, 2$. Let $f : V_1 \longrightarrow V_2$ be a linear map, by composing with the inclusion $l : V_2 \longrightarrow C_{Q_2}$ there is an induced map $\varphi : V_1 \longrightarrow C_{Q_2}$ such that for all $v \in V_1$ we have

$$\varphi(v)^2 = f(v)^2 = Q_2(f(v)) \cdot 1 \tag{243}$$

and so if $Q_2(f(v)) = Q_1(v)$ for all $v \in V$ we have by the universal property of C_{Q_1} that there exists a unique morphism $C_{Q_1} \longrightarrow C_{Q_2}$ which we denote by $C(f)$.

Lemma 5.3.31. *The map $C(f)$ is an isomorphism if f is.*

Proof. Easy. □

5.4 Splitting Idempotents

Given a finite dimensional complex vector space V along with a projection $P : V \longrightarrow V$ onto some subspace $\operatorname{im} P \subseteq V$ we have that V splits into a direct sum

$$V \cong \operatorname{im} P \oplus \operatorname{im}(\mathrm{id}_V - P) \tag{244}$$

For any noetherian $\mathbb{Q}$-algebra k, this property of the idempotent P can be generalised to k-linear category $\mathcal{C}$. A k-linear category is one where each homset is endowed with a k-algebra structure.

Definition 5.4.1. Let $\mathcal{C}$ be a category. An **idempotent** in $\mathcal{C}$ is an endomorphism $e : C \longrightarrow C$ such that $e^2 = e$.

An idempotent e is **split** if there exists a pair of morphisms $s : R \longrightarrow C, r : C \longrightarrow R$ such that $sr = e, rs = \mathrm{id}_R$.

Lemma 5.4.2. *Let $e : C \longrightarrow C$ be an idempotent in $\mathcal{C}$. Then the following are equivalent.*

- *$e = sr$ is split where $s : R \longrightarrow C, r : C \longrightarrow R$.*
- *The Equaliser $\mathrm{Eq}(e, \mathrm{id}_e)$ exists and is equal to $s : R \longrightarrow C$.*
- *The Coequaliser $\mathrm{Coeq}(e, \mathrm{id}_e)$ exists and is equal to $r : C \longrightarrow R$.*

Proof. See [**?**][Lemma B.1] or [**?**][Proposition 6.5.4]. □

Lemma 5.4.3. *Assume $\mathcal{C}$ is the category of vector spaces over some field k. Let $e : C \longrightarrow C$ be an idempotent. Assume $e = sr$ is split with $s : R \longrightarrow C, r : C \longrightarrow R$ and $1 - e = s'r'$ is also split with $s' : R' \longrightarrow C, r' : C \longrightarrow R'$. Then there is a split short exact sequence*

$$0 \longrightarrow R \xrightarrow{s} C \xrightarrow{r'} R' \longrightarrow 0 \tag{245}$$

Proof. Consider the morphism $(r, r') : C \longrightarrow R \oplus R'$. Then $\forall x \in R$ we have

$$\begin{aligned}(r, r')s(x) &= (rs(x), r's(x)) \\ &= (x, r's(x))\end{aligned}$$

we claim $r's(x) = 0$. By Lemma **??** we have that $r' : C \longrightarrow R'$ is the coequaliser $\mathrm{Coeq}(1 - e, \mathrm{id}_C)$. Thus $r's(x) = r'(1 - e)s(x)) = r's(x) - r'es(x)$. On the other hand, $s : R \longrightarrow C$ is the equaliser $\mathrm{Eq}(e, \mathrm{id}_C)$ and so $es = s$.

Thus we have a commuting diagram

$$\begin{tikzcd}
0 \arrow[r] & R \arrow[r, "r"] \arrow[dr] & C \arrow[r, "r'"] \arrow[d, "{(r,r')}"'] & R' \arrow[r] & 0 \\
& & R \oplus R' \arrow[ur] & &
\end{tikzcd}$$

Moreover, the homomorphism (r, r') is an isomorphism. To see this, say $x, x' \in C$ are such that $(r, r')(x) = (r, r')(x')$. Then $r(x) = r(x')$ implies $s(r(x)) = s(r(x'))$ which implies $e(x) = e(x')$ and similarly $(1 - e)(x) = (1 - e)(x')$. Thus we have

$$\begin{aligned}x &= (1 - e)(x) + e(x) \\ &= (1 - e)(x') + e(x') \\ &= x'\end{aligned}$$

For surjectivity, notice if $(x, x') \in R \oplus R'$ are given, then $(r, r')(s, s')(x, x') = (x, x')$. □

The next Lemma states that splitting an idempotent is equivalent to finding its image.

Lemma 5.4.4. *Let $\mathcal{C}$ be linear and admit kernels and cokernels. Then if $e : C \longrightarrow C$ is split we have*

$$\mathrm{Eq}(\mathrm{id}, e) \cong \mathrm{im}(e) \cong \mathrm{Coeq}(\mathrm{id}, e) \tag{246}$$

Sketch. We have

$$\mathrm{Eq}(\mathrm{id}, e) \cong \ker(\mathrm{id} - e) \cong \mathrm{im}(e) \tag{247}$$

and

$$\mathrm{Coeq}(\mathrm{id}, e) \cong \mathrm{Coker}(\mathrm{id} - e) \cong \mathrm{im}(e) \tag{248}$$

□

Remark 5.4.5. Another way of understanding Lemma **??** is that given a vector space C and $v \in C$ along with an idempotent $e : C \longrightarrow C$ we have $x = e(x) + (\mathrm{id} - e)x$. It follows that

$$C \cong \mathrm{im}\, e \oplus \mathrm{im}(\mathrm{id} - e) \tag{249}$$

From this it is clear that $\mathrm{Coker}(\mathrm{id} - e) \cong \mathrm{im}(e)$.

Thus, to split an idempotent is to calculate the image of the idempotent. This is where the suggestion that the splitting of idempotents is a fundamental component of the abstract study of computation comes from, idempotents dictate the projection onto states of knowledge, which reduces entropy, and the calculation of the image of these spaces is the arrival at such a state of knowledge.

6 Quantum computing

The goal of this document is to define a mathematical theory of *qubits* as well as their *measurements*, *time evolutions*, etc, and then to develop a theory of error correction upon this foundation. An optional next step after understanding this mathematics is to find a physical phenomena adhering to these conditions. This optional step though is not part of this document.

Our standard of *information* will be sequences of binary integers. The form this information can be encoded into during transmission however will be more liberal. A bit of *quantum information*, that is, a *qubit*, will be any norm 1 element of the complex Hilbert space $\mathcal{H} := \mathbb{C}^2$. Actually, we identify elements of $\mathcal{H}$ with linear operators from $\mathbb{C}$ into $\mathcal{H}$ and use Dirac notation. For example, $|0\rangle : \mathbb{C} \longrightarrow \mathcal{H}$ denotes the map defined by linearity and the rule $1 \longmapsto (1, 0)$, whereas $|1\rangle$ denotes the map defined by linearity and the rule $1 \longmapsto (0, 1)$.

Definition 6.0.1. A **qubit** is a copy of the $\mathbb{C}$-Hilbert space $\mathbb{C}^2$.

The **state** of a qubit $\mathbb{C}^2$ is a vector $|\psi\rangle \in \mathbb{C}^2$ of norm 1.

A pair $(\mathbb{C}^2, |\psi\rangle)$ consisting of a qubit $\mathbb{C}^2$ and a state $|\psi\rangle \in \mathbb{C}^2$ is a **prepared qubit** and we say $\mathbb{C}^2$ has been **prepared** to $|\psi\rangle$.

If clarity is needed, we will refer to a binary integer as a **classical bit**. This is to help distinguish our standard of information from qubits just defined. If we write a state $|\psi\rangle$ of a qubit $\mathcal{H}$ as a linear combination of the standard basis vectors

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{250}$$

We think of $|\alpha|^2$ and $|\beta|^2$ respectively as *probabilities* of the state $|\psi\rangle$ being in state $|0\rangle$ or state $|1\rangle$ respectively. A qubit where $\alpha \neq 0$ and $\beta \neq 0$ is a **superposition state**.

Our goal is to develop a theory of communication of classical bits *via* qubits. The manipulation and transmission of classical bits via qubits will loosely be referred to as *quantum computing*. For any physical computation to take place, it is crucial that reliable error correction is possible, simply due to the huge number of components and interactions involved. The following is our central question.

Question 6.0.2. What tolerance for error does quantum computing allow for?

This is answered formally by Theorem **??**, which classifies necessary and sufficient conditions for a collection of errors to be correctable.

So far, however, we have only considered systems consisting of a single qubit. Since a system consisting of multiple qubits, any of which may be in superposition, may *itself* be in a superposition state, the definition of a *composite* system of qubits is not as simple as the *product* of qubits, in the category of Hilbert spaces.

More precisely, say we had two qubits prepared respectively to states $|\psi\rangle, |\varphi\rangle$. Then the pair $(|\psi\rangle, |\varphi\rangle)$ may also be in superposition. That is, the state

$$\alpha(|\psi\rangle, |\varphi\rangle) + \beta(|\psi\rangle, |\varphi\rangle) \tag{251}$$

where $|\alpha|^2 + |\beta|^2 = 1$ is a valid state of the combined system consisting of the two qubits. Thus, states of *pairs* of systems are vectors in a subspace of the Hilbert space freely generated by the pairs $(|\psi\rangle, |\varphi\rangle)$ of states of the qubits. in fact, we will take the composite system to be the tensor product of the two spaces, which means we need to justfiy the bilinearity conditions too. At the time of writing, the author does not know a satisfying way to motivate these conditions mathematically (although $L(X \times Y) \cong L(X) \otimes L(Y)$ is surely relevant).

A qubit as well as any composite of a finite collection of qubits are examples of finite dimensional complex Hilbert spaces. We define a **state space** to be any finite dimensional Hilbert space $\mathcal{H}$.

Definition 6.0.3. Let $\mathcal{H}_1, \mathcal{H}_2$ be two state spaces. The **composite state space** is $\mathcal{H}_1 \otimes \mathcal{H}_2$. A **state** of a composite system is a vector $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ which can be written as a linear combination of pure tensors

$$\alpha_1 |\psi_1\rangle + \ldots + \alpha_n |\psi_n\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \tag{252}$$

where the coefficients satisfy $|\alpha_1|^2 + \ldots + |\alpha_n|^2 = 1$. The condition that each $|\psi_i\rangle$ is a pure tensor means

$$\forall i = 1, \ldots, n, \exists\, |\psi_i^1\rangle \in \mathcal{H}_1, \exists\, |\psi_i^2\rangle \in \mathcal{H}_2, |\psi_i\rangle = |\psi_i^1\rangle \otimes |\psi_i^2\rangle \tag{253}$$

Remark 6.0.4. The tensor product is *not* a product in the category of Hilbert spaces. This is because the states such as (246) are *not* necessarily determined by a choice of state in $\mathbb{H}_1$, and a choice of state in $\mathbb{H}_2$. Thus, it is not a surprise that we observe "bizarre" behavior, as our definition of a coupled system is *not* given by the standard mathematical definition of *product*. A comparison between the monoidal structure of the category of Hilbert spaces and a hypothetical product can be found in [**?**]).

What degree of access do we have to superposition states? The answer, naturally, is we have access to what we can measure. Rather than one particular outcome, we define a measurement as a family of possible outcomes with assocaited probabilities; the states of state spaces are probabilistic, and so the measurements will be too. Moreover, we do *not* assume that measurement leaves the state uneffected, and so measurements are operators upon the state space.

Definition 6.0.5. A **measurement** on a state space $\mathcal{H}$ is a finite family of linear operators $\{M_m : \mathcal{H} \longrightarrow \mathcal{H}\}_{m \in \mathcal{M}}$ satisfying the **completeness condition**.

$$\sum_{m \in \mathcal{M}} M_m^\dagger M_m = I \tag{254}$$

An element $m \in \mathcal{M}$ is an **outcome** (simply a set of labels).

The **resulting state** after measurement $\{M_m\}_{m \in \mathcal{M}}$ and outcome m is:

$$\frac{M_m |\psi\rangle}{\sqrt{p(m)}} \tag{255}$$

Remark 6.0.6. Associated to every measurement and state vector $|\psi\rangle$ there is a value

$$p(m) \coloneqq \langle\psi| M_m^\dagger M_m |\psi\rangle = \| M_m |\psi\rangle \|^2 \tag{256}$$

It follows from (248) that $p(m) \leq 1$ for all $m, |\psi\rangle$. We understand $p(m)$ as the probability of outcome m on the measurement $\{M_m\}_{m\in\mathcal{M}}$. Under this interpretation, we think of (248) as requiring that the probabilities $p(m)$ sum to 1.

The possibility of superposition states is a liberation, and measurements needing to satisfy the completeness condition is a limitation. For instance, where a classical bit is in one of two states (0 or 1) a qubit has an *infinite* number of possible states (a liberation). On the other hand, only *orthogonal* states can be distinguished, due to the completeness condition (Lemma 6.0.7 below) (a limitation).

Lemma 6.0.7. *Let $|\psi_1\rangle, |\psi_2\rangle$ be non-orthogonal states of a qubit $\mathcal{H}$. There is no measurement $\{M_m : \mathcal{H} \longrightarrow \mathcal{H}\}_{m\in\mathcal{M}}$ with $1, 2 \in \mathcal{M}$ satisfying:*

$$p(1) = \langle\psi_1| M_1^\dagger M_1 |\psi_1\rangle = 1 \quad \textit{and} \quad p(2) = \langle\psi_2| M_2^\dagger M_2 |\psi_2\rangle = 1 \tag{257}$$

Proof. Assume such a measurement exists. Since $|\psi_1\rangle, |\psi_2\rangle$ are non-orthogonal, there exists $|\varphi\rangle$, orthorgonal to $|\psi_1\rangle$ such that

$$|\psi_2\rangle = \alpha |\psi_1\rangle + \beta |\varphi\rangle \tag{258}$$

for some $\alpha, \beta \in \mathbb{C}$ satisfying $|\alpha|^2 + |\beta|^2 = 1$. Moreover, since $|\psi_1\rangle, |\psi_2\rangle$ are non-orthogonal, we have $\beta \neq 1$. We have

$$\begin{aligned}
1 &= \langle\psi_2| |\psi_2\rangle &(259)\\
&= \langle\psi_2| M_2^\dagger M_2 |\psi_2\rangle &(260)\\
&= (\bar{\alpha} \langle\psi_1| + \bar{\beta} \langle\varphi|) M_2^\dagger M_2 (\alpha |\psi_1\rangle + \beta |\varphi\rangle) &(261)\\
&= |\alpha|^2 \langle\psi_1| M_2^\dagger M_2 |\psi_1\rangle + \bar{\alpha}\beta \langle\psi_1| M_2^\dagger M_2 |\varphi\rangle &(262)\\
&\qquad + \bar{\beta}\alpha \langle\varphi| M_2^\dagger M_2 |\psi_1\rangle + |\beta|^2 \langle\varphi| M_2^\dagger M_2 |\varphi\rangle &(263)
\end{aligned}$$

Now, by the completeness condition, we have

$$\langle\psi_1| \sum_{m\in\mathcal{M}} M_m^\dagger M_m |\psi_1\rangle = \langle\psi_1| I |\psi_1\rangle = 1 \tag{264}$$

This, combined with $p(1) = 1$ implies $\langle\psi_1| M_2^\dagger M_2 |\psi_1\rangle = 0$. In other words, $\| M_2 |\psi_1\rangle \|^2 = 0$. This implies $M_2 |\psi_1\rangle = 0$ (the zero vector). Thus, (256) implies:

$$1 = |\beta|^2 \langle\varphi| M_2^\dagger M_2 |\varphi\rangle = |\beta|^2 \| M_2 |\varphi\rangle \|^2 \leq |\beta|^2 < 1 \tag{265}$$

This stands in contradiction to (251). □

The liberty of superposition means the following are four valid states of a single qubit.

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad \frac{-|0\rangle + |1\rangle}{\sqrt{2}} \quad \frac{-|0\rangle - |1\rangle}{\sqrt{2}} \tag{266}$$

Since these are non-orthogonal though, Lemma 6.0.7 renders these indistinguishable. Desigining algorithms amongst the push and pull of superposition and measurement is the art of quantum computing.

Lemma 6.0.8. *If $|\psi_1\rangle, \ldots, |\psi_n\rangle$ are orthogonal states of a state space, then there exists a measurement $\{M_m\}_{m\in\mathcal{M}}$ such that for all $i = 1, \ldots, n$:*

$$p(i) = \langle\psi_i| M_i^\dagger M_i |\psi_i\rangle = 1 \tag{267}$$

Proof. The operator

$$E := \sum_{i=1}^{n} |\psi_i\rangle\langle\psi_i| \tag{268}$$

is equal to the identity when restricted to the subspace $\mathrm{Span}\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ and when written with respect to the basis $|1\rangle, \ldots, |n\rangle$ of this subspace. A trick to extend this to a measurement of the whole space, and written with respect to the standard basis is to add an operator M_0 defined by $I - E$. The set $\{|\psi_i\rangle\langle\psi_i|\}_{i=1,\ldots,n} \cup M_0$ is a measurement distinguishing $|1\rangle, \ldots, |n\rangle$. □

Definition 6.0.9. Let $\mathcal{H}$ be a state space. A **single step time evolution** of $\mathcal{H}$ is a unitary operator U on $\mathcal{H}$. A **single step time evolution** of a state vector $|\psi\rangle$ with respect to U is the pair $(|\psi\rangle, U|\psi\rangle)$.

An **evolution** of $\mathcal{H}$ is a sequence of unitary operators $(U_1, ..., U_n)$ on $\mathcal{H}$, an **evolution** of a state vector $|\psi\rangle$ with respect to the evolution $(U_1, ..., U_n)$ is the sequence $(|\psi\rangle, U_1|\psi\rangle, ..., U_n \cdots U_1|\psi\rangle)$.

Example **??** falls into the special setting where the measurement used to distinguish the states (**??**) is **projective**, ie, all the measurement operators are projectors.

Definition 6.0.10. A linear transformation P is a **projector** if $P^2 = P$.

These simple measurements are sufficient in many situations.

The exact relationship between projective measurements and measurements is given by Proposition 6.0.12 below which says in a precise sense that general measurements are projective measurements augmented by a unitary operator.

Lemma 6.0.11. *Let $W \subseteq V$ be a subspace of a Hilbert space V, and let $U : W \longrightarrow V$ be a unitary operator. Then U extends to a unitary operator U' on all of V.*

Proof. Take $U' = U \otimes \mathrm{Id}_{W^\perp}$. □

Proposition 6.0.12. *Let $\{M_m\}_{m\in\mathcal{M}}$ be a measurement on $\mathcal{H}$. Then there exists a projective measurement $\{P_m\}_{m\in\mathcal{M}}$, a state space Q, and a unitary operator $U : \mathcal{H}\otimes Q \longrightarrow \mathcal{H}\otimes Q$ such that for any state $|\psi\rangle$ of the composite system $\mathcal{H}\otimes Q$ and any $n \in \mathcal{M}$:*

$$\langle\psi| U^\dagger P_n^\dagger P_n U |\psi\rangle = \langle\psi| M_n^\dagger M_n |\psi\rangle \tag{269}$$

Proof. Let Q be the Hilbert space freely generated by the set $\{|1\rangle, ..., |m\rangle\}$. Define the following linear map.

$$U : \mathcal{H} \longrightarrow \mathcal{H} \otimes Q \tag{270}$$

$$|\psi\rangle = \sum_{m \in \mathcal{M}} M_m |\psi\rangle \otimes |m\rangle \tag{271}$$

We first prove this is unitary, by Corollary A.2.8 it suffices to check that $\langle\psi| U^\dagger U |\psi\rangle = \langle\psi||\psi\rangle$ for arbitrary $|\psi\rangle \in \mathcal{H}$. We perform the following calculation, note: we have written $\langle\psi| M_m^\dagger \otimes \langle m|$ for the linear functional which sends $a \otimes b$ to the product $\langle\psi| M_m^\dagger a \langle m| b$.

$$\begin{aligned}
\langle\psi| U^\dagger U |\psi\rangle &= \Big(\sum_{m \in \mathcal{M}} \langle\psi| M_m^\dagger \otimes \langle m|\Big)\Big(\sum_{m' \in \mathcal{M}} M_{m'} |\psi\rangle \otimes |m'\rangle\Big) \\
&= \sum_{m \in \mathcal{M}} \sum_{m' \in M} \langle\psi| M_m^\dagger M_{m'} |\psi\rangle \langle m||m'\rangle \\
&= \sum_{m \in \mathcal{M}} \langle\psi| M_m^\dagger M_{m'} |\psi\rangle \\
&= \langle\psi||\psi\rangle
\end{aligned}$$

We now want to extend U to a unitary operator on all of $\mathcal{H} \otimes Q$ using Lemma 6.0.11, however we must first identify $\mathcal{H}$ with a subspace of $\mathcal{H} \otimes Q$. There are many ways this can be done, here we choose the basis vector $|1\rangle \in Q$ to be special, and identify $\mathcal{H}$ with $\mathcal{H} \otimes \operatorname{Span}|1\rangle \subseteq \mathcal{H} \otimes Q$.

Now consider the following projective measurement on $\mathcal{H} \otimes Q$:

$$P_m := I_q \otimes |m\rangle \langle m| \tag{272}$$

Then the probability outcome n occurs is:

$$\begin{aligned}
p(n) &= \langle\psi| U^\dagger P_n U |\psi\rangle \\
&= \Big(\sum_{m \in \mathcal{M}} \langle\psi| M_m^\dagger \otimes \langle m|\Big) I_Q \otimes |n\rangle \langle n| \Big(\sum_{m' \in \mathcal{M}} M_{m'} |\psi\rangle \otimes |m\rangle\Big) \\
&= \Big(\sum_{m \in \mathcal{M}} \langle\psi| M_m^\dagger \otimes \langle m|\Big) \sum_{m' \in \mathcal{M}} M_{m'} |\psi\rangle \otimes |n\rangle \langle n||m\rangle \\
&= \sum_{m \in \mathcal{M}} \Big(\langle\psi| M_m^\dagger \otimes \langle m|\Big) M_n |\psi\rangle \otimes |n\rangle \\
&= \sum_{m \in \mathcal{M}} \langle\psi| M_m^\dagger M_n |\psi\rangle \langle m||n\rangle \\
&= \langle\psi| M_n^\dagger M_n |\psi\rangle
\end{aligned}$$

□

Remark 6.0.13. The defining equation (265) of the linear map (264) may look opaque. We derive it from a more natural starting point here. See [**?**, §Partial Trace] for a justification of the natural isomorphisms used in the following calculation.

$$\operatorname{Hom}(Q, \operatorname{Hom}(\mathcal{H}, \mathcal{H})) \cong \operatorname{Hom}(Q \otimes \mathcal{H}, \mathcal{H}) \tag{273}$$

$$\cong \operatorname{Hom}(\mathcal{H}, \mathcal{H} \otimes Q^*) \tag{274}$$

Then, by identifying Q with Q^* via the anti-linear, isometric bijection given by the Riesz Representation Theorem (see Corollary A.1.4), a linear map $\mathcal{H} \longrightarrow \mathcal{H} \otimes Q$ can be given by a linear map $Q \longrightarrow \mathcal{H} \otimes \mathcal{H}$. We claim that (264) corresponds under this correspondence to the following linear map.

$$Q \longrightarrow \mathrm{Hom}(\mathcal{H}, \mathcal{H}) \tag{275}$$

$$|m\rangle \longmapsto M_m \tag{276}$$

We now validate this claim. This is a matter of a calculation.

$$\big(|m\rangle \mapsto M_m \big) \longmapsto \big(|m\rangle \otimes |\psi\rangle \mapsto M_m |\psi\rangle \big) \tag{277}$$

$$\longmapsto \big(\psi \mapsto \sum_{m \in \mathcal{M}} M_m |\psi\rangle \otimes |m\rangle \big) \tag{278}$$

See Corollary [**?**, 1.2.6] for a justification of the last step.

6.1 Error correction

The more informed two parties are, the more communication may be prone to error while still sustaining certainty on the intended message. This is because both parties can "error correct" the other.

Throughout, $\mathbb{H}$ denotes a qubit $\mathbb{C}^2$, that is, the complex Hilbert space $\mathbb{C}^2$.

Definition 6.1.1. A **message** is a state $|\psi\rangle \in \mathbb{H}^{\otimes n}$, for some n. An **error** is a pair of states $(|\varphi\rangle, |\psi\rangle)$ where $|\varphi\rangle, |\psi\rangle \in \mathbb{H}^{\otimes n}$ for some n, note that an error may be such that $|\varphi\rangle = |\psi\rangle$. The message $|\varphi\rangle$ is the **intended message** and $|\psi\rangle$ is the **received message**.

Definition 6.1.2. An **n-encoding of a single state** (sometimes just an **encoding**) is an injective linear map $\iota : \mathbb{H} \longrightarrow \mathbb{H}^{\otimes n}$. An **$n$-encoding of a message** $|m\rangle \in \mathbb{H}^{\otimes k}$ is an n-encoding ι along with a message $|m\rangle \in \mathbb{H}^{\otimes nk}$ for which there exists $|m'\rangle \in \mathbb{H}^{\otimes k}$ satisfying $\iota^{\otimes k} |m'\rangle = |m\rangle$.

Definition 6.1.3. A **quantum error correcting code (QECC)** is a pair $\mathcal{Q} = (\mathcal{H}, S)$ consisting of a state space $\mathcal{H}$ along with a set of operators S on $\mathcal{H}$. The elements of S are the **stabilisers**. The **codespace** $\mathcal{H}^S$ of $\mathcal{Q}$ is the maximal subspace of $\mathcal{H}$ invariant under all the operators in S.

In Section 6.3 we will present a method for proving when a set of vectors generate the codespace of a quantum error correction code.

6.2 Bit flip error correction

Throughout, $\mathbb{H}$ denotes a qubit $\mathbb{C}^2$, that is, the complex Hilbert space $\mathbb{C}^2$.

Definition 6.2.1. We define the following operators:

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$
$$Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The matrices X, Y, Z are the **Pauli matrices**, and H is the **Hadamard matrix**.

We make the passing observation that all of X, Y, Z, H square to the identity matrix. The basis vectors

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{279}$$

are the **Bell states** and are denoted $|+\rangle, |-\rangle$ respectively. Notice that as already stated, $H^2 = I$, so $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$.

Definition 6.2.2. The standard basis $|0\rangle, |1\rangle$ of $\mathbb{H}$ induces a basis of $\mathbb{H}^{\otimes n}$, we denote $|0\rangle \otimes \cdots \otimes |0\rangle$ by $|0 \cdots 0\rangle$, etc.

Notation 6.2.3. Given a Pauli matrix $W \in \{X, Y, Z\}$ the operator on $\mathbb{H}^{\otimes n}$ given by the tensor product consisting of W in the i^{th} slot (for $i \leq n$) and the identity operator in all other slots by W_i. For example, the operator Z_1 on $\mathbb{H}^{\otimes 3}$ is the operator $Z \otimes I \otimes I$.

Given a collection of Pauli matrices $W_{i_1}, ..., W_{i_m} \in \{X, Y, Z\}$ where $0 < i_1 < \cdots < i_m \leq n$ we denote by $W_{i_1} \ldots W_{i_m}$ the composition $W_{i_1} \circ \ldots \circ W_{i_m}$. For example, the operator $Z_1 Z_2$ on $\mathbb{H}^{\otimes 3}$ is the operator

$$(Z \otimes I \otimes I) \circ (I \otimes Z \otimes I) = Z \otimes Z \otimes I : \mathbb{H}^{\otimes 3} \longrightarrow \mathbb{H}^{\otimes 3} \tag{280}$$

Consider the **bit flip encoding**

$$\mathrm{BitFlip} : \mathbb{H} \longrightarrow \mathbb{H}^{\otimes 3} \tag{281}$$
$$|0\rangle \longmapsto |000\rangle \tag{282}$$
$$|1\rangle \longmapsto |111\rangle \tag{283}$$

then an encoding of a message with respect to this encoding might be $|000111000\rangle$, but could not be $|000111001\rangle$. We call Encoding 275 the **bit flip encoding**.

Definition 6.2.4. A **bit flip error** is an error $(|\varphi\rangle, |\psi\rangle)$ where $|\varphi\rangle$ is an encoding of a message with respect to the encoding $\mathrm{BitFlip}^{\otimes m}$ for some m, such that $X_i|\varphi\rangle = |\psi\rangle$ for some i.

Let $(|\varphi\rangle, |\psi\rangle)$ be a bit flip error. The following algorithm takes as input $|\psi\rangle$ and reconstructs $|\varphi\rangle$: We now prove correctness of Algorithm 6.2:

Input: a received message $|\psi\rangle$,

1. perform the following projective measurements:

$$\langle\psi| Z_1Z_2 |\psi\rangle \text{ with resulting state } |\psi'\rangle, \tag{284}$$

   followed by

$$\langle\psi'| Z_2Z_3 |\psi'\rangle \tag{285}$$

   let (r_1, r_2) be the pair of results from these measurements.

2. It will be shown that $r_1, r_2 \in \{1, -1\}$, and the resulting state of the second measurement is $|\psi\rangle$.

3. Now retrieve $|\varphi\rangle$ based on the values of r_1, r_2:

   - if $(r_1, r_2) = (1, 1)$, return $|\psi\rangle$,
   - if $(r_1, r_2) = (-1, 1)$, return $X_1 |\psi\rangle$,
   - if $(r_1, r_2) = (1, -1)$, return $X_3 |\psi\rangle$,
   - if $(r_1, r_2) = (-1, -1)$, return $X_2 |\psi\rangle$

Proof. It will be helpful to first notice:

$$\begin{aligned}
Z_1Z_2 |000\rangle &= |000\rangle & Z_1Z_2 |001\rangle &= |001\rangle \\
Z_1Z_2 |010\rangle &= -|010\rangle & Z_1Z_2 |011\rangle &= -|011\rangle \\
Z_1Z_2 |100\rangle &= -|100\rangle & Z_1Z_2 |101\rangle &= -|101\rangle \\
Z_1Z_2 |110\rangle &= |110\rangle & Z_1Z_2 |111\rangle &= |111\rangle
\end{aligned}$$

Let $|\psi\rangle := a|010\rangle + b|101\rangle$ be a state, ie, an element of $\mathbb{H}^{\otimes 3}$. We perform the measurement Z_1Z_2 followed by Z_2Z_3:

$$\begin{aligned}
\langle\psi| Z_1Z_2 |\psi\rangle &= (a\langle 010| + b\langle 101|)Z_1Z_2(a|010\rangle + b|101\rangle) \\
&= (a\langle 010| + b\langle 101|)(-a|010\rangle - b|101\rangle) \\
&= -a^2 - b^2 = -1
\end{aligned}$$

and

$$\begin{aligned}
\langle\psi| Z_2Z_3 |\psi\rangle &= (a\langle 010| + b\langle 101|)Z_1Z_2(a|010\rangle + b|101\rangle) \\
&= (a\langle 010| + b\langle 101|)(-a|010\rangle - b|101\rangle) \\
&= -a^2 - b^2 = -1
\end{aligned}$$

We can infer from the fact that both of these came out as -1 that it was the second bit which was flipped, and so we can correct this. However, what is the impact of this measurement on the state? Again we calculate:

$$\begin{aligned} Z_1Z_2(a\left|010\right\rangle + b\left|101\right\rangle) &= Z_1(-a\left|010\right\rangle + b\left|101\right\rangle) \\ &= -a\left|010\right\rangle - b\left|101\right\rangle \end{aligned}$$

and

$$\begin{aligned} Z_2Z_3(-a\left|010\right\rangle - b\left|101\right\rangle) &= Z_2(-a\left|010\right\rangle + b\left|101\right\rangle) \\ &= a\left|010\right\rangle + b\left|101\right\rangle \end{aligned}$$

and so the measurements (in the end) did not impact our state. □

Later, using the theory of *stabiliser codes*, we will show that in fact single bit flip errors form the full set of correctable errors using Z_1Z_2, Z_1Z_3, Z_2Z_3.

6.3 Stabilisers

We provide a means for determining when a vector subspace consisting of correctable errors is the largest such. That is, we establish a method for proving that a set of vectors span the codespace of a QECC (Definition 6.1.3).

Throughout, $\mathbb{H}$ denotes a qubit $\mathbb{C}^2$, that is, the complex Hilbert space $\mathbb{C}^2$.

Recall the Pauli operators of Definition 6.2.1.

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{286}$$

Recall also our notation that, for example, Z_1Z_2 on $\mathbb{H}^{\otimes 3}$ denotes the operator $Z \otimes Z \otimes I$, see Notation 6.2.3.

Definition 6.3.1. Let $n > 0$. The n^{th}-**Pauli Group**, denoted G_n, is the set of operators $\mathbb{H}^{\otimes n} \longrightarrow \mathbb{H}^{\otimes n}$ generated by of all operators $\pm I, iI, X_j, Y_j, Z_j$ for $j = 1, ..., n$.

Definition 6.3.2. Given a subgroup $S \subseteq G_n$ of the Pauli group G_n, we denote by V^S the subspace of $\mathbb{H}^{\otimes n}$ which is invariant under the operators S. That is, $\left|\psi\right\rangle \in V^S$ if and only if

$$\forall W \in S, W\left|\psi\right\rangle = \left|\psi\right\rangle \tag{287}$$

Denote by $\mathscr{X}$ the following Pauli operators

$$\mathscr{X} := \{I, X, Y, Z\} \tag{288}$$

For an arbitrary element $g \in G_n$, let $g_1, ..., g_n \in \mathscr{X}$ be such that

$$g = \alpha g_1 \otimes \cdots \otimes g_n, \quad \alpha \in \{1, -1, i, -i\} \tag{289}$$

then the sequence $g_1, ..., g_n$ is the unique such, and we denote a length $2n$ sequence $x = (x_1, ..., x_{2n})$ in $\mathbb{Z}_2^{2n}$ by $r(g)$ defined by the following schemata:

- $x_i = 1$ if and only if $g_i = X$,
- $x_{i+n} = 1$ if and only if $g_i = Z$,
- $x_i = x_{i+n} = 1$ if and only if $g_i = Y$.

Given a set $\{g_1, ..., g_k\}$ of elements of the Pauli group, the **check matrix** is the $k \times 2n$ matrix whose j^{th} row is $r(g_j)$. The check matrix is denoted $\text{Check}(g_1, ..., g_k)$.

Remark 6.3.3. Let (g, h) be a pair of elements of G_n and let $g_1, ..., g_n, h_1, ..., h_n \in \mathscr{X}$ be such that

$$g = \alpha g_1 \otimes \cdots \otimes g_n, \quad \alpha \in \{1, -1, i, -i\}$$
$$h = \beta h_1 \otimes \cdots \otimes h_n, \quad \beta \in \{1, -1, i, -i\}$$

we see that g and h commute if and only if the number of times g_j and h_j are distinct matrices with neither equal to the identity is even.

Defining

$$\Lambda := \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \tag{290}$$

we have the following Lemma.

Lemma 6.3.4. *Let $(g_1, g_2) \in G_n$. Then g_1, g_2 commute if and only if*

$$r(g_1)\Lambda r(g_2)^T = 0 \tag{291}$$

Rough sketch. The form of $r(g_1)$:

$$r(g_1) = \big(X \text{ or } Y \text{ in } g_1 \quad | \quad Z \text{ or } Y \text{ in } g_1\big) \tag{292}$$

and similarly for $r(g_2)$. Thus we have

$$r(g_1)\Lambda r(g_2)^T = \big(X \text{ or } Y \text{ in } g_1 \quad | \quad Z \text{ or } Y \text{ in } g_1\big) \begin{pmatrix} Z \text{ or } Y \text{ in } g_2 \\ X \text{ or } Y \text{ in } g_2 \end{pmatrix} \tag{293}$$

This contains the data of the requirements specified by Observation 6.3.3. □

The Check matrix is useful for more:

Definition 6.3.5. A set of elements $g_1, ..., g_r \in G_n$ of the Pauli group G_n are **independent** if the for any j we have, where we write $\hat{g}_i$ for the omission of g_i:

$$\langle g_1, ..., g_r \rangle \neq \langle g_1, ..., \hat{g}_j, ..., g_n \rangle \tag{294}$$

(here, the notation $\langle g_1, ..., g_n \rangle$ denotes the group generated by these elements).

Lemma 6.3.6. *Let $g_1, ..., g_r \in G_n$ be a set of elements such that $-I \notin \langle g_1, ..., g_r \rangle$, then the elements $g_1, ..., g_r$ are independent if and only if $r(g_1), ..., r(g_r)$ and linearly independent (over the field $\mathbb{Z}_2$).*

Proof. See [**?**, Page 457, Proposition 10.3] □

The following Lemma will be used to calculate the dimension of V^S:

Lemma 6.3.7. *Let $g_1, ..., g_k$ be independent elements of the Pauli group G_n and denote by S the group they generate. Assume $-I \notin S$. Then for each $i = 1, ..., k$ there exists $g \in G_n$ such that g anti-commutes with g_i and commutes with all g_j satisfying $i \neq j$.*

Proof. The set $r(g_1), ..., r(g_k)$ is linearly independent by Lemma 6.3.6, thus the check matrix of $g_1, ..., g_k$ has k linearly independent columns. So, there exists a vector $x \in \mathbb{Z}_2^k$ such that

$$\text{Check}(g_1, ..., g_n)\Lambda x = e_i \tag{295}$$

where e_i is the i^{th} standard basis vector of $\mathbb{Z}_2^k$. Let g be such that $r(g)^T = x$. The result follows from Lemma 6.3.6. □

Theorem 6.3.8. *Let $S = \langle g_1, ..., g_k \rangle \subseteq G_n$ and say $-I \notin S$. Then* $\dim V^S = 2^{n-k}$.

Proof. We notice that $(1/2)(I + g_j)$ is the projector onto the +1-Eigenspace of g_j. We let $x = (x_1, ..., x_k) \in \mathbb{Z}_2^k$ and define the operator

$$P_S^x := 1/2^k \prod_{j=1}^{k} (I + (-1)^{x_j} g_j) \tag{296}$$

By Lemma 6.3.7 we have for each g_j there exists g_{x_j} such that $g_{x_j} g_j g_{x_j}^{-1} = -g_j$. Let $g_x = g_{x_1} \cdots g_{x_k}$, then

$$\begin{aligned} g_x P_S^{(0,...,0)} g_x^{-1} &= 1/2^k \prod_{j=1}^{k} (g_{x_j} g_{x_j}^{-1} + g_{x_j} g_j g_{x_j}^{-1}) \\ &= P_S^x \end{aligned}$$

Thus there is an isomorphism

$$\operatorname{im} P_S^x \cong \operatorname{im} P_S^{(0,...,0)} \tag{297}$$

Since $\operatorname{im} P_S \cong V_S$ we have $\dim \operatorname{im} P_S^x = \dim V_S$. Finally we note that

$$I = \sum_{x \in \mathbb{Z}_2^k} P_S^x \tag{298}$$

The operator I is a projector onto an n-dimensional space, and $\sum_{x \in \mathbb{Z}_2^k} P_S^x$ is a sum of 2^k orthogonal projectors all of the same dimension as V_S, thus the only possibility is $\dim V_S = 2^{n-k}$. □

Example 6.3.9. In the context of the bitflip error correction, we have:

$$S = \langle Z_1Z_2, Z_2Z_3\rangle \subseteq G_3 \tag{299}$$

It is clear that

$$V^S \supseteq \text{Span}\{|000\rangle, |111\rangle\} \tag{300}$$

Now we want to use Theomre 6.3.8 to prove that in fact (294) holds up to equality.

Since Z_1Z_2, Z_2Z_3 are 2 independent generators for S, it follows from Theorem 6.3.8 that

$$\dim V^S = 2^{3-2} = 2 = \dim\big(\text{Span}\{|000\rangle, |111\rangle\}\big) \tag{301}$$

7 Geometry of interaction models, MLL

A Operator Theory

A.1 Adjoint operators

We will be chiefly concerned with the Hilbert space ℓ^2 but we work in a more general setting for now. A *Hilbert space* will always mean over $\mathbb{C}$. Associated to every operator between Hilbert spaces is an operator between their *dual spaces*:

In general, if $\mathcal{I}$ is any inner product space over $\mathbb{C}$ and we have two vectors $x, y \in I$ then we can consider the projection of y onto x which is given by

$$\text{Proj}_y(x) := \frac{\langle x, y\rangle}{||y||}\frac{y}{||y||} \tag{302}$$

Thus, if $U \subseteq \mathcal{I}$ is a one dimensional subspace spanned by a unit vector $u \in U$ then the projection of any $x \in \mathcal{I}$ onto u is given by the simple formula $\langle x, u\rangle u$. The following Lemma shows what we can say when the subspace is of arbitrary dimension but with U closed:

Lemma A.1.1. *Let $\mathbb{H}$ be a Hilbert space and $U \subseteq \mathbb{H}$ a closed subspace. Then*

$$\mathbb{H} = U \oplus U^{\perp}$$

Proof. We will define a projection

$$\begin{aligned} P_U : \mathbb{H} &\longrightarrow U \\ x &\longmapsto \inf\{||x-y|| \mid y \in U\} \end{aligned}$$

We let d denote $\inf\{||x-y|| \mid y \in U\}$. By definition of inf there exists a sequence $(x_n)_{n=0}^{\infty}$ of elements in U such that $\lim_{n\to\infty} ||x - x_n|| = d$. Since U is closed it is complete and the norm is continuous so it suffices to show that the sequence $(x_n)_{n=0}^{\infty}$ is Cauchy. This can be done for example using the parallelogram identity: for all $n, m \geq 0$:

$$||x_n - x_m||^2 + ||(x - x_n) + (x - x_m)||^2 = 2||x - x_n||^2 + 2||x - x_m||^2 \tag{303}$$

As given $\epsilon > 0$ there exists $N \geq 0$ such that $||x - x_n||^2 < d^2 + \epsilon^2/4$, for $n \geq N$. Thus

$$\begin{aligned}||x_n - x_m||^2 &= 2||x - x_n||^2 + 2||x - x_m||^2 - 4||x = ||1/2(x_n + x_m)||^2 \\ &\leq 4d^2 + \epsilon^2 - 4||x - 1/2(x_n + x_m)||^2\end{aligned}$$

which since $1/2(x_n + x_m) \in C$ we have $d \leq ||x - 1/2(x_n + x_m)||$, proving $(x_n)_{n=0}^{\infty}$ is Cauchy. This also shows linearity.

It remains to show $x - P_U(x) \in U^{\perp}$. To do this, we will consider the family of vectors $c(t) = (1-t)P_U(x) + ty$, $(t \in \mathbb{R})$ and analyse the derivative of $||x - y_t||^2$ at $t = 0$.

Consider the composition

$$\begin{aligned}\gamma : \mathbb{R} &\longrightarrow \mathbb{R} && (304)\\ t &\longmapsto ||x - c(t)||^2 && (305)\end{aligned}$$

We can write γ in a more explicit form:

$$\begin{aligned}\gamma(t) &= ||x - P_U(x) + t(y - P_U(x))||^2 \\ &= \big\langle x - P_U(x) + t(y - P_U(x)), x - P_U(x) + t(y - P_U(x))\big\rangle \\ &= ||x - P_U(x)||^2 - 2t \operatorname{Re}\langle x - P_U(x), y - P_U(x)\rangle + t^2||y - P_U(x)||\end{aligned}$$

which is clearly differentiable and has derivative $-2\operatorname{Re}\langle x - P_U(x), y - P_U(x)\rangle$ at $t = 0$. Since $P_U(x)$ (which equals $c(0)$) is a minimum of $\gamma(t)$ we have that $\operatorname{Re}\langle x - P_U(x), y - P_U(x)\rangle = 0$. This holds true for arbitrary $y \in U$ and lastly we have

$$\{y - P_U(x) \mid y \in U\} = U$$

thus for all $y \in U$:

$$\operatorname{Re}\langle x - P_U(x), y\rangle = 0 \qquad (306)$$

This shows that $x - P_U(x) \in U^{\perp}$. □

Given a Hilbert space $\mathbb{H}$ there is a map

$$\begin{aligned}\Phi : \mathbb{H} &\longrightarrow \mathbb{H}^* && (307)\\ b &\longmapsto \langle \_, b\rangle && (308)\end{aligned}$$

Notice that in order to produce a *linear* functional, it was important we put b in the second argument, we must define Φ so that $\Phi(b) \neq \langle b, \_\rangle$. By anti-linearity of the second argument of the inner product we have that Φ is anti-linear, and moreover is injective as

$$\begin{aligned}\Phi(b) = \Phi(b') &\Longrightarrow \langle \_, b\rangle = \langle \_, b'\rangle \\ &\Longrightarrow \forall b'' \in \mathbb{H}, \langle b'', b - b'\rangle = 0 \\ &\Longrightarrow \text{ in particular, } \langle b - b', b - b'\rangle = 0 \\ &\Longrightarrow b - b' = 0\end{aligned}$$

In the special case where $\mathbb{H}$ is finite dimensional, we automatically have that this map is surjective as it is injective, and any anti-linear, injective map between two finite dimensional spaces of equal dimension is automatically surjective. More generally, if $\mathbb{H}$ has arbitrary dimension, then for any $y \in \mathbb{H}$ the map $\langle \_, y \rangle$ is bounded (see Remark A.1.5) so the image of Φ is contained in the set of continuous linear functionals, the following establishes the reverse inequality:

Theorem A.1.2 (Riesz Representation Theorem)**.** *Let $\mathbb{H}$ be a Hilbert space. For every continuous linear functional $\varphi \in \mathbb{H}^*$ there exists a unique element $h_\varphi \in \mathbb{H}$ such that*

$$\varphi = \langle \_, h_\varphi \rangle \tag{309}$$

Moreover, we have

$$||\varphi||_{\mathbb{H}^*} = ||h_\varphi||_{\mathbb{H}} \tag{310}$$

We will use the following Lemma:

Lemma A.1.3. *Let $\mathbb{H}$ be a Hilbert space and $\varphi \in \mathbb{H}^*$ be non-zero and continuous. Then $(\ker \varphi)^\perp$ is one dimensional.*

Proof. Since φ is continuous the set $\ker \varphi$ is closed and so by Lemma A.1.1 we have $\mathbb{H} = \ker \varphi \oplus (\ker \varphi)^\perp$, which since $\varphi \neq 0$ implies there exists $v \neq 0 \in (\ker \varphi)^\perp$, so $\dim(\ker \varphi)^\perp > 0$. Now, say $v_1, v_2 \in (\ker \varphi)^\perp$ so that $\varphi(v_1) \neq 0$ and $\varphi(v_2) \neq 0$. These are complex numbers and so there exists $\lambda \in \mathbb{C}$ such that

$$0 = \lambda \varphi(v_1) - \varphi(v_2) = \varphi(\lambda v_1 - v_2)$$

which means $\lambda v_1 - v_2 \in \ker \varphi \cap (\ker \varphi)^\perp = \{0\}$. □

Proof of Theorem A.1.2. Clearly if $\ker \varphi = \mathbb{H}$ we can take $h_\varphi = 0$ so assume this is not the case. Since φ is continuous its kernel $\ker \varphi$ is a closed subset of $\mathbb{H}$. Thus, by Lemma A.1.1 the Hilbert space $\mathbb{H}$ decomposes: $\mathbb{H} = \ker \varphi \oplus (\ker \varphi)^*$. Since $\ker \varphi$ is a proper subset it then follows that there exists a non-zero element $v \neq 0 \in (\ker \varphi)^*$, by normalising we may assume that v is a unit vector. We will show that $\overline{\varphi(v)} v$ is the appropriate unique choice for h_φ.

By Lemma A.1.3 the subspace $(\ker \varphi)^\perp$ is one dimensional, hence we can use formula (296) for the projection of arbitrary x onto $(\ker \varphi)^\perp$. Observe the following calculation:

$$\begin{aligned}
\varphi(x) &= \varphi(x - \langle x, v \rangle v + \langle x, v \rangle v) \\
&= \varphi(x - \langle x, v \rangle v) + \varphi(\langle x, v \rangle v) \\
&= 0 + \langle x, v \rangle \varphi(v) \\
&= \langle x, \overline{\varphi(v)} v \rangle
\end{aligned}$$

For uniqueness, say h'_φ was another such element. Then

$$\begin{aligned}
&\forall x \in \mathbb{H}, \langle x, h_\varphi \rangle = \langle x, h'_\varphi \rangle \\
&\implies \forall x \in \mathbb{H}, \langle x, h_\varphi - h'_\varphi \rangle = 0 \\
&\implies \|h_\varphi - h'_\varphi\| = 0 \\
&\implies h_\varphi = h'_\varphi
\end{aligned}$$

For the second claim, we use the Cauchy-Schwartz inequality:

$$|\varphi(x)| = |\langle x, \overline{\varphi(v)} v\rangle| \leq \|x\| \|\overline{\varphi(v)}\| \|v\| = \|x\| |\varphi(v)|$$

and so if x has unit norm $|\varphi(x)| \leq |\varphi(v)|$, in other words, $\|\varphi\|_{\mathbb{H}^*} \leq |\varphi(v)|$ however v has unit norm itself, so $\|\varphi\|_{\mathbb{H}^*} = |\varphi(v)|$. The proof is now complete once it is noted that $\|h_\varphi\|_{\mathbb{H}} = |\varphi(v)|$. □

Corollary A.1.4. *There existgs an antilinear, isometric injection:*

$$\begin{aligned}
\mathbb{H} &\longrightarrow \mathbb{H}^* && (311)\\
v &\longmapsto \langle v, \_ \rangle && (312)
\end{aligned}$$

and hence a bijection when $\mathbb{H}$ is finite dimensional.

Remark A.1.5. Let $y \in \mathbb{H}$ be an element of a Hilbert space $\mathbb{H}$ and consider the function $\langle \_, y\rangle$. This is bounded, as by Cauchy-Schwartz:

$$|\langle x, y\rangle| \leq \|x\| \|y\|$$

thus $|\langle \_, y\rangle| / \|x\| \leq \|y\|$ and in fact this is equality as $|\langle y/\|y\|, y\rangle| = \|y\|$.

Given an operator $u : \mathbb{H}_1 \longrightarrow \mathbb{H}_2$ there is for each $y \in \mathbb{H}_2$ an associated linear functional $x \longmapsto \langle u(x), y\rangle$ which we denote by $\langle u(\_), y\rangle$. By Theorem A.1.2 there is thus an element $y^* \in \mathbb{H}_1$ such that $\langle u(\_), y\rangle = \langle \_, y^*\rangle$. The assignment $y \mapsto y^*$ is in fact linear, we show additivity:

$$\langle u(\_), y_1 + y_2\rangle = \langle \_, (y_1 + y_2)^*\rangle$$

and

$$\begin{aligned}
\langle u(\_), y_1 + y_2\rangle &= \langle u(\_), y_1\rangle + \langle u(\_), y_2\rangle \\
&= \langle \_, y_1^*\rangle + \langle \_, y_2^*\rangle \\
&= \langle \_, y_1^* + y_2^*\rangle
\end{aligned}$$

which implies $(y_1 + y_2)^* = y_1^* + y_2^*$. We define:

Definition A.1.6. The **adjoint operator** associated to an operator $u : \mathbb{H}_1 \longrightarrow \mathbb{H}_2$ is the linear map:

$$\begin{aligned} u^* : \mathbb{H}_2 &\longrightarrow \mathbb{H}_1 \\ y &\longmapsto y^* \end{aligned}$$

Its existence is established by the Riesz Representation Theorem (A.1.2) and it is uniquely determined by the property:

$$\forall x \in \mathbb{H}_1, y \in \mathbb{H}_2, \langle u(x), y \rangle = \langle x, u^*(y) \rangle \tag{313}$$

Remark A.1.7. Let $\big(\mathbb{H}_1, \langle \cdot, \cdot \rangle_B\big), \big(\mathbb{H}_2, \langle \cdot, \cdot \rangle\big)_C$ be Hilbert spaces and let $u : \mathbb{H}_1 \longrightarrow \mathbb{H}_2$ be an operator. The **adjoint** to u, denoted u^* is the operator:

$$\_ \circ u : \mathbb{H}_2^* \longrightarrow \mathbb{H}_1^* \tag{314}$$

$$\varphi \longmapsto \varphi \circ u \tag{315}$$

The following diagram commutes:

$$\begin{tikzcd}
\mathbb{H}_2^* \arrow[rrrr, "\_\circ u"] \arrow[ddd, "\cong"'] & & & & \mathbb{H}_1^* \arrow[ddd, "\cong"] \\
& \langle \_, v \rangle \arrow[r, mapsto] & \langle u(\_), v \rangle \arrow[r, leftrightarrow] & \langle \_, v^* \rangle & \\
& v \arrow[u, mapsto] \arrow[r, mapsto] & u^*(v) \arrow[ur, mapsto] & & \\
\mathbb{H}_2 \arrow[rrrr, "u^*"'] & & & & \mathbb{H}_1
\end{tikzcd} \tag{316}$$

which explains the overloading of terminology.

Notation A.1.8. Given a complex matrix A, the matrix given by conjugating each element $a \in A$ and then transposing the result, ie, the **conjugate transpose** is denoted $A^\dagger$. Due to Proposition A.1.9 below, the conjugate transpose of a matrix is often referred to as the **adjoint**.

Proposition A.1.9. *Let $\mathbb{H}_1, \mathbb{H}_2$ be finite dimensional, and let $v_1, ..., v_n \in \mathbb{H}_1, w_1, ..., w_m \in \mathbb{H}_2$ be orthonormal bases for $\mathbb{H}_1, \mathbb{H}_2$ respectively. If $\varphi : \mathbb{H}_1 \longrightarrow \mathbb{H}_2$ is a linear transformation and A its matrix representation with respect to these bases, then the matrix representation of the adjoint φ^* is $A^\dagger$, the conjugate transpose of A.*

Proof. ‘ For each $j = 1, ..., m$ write $w_j^* = \alpha_1 v_1 + \cdots + \alpha_n v_n$ and each $i = 1, ..., n$ write $\varphi(v_i) = \beta_1 w_1 + \cdots + \beta_m w_m$. We calculate:

$$\langle \varphi(v_i), w_j \rangle = \beta_m \langle w_1, w_j \rangle + \cdots + \beta_m \langle w_m, w_j \rangle = \beta_j \tag{317}$$

and

$$\langle v_i, w_j^* \rangle = \bar{\alpha}_1 \langle v_i, v_1 \rangle + \cdots + \bar{\alpha}_n \langle v_i, v_n \rangle = \bar{\alpha}_i \tag{318}$$

Since by definition $\langle \varphi(v_i), w_j \rangle = \langle v_i, w_j^* \rangle$ the proof is complete. □

A.2 Hermitian and unitary operators

Throughout, V is a complex vector space.

Definition A.2.1. A square, complex matrix A is **Hermitian** if it is self-adjoint, that is $A^\dagger = A$.

A matrix is **normal** if $AA^\dagger = A^\dagger A$

An operator $\varphi : V \longrightarrow V$ is **Hermitian** (**normal**) if a (and hence all) matrix representation(s) of V is Hermitian (normal).

Clearly, all Hermitian matrices are normal.

Theorem A.2.2 (Spectral decomposition)**.** *Let V be a finite dimensional complex inner product space and A a matrix representation of an operator on V. The matrix A is normal if and only if it is diagonalisable with respect to some orthonormal basis for V.*

Proof. We prove that normal matrices are diagonalisable.

We proceed by induction on the size of the matrix. If the matrix is 1×1 then there is nothing to prove. Now for the inductive step. Let λ be an eigenvalue of A, and P the matrix which projects onto the λ-eigenspace. We let Q denote $I - P$, the projector onto the complement subspace. We notice that

$$A = (P+Q)A(P+Q) = PAP + QAP + PAQ + QAQ \tag{319}$$

We have that $QAP = 0$ because A maps the λ-eigenspace onto itself, and we claim moreover that $PAQ = 0$. To see this, let v be an eigenvector with eigenvalue λ, then

$$AA^\dagger v = A^\dagger A v = A^\dagger \lambda v = \lambda A^\dagger v \tag{320}$$

which means $A^\dagger$ maps the λ-eigenspace onto itself. This implies $QA^\dagger P = 0$, taking the transpose of which we end at $PAQ = 0$ as claimed.

Thus $A = PAP + QAQ$. The matrix PAP is diagonalisable with respect to some orthonormal basis for P. Since $P \cap Q = 0$ it remains to show that QAQ is diagonalisable with respect to some orthonormal basis for Q. The space Q has strictly smaller size than A and so this follows by induction once we have shown that QAQ is normal. This is a simple calculation:

$$\begin{aligned} QAQQA^\dagger Q &= QAQA^\dagger Q \\ &= QA(P+Q)A^\dagger Q \\ &= QAA^\dagger Q \\ &= QA^\dagger AQ \\ &= QA^\dagger(P+Q)AQ \\ &= QA^\dagger QAQ \\ &= QA^\dagger QQAQ \end{aligned}$$

□

Definition A.2.3. Let $\mathbb{H}$ be a possibly inifinite dimensional Hilbert space, an operator $U : \mathbb{H} \longrightarrow \mathbb{H}$ is **unitary** if $U^\dagger U = UU^\dagger = \mathrm{Id}_n$.

Definition A.2.4. A matrix U is **unitary** if $U^\dagger U = I$.

Lemma A.2.5. *A square, unitary matrix U satisfies $UU^\dagger = I$.*

Proof. Let u_{ij} denote the entry of U in row i and column j. The entry in row i and column j of $U^\dagger U$ is $\sum_{k=1}^n \overline{u}_{ik} u_{kj}$ which by hypothesis is equal to δ_{ij}. Hence, $\sum_{k=1}^n \overline{u}_{ki} u_{kj}$ is equal to $\sum_{k=1}^n u_{ik} \overline{u}_{jk}$ which is the entry in row i and column j of $UU^\dagger$. □

Corollary A.2.6. *If $\mathbb{H}$ is a finite dimensional Hilbert space and $U : \mathbb{H} \longrightarrow \mathbb{H}$ is an operator on $\mathbb{H}$, then U is unitary if and only if for all $u, v \in \mathbb{H}$ we have $\langle Uu, Uv \rangle = \langle u, v \rangle$.*

Proof. First we observe the following calculation, where $u \in \mathbb{H}$ is arbitary.

$$\begin{aligned}
||U^\dagger U u - u|| &= \langle U^\dagger U u - u, U^\dagger U u - u \rangle \\
&= \langle U^\dagger U u, U^\dagger U u \rangle - \langle U^\dagger U u, u \rangle - \langle u, U^\dagger U u \rangle + \langle u, u \rangle \\
&= \langle UU^\dagger U u, U u \rangle - \langle U u, U u \rangle - \langle U u, U u \rangle + \langle u, u \rangle \\
&= \langle U^\dagger U u, u \rangle - \langle u, u \rangle - \langle u, u \rangle + \langle u, u \rangle \\
&= \langle U u, U u \rangle - \langle u, u \rangle \\
&= \langle u, u \rangle - \langle u, u \rangle \\
&= 0
\end{aligned}$$

Hence $U^\dagger U u = u$ for all $u \in \mathbb{H}$ and so $U^\dagger U = \mathrm{Id}_{\mathbb{H}}$.

Let $u_1, ..., u_n$ be an orthonormal basis for $\mathbb{H}$ and let $\underline{U}$ denote the matrix of U written with respect to this basis. Since U is unitary we have that $\underline{U}$ is unitary and so $\underline{U}^\dagger \underline{U} = I$ and by Lemma A.2.5 we have $\underline{UU}^\dagger = I$. It follows from this that $UU^\dagger = \mathrm{Id}_{\mathbb{H}}$ and so U is unitary.

The converse is obvious. □

In fact, it is sufficient to check even less.

Lemma A.2.7. *Let $U : \mathbb{H} \longrightarrow \mathbb{H}$ be an operator on a finite dimensional Hilbert space. If $\langle Uu, Uu \rangle = \langle u, u \rangle$ for all $u \in \mathbb{H}$, then for all $u, v \in \mathbb{H}$ we have $\langle Uu, Uv \rangle = \langle u, v \rangle$.*

Proof. It suffices to prove that if $C : \mathbb{H} \longrightarrow \mathbb{H}$ is an operator on $\mathbb{H}$ such that for all $x \in \mathbb{H}$ we have $\langle Cx, x \rangle = 0$ then $C = 0$.

We let $x, y \in \mathbb{H}$ be arbitrary and consider $\langle C(x+y), x+y \rangle$. Since this is 0 it follows that $\langle Cx, y \rangle = -\langle Cy, x \rangle$. On the other hand, $\langle C(x+iy), x+iy \rangle$ is also 0, which implies $\langle Cx, y \rangle = \langle Cx, y \rangle$. Hence $\langle Cx, y \rangle = \langle Cy, x \rangle = 0$. □

Corollary A.2.8. *If $U : \mathbb{H} \longrightarrow \mathbb{H}$ is an operator and $\mathbb{H}$ is finite dimensional, then U is unitary if and only if $\forall u \in \mathbb{H}, \langle Uu, Uu \rangle = \langle u, u \rangle$.*

Proof. Immediate from Corollary A.2.6 and Lemma A.2.7. □

Notice that the spectral decomposition (A.2.2) states that the matrix A is such that $A = U^{\dagger}DU$ for a diagonal matrix D and a unitary matrix U.

Corollary A.2.9. *A normal matrix A is Hermitian if and only if its eigenvalues are real.*

Proof. First notice that if a matrix is Hermitian then for any eigenvector v with eigenvalue λ:

$$\lambda |v|^2 = \langle \lambda v, v\rangle = \langle Av, v\rangle = \langle v, Av\rangle = \bar{\lambda}|v|^2 \tag{321}$$

Now we prove the other direction. Let D be diagonal and U a unitary matrix such that $A = U^{-1}DU$. Then

$$A^{\dagger} = U^{\dagger}D^{\dagger}U^{-1^{\dagger}} = U^{-1}DU = A \tag{322}$$

□

Definition A.2.10. An operator $\varphi : V \longrightarrow V$ is **positive** if:

$$\forall v \in V, \langle v, \varphi v\rangle \geq 0 \tag{323}$$

which means, $\langle v, \varphi v\rangle$ is real and non-negative. If the inequality is strict, then φ is **positive definite**.

Example A.2.11. Let A be any operator. Then for any $v \in V$:

$$\langle v, A^{\dagger}Av\rangle = \langle Av, Av\rangle = ||Av||^2 \geq 0 \tag{324}$$

Thus $A^{\dagger}A$ is positive.

Proposition A.2.12. *A positive operator on a finite dimensional vector space is necessarily Hermitian.*

Proof. Let A be a matrix representation of the positive operator. Notice the following calculation:

$$\begin{aligned} 0 \leq \langle v, (A - A^{\dagger})v\rangle &= \langle (A^{\dagger} - A)v, v\rangle \\ &= \overline{\langle v, (A^{\dagger} - A)v\rangle} \\ &= \langle v, (A^{\dagger} - A)v\rangle \\ &= -\langle v, (A - A^{\dagger})v\rangle \geq 0 \end{aligned}$$

and so for all $v \in V$ we have $\langle v, (A - A^{\dagger})v\rangle = 0$.

Moreover, we notice that $A - A^{\dagger}$ is normal and hence diagonalisable, by the Spectral decomposition. It follows from these two observations that $A - A^{\dagger} = 0$. □

Definition A.2.13. Let A, B be matrices, then the **commutator** is $[A, B] := AB - BA$. The **anticommutator** is $\{A, B\} = AB + BA$.

Theorem A.2.14 (Simultaneous Diagonalisation Theorem)**.** *Let A, B be Hermitian operators. Then $[A, B] = 0$ if and only if A and B are simultaneously diagonalisable.*

Proof. If A and B are simultaneously diagonalisable, then let U be a unitary matrix and D_1, D_2 diagonal matrices such that

$$A = U^{-1}D_1U, \qquad B = U^{-1}D_2U \tag{325}$$

We then have:

$$\begin{aligned} AB &= U^{-1}D_1UU^{-1}D_2U \\ &= U^{-1}D_1D_2U \\ &= U^{-1}D_2D_1U \\ &= U^{-1}D_2UU^{-1}D_1U \\ &= BA \end{aligned}$$

Conversely, say $[A, B] = 0$. We have that A is Hermitian and so admits a spectral decomposition. Let $a_1, ..., a_n$ be the eigenvalues corresponding to this decomposition and let V_{a_i} denote the a_i-eigenspace. We first notice that B maps V_{a_i} into itself: for any $v \in V_{a_i}$

$$ABv = BAv = a_iBv \tag{326}$$

Now, since B is Hermitian, it follows that $B_{V_{a_i}} : V_{a_i} \longrightarrow V_{a_i}$ is and so there exists a spectral decomposition of $B_{V_{a_i}}$ for each vector space V_{a_i}. Denote by $b_1^{a_i}, ..., b_{k_{a_i}}^{a_i}$ an orthonormal basis for V_{a_i}. We then have that

$$\{b_1^{a_i}, ..., b_{k_{a_i}}^{a_i}\}_{i=1}^n \tag{327}$$

is a basis of eigenvectors of both A and B for the whole space V. □

There is another decomposition which is often helpful:

Remark A.2.15. Let $T : V \longrightarrow V$ be a linear operator on a finite dimensional vector space V. We could ask if T can be factored $T = UT'$ where U is unitary? Say this was possible, then

$$T^\dagger T = T'^\dagger U^\dagger UT' \tag{328}$$

so if T' were Hermitian we would have $T^\dagger T = T'^2$ which would imply $T' = \sqrt{T^\dagger T}$, in fact $T^\dagger T$ is Hermitian (indeed it is positive) and thus so is $\sqrt{T^\dagger T}$ and so our assumption that T' be Hermitian is not too much to ask for, and if U were to exist it must be that $T' = \sqrt{T^\dagger T}$. Thus we are prompted to make the following calculation: let $v_1, ..., v_n$ be a basis for V such that (we write P_{v_i} for the projection onto v_i)

$$\sqrt{T^\dagger T} = \sum_{i=1}^n \lambda_i P_{v_i} \tag{329}$$

then

$$\sqrt{T^\dagger T} v_i \lambda_i \tag{330}$$

and indeed we want U such that $\lambda_i U v_i = T v_i$. One might suggest defining $U v_i = T v_i / \lambda_i$ at this point, however there is no reason for this to be unitary. Instead we define

$$U = \sum_{j=1}^{n} T v_j P_{v_j} / \sqrt{\lambda_j} \tag{331}$$

which indeed is unitary. In fact we read off from this that $\{T v_1/\sqrt{\lambda_1}, ..., T v_n/\sqrt{\lambda_n}\}$ is an orthonormal basis for V. Notice however that this assumes $\lambda_i \neq 0$ for all i. This can be fixed by doing this process first for all $\lambda_i \neq 0$, and to construct an orthonormal set $\{T v_1/\sqrt{\lambda_1}, ..., T v_j/\sqrt{\lambda_j}\}$ and then extending this to an orthonormal basis for V via the Gram-Schmidt process.

We have proven the first half of:

Theorem A.2.16 (Polar decomposition)**.** *Let $T : V \longrightarrow V$ be a linear operator on an n-dimensional vector space V. Then there exists a unitary operator U and positive operators J, K such that*

$$T = UJ = KU \tag{332}$$

with $J = \sqrt{T^\dagger T}, K = \sqrt{TT^\dagger}$.

To obtain K we simply notice

$$A = JU = UJU^\dagger U \tag{333}$$

so we set $K = UJU^\dagger$, which is a positive operator. Then $AA^\dagger = KUU^\dagger K = K^2$.

If we have such a decomposition $T = UJ$, then J is diagonalisable, being positive, thus $T = USDS^\dagger$ for unitary S and diagonal D. Setting $V = S^\dagger$ we obtain:

Corollary A.2.17 (Singular value decomposition)**.** *Let $T : V \longrightarrow V$ be a linear operator on an n-dimensional vector space, then there exists unitary operators U, V and a diagonal operator D such that*

$$T = UDV \tag{334}$$

Remark A.2.18. We make a remark on notation. Given a vector $v \in \mathbb{H}$ in some Hilbert space $\mathbb{H}$ (which we assume to be finite dimensional for simplicity), the linear functional which we have been notating as $\langle v, \_ \rangle$ can also be written simply as $\langle v|$. Symmetrically, the vector v can be identified with the linear map $k \longrightarrow \mathbb{H}$ sending $1 \longmapsto v$, we notate this map by $|v\rangle$. Hence, given two vectors $v, u \in V$, the notation $\langle v||u\rangle$ denotes the linear map $k \longrightarrow k$ sending $1 \longmapsto \langle v, u\rangle$. We now describe how some of the concepts introduced in this Section and the last are written using this notation.

- The linear map given in Corollary A.1.4 can be written as $|v\rangle \longmapsto \langle v|$.

- Let $U : \mathbb{H} \longrightarrow \mathbb{H}$ be an operator. We have for any $v \in \mathbb{H}$ that:

$$\langle Uv| = \langle Uv, \_\rangle = \langle v, U^\dagger\_\rangle = \langle v| U^\dagger \tag{335}$$

  Hence, in light of Corollary A.2.6 we have that U is unitary if and only if for all $v \in \mathbb{H}$ we have $\langle v| U^\dagger U |v\rangle = \langle v||v\rangle$. This is the condition which is checked throughout the body of this paper.

A The Untyped λ-Calculus

The untyped λ-calculus sits among a collection of *type theories* which have been used as a foundation for mathematics [**?**], a foundation for logic [**?**], (although it was later found to be inconsistent [**?**]), and a foundation of certain programming languages such as AGDA, Lisp, Haskell, Coq, COC, etc. The untyped λ-calculus is the simplest of these theories, and although is rarely used in its original form, is a good entry point to many of the important ideas concerning the more modern type theories.

The main reference for this section is [**?**, §3.3].

Definition A.0.1. Let $\mathscr{V}$ be a (countably) infinite set of variables, and let $\mathscr{L}$ be the language consisting of $\mathscr{V}$ along with the special symbols

$$\lambda \qquad . \qquad (\qquad)$$

Let $\mathscr{L}^*$ be the set of words of $\mathscr{L}$, more precisely, an element $w \in \mathscr{L}^*$ is a finite sequence $(w_1, ..., w_n)$ where each w_i is in $\mathscr{L}$, for convenience, such an element will be written as $w_1...w_n$. Now let Λ_p denote the smallest subset of $\mathscr{L}^*$ such that

- if $x \in \mathscr{V}$ then $x \in \Lambda_p$,
- if $M, N \in \Lambda_p$ then $(MN) \in \Lambda_p$,
- if $x \in \mathscr{V}$ and $M \in \Lambda_p$ then $(\lambda x.M) \in \Lambda_p$

Λ_p is the set of **preterms**. A preterm M such that $M \in \mathscr{V}$ is a **variable**, if $M = (M_1M_2)$ for some preterms M_1, M_2, then M is an **application**, and if $M = (\lambda x, M')$ for some $x \in \mathscr{V}$ and $M' \in \Lambda_p$ then M is an **abstraction**.

In practice, it becomes unwieldy to use this notation for the preterms exactly, and so the following notation is adopted:

Definition A.0.2.

- For preterms M_1, M_2, M_3, the preterm $M_1M_2M_3$ means $((M_1M_2)M_3))$,
- For variables x, y and a preterm M, the preterm $\lambda xy.M$ means $(\lambda x.(\lambda y.M))$.

The variables x which appear in the subpreterm M of a preterm $\lambda x.M$ are viewed as "markers for substitution", (see Remark A.0.9). For this reason, a distinction is made between the variable x and the variable y in, for example, the preterm $\lambda x.xy$:

Definition A.0.3. Given a preterm M, let $\mathrm{FV}(M)$ be the following set of variables, defined recursively

- if $M = x$ where x is a variable then $\mathrm{FV}(M) = \{x\}$,
- if $M = M_1 M_2$ then $\mathrm{FV}(M) = \mathrm{FV}(M_1) \cup \mathrm{FV}(M_2)$,
- if $M = \lambda x.M'$ then $\mathrm{FV}(M) = \mathrm{FV}(M') \setminus \{x\}$.

A variable $x \in \mathrm{FV}(M)$ is a **free variable** of M, a variable x which appears in M but is not a free variable is a **bound variable**.

As mentioned, bound variables will be viewed as "markers for substitution", so we define the following equivalence relation on Λ_p which relates a preterm M to M' if M can be obtained by replacing every bound occurrence of a variable x in M' with another variable y:

Definition A.0.4. For any term M, let $M[x := y]$ be the preterm given by replacing every bound occurrence of x in M with y. Define the following equivalence relation on Λ_p: $M \sim_\alpha M'$ if there exists $x, y \in \mathscr{V}$ such that $M[x := y] = M'$, where no free variable of M becomes bound in $M[x := y]$. In such a case, we say that M is **α-equivalent** to M'.

Remark A.0.5. The reason why we need to let x and y be such that no free variable of M becomes bound in $M[x := y]$ is so that a preterm such as $\lambda x.y$ does not get identified with the preterm $\lambda y.y$.

We are now in a position to define the underlying language of λ-calculus:

Definition A.0.6. Let $\Lambda = {}^{\Lambda_p}\!/\!_{\sim_\alpha}$ be the set of **λ-terms**. The set of **free variables** of a λ-term $[M]$ is $\mathrm{FV}(M)$, which can be shown to be well defined. For convenience, M will be written instead of $[M]$.

Now the dynamics of the computation of λ-terms will be defined.

Definition A.0.7. Single step β-reduction $\to_\beta$ is the smallest relation on Λ satisfying:

- the **reduction axiom**:
  - for all variables x and λ-terms M, M', $(\lambda x.M)M' \to_\beta M[x := M']$, where $M[x := M']$ is the term given by replacing every free occurrence of x in M with M',
- the following **compatibility axioms**:
  - if $M \to_\beta M'$ then $(MN) \to_\beta (M'N)$ and $(NM) \to_\beta (NM')$,
  - if $M \to_\beta M'$ then for any variable x, $\lambda x.M \to_\beta \lambda x M'$.

A subterm of the form $(\lambda x.M)M'$ is a **β-redex**, and $(\lambda x.M)M'$ **single step β-reduces** to $M[x := M']$.

Remark A.0.8. Strictly, single step β reduction should be defined on preterms and then shown that a well defined relation is induced on terms, but this level of detail has been omitted for the sake of clarity.

Remark A.0.9. The reducition axiom shows precisely in what sense a bound variable is a "marker for substitution". For example, $(\lambda x.x)M \to_\beta M$ and $(\lambda y.y)M \to_\beta M$, which is why $\lambda x.x$ is identified with $\lambda y.y$.

It is through single step β-reduction that computation may be performed. In fact, λ-calculus is capable of performing natural number addition:

Example A.0.10. Define the following λ-terms:

- ONE := $\lambda fx.fx$,
- TWO := $\lambda fx.ffx$,
- THREE := $\lambda fx.fffx$,
- PLUS := $\lambda mnfx.mf(nfx)$

then

$$\begin{aligned}
PLUS\ ONE\ TWO &= (\lambda mnfx.\underline{m}f(nfx))\underline{(\lambda fx.fx)}(\lambda fx.ffx)\\
&\to_\beta (\lambda nfx.(\lambda fx.\underline{f}x)\underline{f}(nfx))(\lambda fx.ffx)\\
&\to_\beta (\lambda nfx.(\lambda x.f\underline{x})\underline{(nfx)})(\lambda fx.ffx)\\
&\to_\beta (\lambda nfx.f\underline{n}fx)\underline{(\lambda fx.ffx)}\\
&\to_\beta (\lambda fx.f(\lambda fx.\underline{ff}x)\underline{f}x)\\
&\to_\beta (\lambda fx.f(\lambda x.ff\underline{x})\underline{x})\\
&\to_\beta (\lambda fx.fffx) = THREE
\end{aligned}$$

where each step is obtained by substituting the right most underlined λ-term inplace of the left most underlined variable.

Historically, is this how Church first defined computable functions.

B Regular and quasi-regular sequences

We define:

Definition B.0.1. The **mapping cone** of multiplication $\mathscr{G} \xrightarrow{y} \mathscr{G}$ is the tensor product:

$$K(y) \otimes \mathscr{G} \tag{336}$$

The usefulness of the mapping cone comes from the following property:

Proposition B.0.2. *Let $\mathscr{G}$ be a chain complex of R-modules and let $y \in R$ be an arbitrary element of R. Then there exists a long exact sequence of homology groups:*

$$\cdots \longrightarrow H_{i-1}(\mathscr{G}) \xrightarrow{y} H_{i-1}(\mathscr{G}) \longrightarrow H_i(K(y) \otimes \mathscr{G}) \longrightarrow H_i(\mathscr{G}) \xrightarrow{y} H_i(\mathscr{G}) \longrightarrow \cdots \tag{337}$$

where the connecting morphisms are multiplication by y.

Proof. Construct the following short exact sequence of chain complexes:

$$\begin{tikzcd}
R(-1) \arrow[d] & 0 \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & R \arrow[r] \arrow[d] & 0 \arrow[d] \\
K(y) \arrow[d] & 0 \arrow[r] \arrow[d] & R \arrow[r, "y"] \arrow[d] & R \arrow[r] \arrow[d] & 0 \arrow[d] \\
R & 0 \arrow[r] & R \arrow[r] & 0 \arrow[r] & 0
\end{tikzcd} \tag{338}$$

We can tensor this entire diagram with $\mathscr{G}$ to obtain the following short exact sequence:

$$\begin{tikzcd}
\mathscr{G}(-1) \arrow[d] & \cdots \arrow[r] & G_{i-2} \arrow[r] \arrow[d] & G_{i-1} \arrow[r] \arrow[d] & G_i \arrow[r] \arrow[d] & \cdots \\
K(y) \otimes \mathscr{G} \arrow[d] & \cdots \arrow[r] & G_{i-2} \oplus G_{i-1} \arrow[r] \arrow[d] & G_{i-1} \oplus G_i \arrow[r] \arrow[d] & G_i \oplus G_{i+1} \arrow[r] \arrow[d] & \cdots \\
\mathscr{G} & \cdots \arrow[r] & G_{i-1} \arrow[r] & G_i \arrow[r] & G_{i+1} \arrow[r] & \cdots
\end{tikzcd} \tag{339}$$

which induces the exact sequence (331). □

B.0.1 Regular sequences and the Koszul complex

Throughout, all rings are commutative, associative, and unital.

Definition B.0.3. Let M be a left R-module. A sequence $(x_1, ..., x_n)$ where each $x_i \in R$ is **regular** if

- for all $i = 1, ..., n$ the element f_i is a nonzerodivisor of $M/(x_1, ..., x_{i-1})M$
- the module $M/(x_1, ..., x_n)M$ is non-zero.

For now we focus on regular sequences of a *ring*, which of course obeys the same definition as B.0.3 where the ring is considered as a module over itself.

Example B.0.4. Let k be a field, the sequence $(x, y(1-x), z(1-x))$ is regular in $k[x, y, z]$

Proof.

- x is clearly a nonzerodivisor of $k[x,y,z]$.
- Say $m \in k[x,y,z]/(x)$ satisfied $m(y(1-x)) = 0$, then y is a zero divisor in $k[x,y,z]/(x) \cong k[y,z]$ which is a contradiction.
- A similar argument shows that $z(1-x)$ is not a zero divisor of $k[x,y,z]/(x,y)$
- Lastly, $1 \neq 0 \in k[x,y,z]/(x,y,z)$.

□

Remark B.0.5. It is *not* necessarily the case that for a regular sequence $(f_1, ..., f_n)$ in a ring R, f_j is a non zero divisor of $R/(f_1, ..., f_{j-2})$. For instance, the sequence (x,y) is a regular sequence in $k[x,y,w_1,w_2,...]/I$, where k is a field and I is the ideal generated by all yw_i and all $w_i - xw_{i+1}$, even though y is a zero divisor.

One way of thinking about regular sequences is that they "cut R down" as much as possible at each stage of modding out. More precisely, if r is a non zero divisor of R then the map $R \to R$ given by multiplication by r is injective. In this sense we "kill just as much, if not more of R" by modding out by (r) than if we had modded out by (r'), where $r' \in R$ is a zero divisor.

Definition B.0.6. Let M be a left R-module and $x \in M$ an element. The **Koszul complex** $K(x)$ is the following chain complex

$$0 \longrightarrow R \longrightarrow M \longrightarrow \wedge^2 M \longrightarrow \wedge^3 M \longrightarrow \cdots \longrightarrow \wedge^n M \xrightarrow{d_x^n} \wedge^{n+1} M \longrightarrow \cdots \tag{340}$$

where $d_x^n : \wedge^n M \longrightarrow \wedge^{n+1} M$ is defined by the rule $m \longmapsto x \wedge m$.

In the special case where $M = R^m$ and $x = (x_1, ..., x_m)$ we write $K(x_1, ..., x_n)$ for $K(x)$.

Example B.0.7. Let $M = R^2$ and let $x, y \in R$. Then $K(x,y)$ is the following chain complex:

$$0 \longrightarrow R \longrightarrow R^2 \longrightarrow \wedge^2 R^2 \longrightarrow \wedge^3 R^2 \longrightarrow 0 \longrightarrow \cdots \tag{341}$$

which is such that the following diagram commutes, with vertical arrows isomorphisms

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & R \arrow[r, "d^1_{(x,y)}"] \arrow[d] & R^2 \arrow[r, "d^2_{(x,y)}"] \arrow[d] & \wedge^2 R^2 \arrow[r, "d^3_{(x,y)}"] \arrow[d] & \wedge^3 R^2 \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & R \arrow[r, "\begin{pmatrix} x \\ y \end{pmatrix}"] & R^2 \arrow[r, "\begin{pmatrix} y & -x \end{pmatrix}"] & R \arrow[r] & 0 \arrow[r] & \cdots
\end{tikzcd} \tag{342}$$

so we obtain a simple special case.

Further, in the setting where $M = R$ and $x \in R$, the Koszul complex $K(x)$ is simply multiplication by x:

$$0 \longrightarrow R \xrightarrow{x} R \tag{343}$$

We can use the simple description given in Example B.0.7 to solve an exercise:

Exercise B.0.8. Show that if

$$M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{344}$$

is a matrix of elements in R such that M has determinant given by a unit in R, then $K(x,y) \cong K(ax+by, cx+dy)$.

Proof. We construct the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & R \arrow[r] \arrow[d, "\mathrm{id}_R"] & R \oplus R \arrow[r] \arrow[d, "M"] & R \arrow[r] \arrow[d, "\det M"] & 0 \\
0 \arrow[r] & R \arrow[r] & R \oplus R \arrow[r] & R \arrow[r] & 0
\end{tikzcd} \tag{345}$$

which is invertible by the assumptions on M. □

B.0.2 Koszul Complex and lengths of maximal regular sequences

We will now relate the homology of the Koszul complex to lengths of maximal regular sequences. In the following we make use of the notation:

Notation B.0.9. For ideals I, J, denote:

$$(I : J) := \{f \in R \mid fJ \subseteq I\} \tag{346}$$

Remark B.0.10. The Koszul complex $K(x,y)$ admits $K(x)$ as a subcomplex, which then pushes forward to a cokernel, yielding the following commutative diagram where the vertical sequences are exact:

$$\begin{tikzcd}
0 \arrow[r] & R \arrow[r, "x"] & R \arrow[r] & 0 \\
0 \arrow[r] & R \arrow[u, "\mathrm{id}_R"] \arrow[r, "{\begin{pmatrix} x \\ y \end{pmatrix}}"] & R \oplus R \arrow[u, "\pi_2"] \arrow[r, "{\begin{pmatrix} y & -x \end{pmatrix}}"] & R \arrow[u] \\
& 0 \arrow[u] \arrow[r] & R \arrow[u, "\iota_1"] \arrow[r, "-x"] & R \arrow[u, "\mathrm{id}_R"']
\end{tikzcd} \tag{347}$$

and so we obtain a long exact sequence of homology:

$$0 \longrightarrow H^0(K(x)) \xrightarrow{\delta} H^0(K(x)) \longrightarrow H^1(K(x,y)) \longrightarrow H^1(K(x)) \longrightarrow 0 \tag{348}$$

where the connecting morphism δ is multiplication by y (as can easily be checked).

Notice that if $H^1(K(x,y)) = 0$ then

$$H^0(K(x))/yH^0(K(x)) \cong 0 \tag{349}$$

Under the further assumption that R is a Noetherian local and y is an element of the maximal ideal, we obtain from Nakayama's Lemma that $H^0(K(x)) \cong 0$.

So what is the consequence of this? Since $H^0(K(x)) \cong 0$, we have that x is a nonzerodivisor, as follows straight from the definition. Now we investigate $H^1(K(x,y)) \cong 0$. Since x is a nonzerodivisor, if we have $a, b \in R$ such that $-ax+by = 0$, then a is uniquely determined by b, we let k_a denote this b. In fact, we obtain an isomorphism

$$\begin{aligned} \gamma : (x:y) &\longrightarrow \ker(x \; y) \\ a &\longmapsto (a, -k_a) \end{aligned}$$

Moreover, the image of $R \longrightarrow R \oplus R$ is isomorphic to (x), so we have

$$H^1(K(x,y)) \cong (x:y)/(x) \tag{350}$$

So $H^1K(x,y) \cong 0$ implies $(x:y) = (x)$. In other words, if $f \in R$ is such that $fy \in (x)$ then $f \in (x)$. That is to say that y is a nonzerodivisor of $R/(x)$.

Thus we have proved (the first part of):

Proposition B.0.11. *If R is a Noetherian local ring, and x, y are elements of the maximal ideal, then $H^1(K(x,y)) \cong 0$ if and only if x, y is a regular sequence of R.*

Do regular sequences remain regular if the elements are permuted? In general, no, as Example B.0.12 shows, but Observation B.0.10 can be used to provide a setting where permuting elements of a regular sequence *does* result in a regular sequence (see Proposition B.0.13).

Example B.0.12. Consider the ring $R := k[x,y,z]/(xz)$ along with the sequence $(x-1, xy)$. This sequence is regular as $x-1$ is not a zerodivisor of R and $R/(x-1) \cong k[y] \ncong 0$ inside which y is not a zerodivisor. However, the sequence $(xy, x-1)$ is not regular as xy is a zero divisor in R.

Proposition B.0.13. *Let R be a Noetherian local ring with maximal ideal m and let $(x_1, ..., x_n)$ be a regular sequence with each x_i an element of m. Then any for any permutation $\rho : \{1, ..., n\} \longrightarrow \{1, ..., n\}$ the sequence $(x_{\rho(1)}, ..., x_{\rho(n)})$ is regular.*

Proof. First we prove the case when $n = 2$. We have already seen that the sequence (x_1, x_2) is regular if and only if $H^1(K(x_1, x_2)) \cong 0$ (in the context given by the hypotheses). We then observe the following isomorphism $K(x_1, x_2) \cong K(x_2, x_1)$, where $s : R \oplus R \longrightarrow R \oplus R$ is the swap map $s(r_1, r_2) = (r_2, r_1)$.

$$\begin{tikzcd} 0 \arrow[r] & R \arrow[r] \arrow[d, "\mathrm{id}_R"] & R \oplus R \arrow[r] \arrow[d, "s"] & R \arrow[r] \arrow[d, "-\mathrm{id}_R"] & 0 \\ 0 \arrow[r] & R \arrow[r] & R \oplus R \arrow[r] & R \arrow[r] & 0 \end{tikzcd} \tag{351}$$

Now we abstract to the general setting. Let $(x_1, ..., x_n)$ be regular, it suffices to show that $(x_1, ..., x_{i+1}, x_i, ..., x_n)$ is regular. In turn, it suffices to show that x_{i+1}, x_i is regular in $R/(x_1, ..., x_{i-2})$ which then follows from the first part of this proof. □

The Koszul complex can sometimes provide information about when a sequence is regular or not.

Theorem B.0.14. *Let M be a finitely generated module over a local ring (R, m). Suppose $x_1, ..., x_n \in m$. If for some k we have:*

$$H^k(M \otimes K(x_1, ..., x_n)) \cong 0 \tag{352}$$

then

$$\forall j \leq k, \quad H^j(M \otimes K(x_1, ..., x_n)) \cong 0 \tag{353}$$

Moreover, if $H^{n-1}(M \otimes K(x_1, ..., x_n)) \cong 0$ then $(x_1, ..., x_n)$ is regular.

We will need the following Lemma to prove Theorem B.0.14.

Lemma B.0.15. *Let $N \cong N' \oplus N''$ be a module and $x = (x', x'')$ an element of N. We have*

$$K(x) \cong K(x') \otimes K(x'') \tag{354}$$

Proof. We have from Proposition 5.2.17 that there exists an isomorphism of graded algebras $\wedge N \cong \wedge N' \otimes \wedge N''$, hence it suffices to check commutativity of the following diagram, in what follows we write Ψ^n for the homomorphism Ψ restricted to $\wedge^n N$.

$$\begin{tikzcd}
\cdots \arrow[r] & \wedge^n N \arrow[r] \arrow[d, "\Psi^n"] & \wedge^{n+1} N \arrow[r] \arrow[d, "\Psi^{n+1}"] & \cdots \\
\cdots \arrow[r] & (\wedge N' \otimes \wedge N'')^n \arrow[r] & (\wedge N' \otimes \wedge N'')^{n+1} \arrow[r] & \cdots
\end{tikzcd} \tag{355}$$

To check commutativity of this, we consider an arbitrary element $y \in \wedge N$ which maps under Ψ to a pure tensor $y_1 \otimes y_2$, indeed it suffices to consider such elements. We calculate:

$$\begin{aligned} x \wedge y &\longmapsto (x_1 \otimes 1 + 1 \otimes x_2) \wedge (y_1 \otimes y_2) \\ &= x_1 \wedge y_1 \otimes y_2 + (-1)^{y_1} y_1 \otimes x_2 \wedge y_2 \end{aligned}$$

On the other hand, we have

$$\begin{aligned} (d_{x_1} \otimes d_{x_2})(y_1 \otimes y_2) &= d_{x_1}(y_1) \otimes y_2 + (-1)^{y_2} y_1 \otimes d_{x_2}(y_2) \\ &= x_1 \wedge y_1 \otimes y_2 + (-1)^{y_1} y_1 \otimes x_2 \wedge y_2 \end{aligned}$$

The result follows. □

Remark B.0.16. We touch on a subtle point. Notice that Definition B.0.6 defined the Koszul complex in a general setting where the differential is given by multiplication by an element of the *module* M (as apposed to multiplication by an element of the *ring* R). We wish to relate the Koszul complex $K(x_1,...,x_n)$ to regularity of the sequence $(x_1,...,x_n)$ however in Definition B.0.3 we required that $x_1,...,x_n$ be elements of R. Hence, in order to relate the Koszul complex to regularity of a sequence, we will chiefly be concerned with the special case of the Koszul complex where multiplication is by an element in the *ring* R. In this case, for $x \in R$ we have $M \otimes K(x) \cong K(x \cdot 1_R)$ which follows from the isomorphism $R \otimes M \cong M$.

Remark B.0.17. Recall that we established in a general setting the existence of a long exact sequence given a chain complex $\mathscr{G}$ over a ring R along with an element $y \in R$ (Proposition B.0.2). If M is a module, $x_1, x_2 \in R$, we let $\mathscr{G}$ be $M \otimes K(x_1)$ and $y = x_2$, we first note that:

$$K(x_2) \otimes (M \otimes K(x_1)) = M \otimes K(x_1, x_2)$$

and hence we obtain the following long exact sequence.

$$0 \longrightarrow H^0(M \otimes K(x_1)) \xrightarrow{x_2} H^0(M \otimes K(x_1)) \longrightarrow H^1(M \otimes K(x_1, x_2)) \longrightarrow 0 \tag{356}$$

In fact, more can be said. Recall the following identity which holds for all $1 \leq m \leq n$.

$$\binom{n-1}{m} + \binom{n-1}{m-1} = \binom{n}{m} \tag{357}$$

Hence there exists an isomorphism:

$$\wedge^m R^{n-1} \oplus \wedge^{m-1} R^{n-1} \cong \wedge^m R^n \tag{358}$$

which in turn implies the existence of an isomorphism:

$$\Psi_m : (M \otimes \wedge^m R^{n-1}) \oplus (M \otimes \wedge^{m-1} R^{n-1}) \cong M \otimes \wedge^m R^n \tag{359}$$

This can be used to show that $K(x_n) \otimes (M \otimes K(x_1,...,x_{n-1})) \cong M \otimes K(x_1,...,x_n)$, simply observe the following isomorphism of chain complexes, where the top row is $M \otimes K(x_1,...,x_n)$ and the bottom row is $K(x_n) \otimes (M \otimes \wedge^{m-1} R^{n-1})$.

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d] & M \otimes R^n \arrow[r] \arrow[d, "\psi_1"] & M \otimes \wedge^2 R^n \arrow[r] \arrow[d, "\psi_2"] & \cdots \arrow[r] & M \otimes \wedge^n R^n \arrow[r] \arrow[d, "\psi_n"] & 0 \\
0 \arrow[r] & M \arrow[r] & M \otimes (R \oplus R^{n-1}) \arrow[r] & M \otimes (R^{n-1} \oplus \wedge^2 R^{n-1}) \arrow[r] & \cdots \arrow[r] & M \otimes (\wedge^n R^{n-1} \oplus \wedge^{n-1} R^{n-1}) \arrow[r] & 0
\end{tikzcd} \tag{360}$$

Again, using Proposition B.0.2 we obtain a long exact sequence.

$$\begin{aligned}
\cdots \longrightarrow H^i(M \otimes K(x_1,...,x_{n-1})) \xrightarrow{x_n} H^i(M \otimes K(x_1,...,x_{n-1})) \longrightarrow H^{i+1}(M \otimes K(x_1,...,x_n)) \\
\longrightarrow H^{i+1}(M \otimes K(x_1,...,x_{n-1})) \xrightarrow{x_n} \cdots
\end{aligned}$$

We are nearly in a position to prove Theorem B.0.14, however we need one more result. Proposition B.0.18 writes $H^i(M \otimes K(x_1, ..., x_n))$ out in an explicit form. We adopt the following notation, where I is an ideal of R and M, N are R-modules:

$$(N : IM) \coloneqq \{m \in M \mid Jm \subseteq N\} \tag{361}$$

Notice that $(N : IM)$ is itself an R-module.

Proposition B.0.18. *Let M be finitely generated and $(x_1, ..., x_n)$ is a regular sequence. Then:*

$$H^i(M \otimes K(x_1, ..., x_n)) \cong \big((x_1, ..., x_i)M : (x_1, ..., x_n)\big)/(x_1, ..., x_i)M \tag{362}$$

Proof. We proceed by induction on n. The base case, when $n = 2$, is proved in an exactly similar way to what was done in Observation B.0.10. Now we assume that $n > 3$ and the result holds for $n - 1$. Consider the following.

$$\begin{aligned} H^i(M \otimes K(x_1, ..., x_{n-1})) &\cong \big((x_1, ..., x_i)M : (x_1, ..., x_{n-1})\big)/(x_1, ..., x_i)M \\ &\cong 0 \end{aligned}$$

where the first $\cong$ follows from the inductive hypothesis and the second $\cong$ follows from the fact that $(x_1, ..., x_n)$ is a regular sequence. Using the long exact sequence of Remark B.0.17 we infer that the kernel of the endomorphism on the following module given by multiplication by x_n.

$$H^i(M \otimes K(x_1, ..., x_{n-1})) \tag{363}$$

is isomorphic to $H^i(M \otimes K(x_1, ..., x_n))$. We now use the inductive hypothesis to infer that $H^i(M \otimes K(x_1, ..., x_n))$ is isomorphic to the kernel of the endomorphism on the following module given by multiplication by x_n.

$$\big((x_1, ..., x_i)M : (x_1, ..., x_{n-1})\big)/(x_1, ..., x_i)M \tag{364}$$

The proof is then complete once it is shown that the kernel of this map is isomorphic to the module given in Equation 356. Indeed, an isomorphism is given by the rule $m \longmapsto m$, one checks that the defining conditions of both modules are equivalent. □

Proof of Theorem B.0.14. We proceed by induction on n. The base case, that $K(M \otimes K(x_1, x_2)) \cong 0$ implies that (x_1, x_2) is a regular sequence follows exactly similarly to what was shown in Observation B.0.10. Now we proceed with the inductive step, assume that $n > 2$ and assume the result holds true for all $2 \leq i < n$. We first consider the endomorphism on $H^{n-1}(M \otimes K(x_1, ..., x_{n-1}))$ given by multiplication by x_n. Since $H^i(M \otimes K(x_1, ..., x_n)) \cong 0$, it follows from the long exact sequence of Remark B.0.17 that the endomorphism x_n is surjective. Hence, by Nakayama's Lemma, we have that $H^{n-1}(M \otimes K(x_1, ..., x_{n-1})) \cong 0$. By the inductive hypothesis, this implies that $(x_1, ..., x_{n-1})$ is a regular sequence, and it remains to show that x_n is not a zero divisor of $M/(x_1, ..., x_{n-1})M$.

To do this, we invoke Proposition B.0.18. Indeed,$(x_1, ..., x_n)$ is regular and so:

$$\big((x_1, ..., x_{n-1})M : (x_1, ..., x_n)\big)/(x_1, ..., x_i)M \cong 0 \tag{365}$$

completing the proof. □

The following two results are bonus, and are not relevant to the core point of this Section. Indeed, these results are used in [**?**, §17.3] as part of an investigation into what happens when R is not local.

Proposition B.0.19. *Let $x_1, ..., x_n \in R$ be elements of R and I the ideal they generate. Assume $y_1, ..., y_r \in I$ are elements of I, then there is an isomorphism*

$$K(x_1, ..., x_n, y_1, ..., y_r) \cong K(x_1, ..., x_n) \otimes \wedge R^r \tag{366}$$

Proof. First, write $y_i = \sum_{j=1}^n a_{ij} x_j$ for each y_i and let A denote the matrix (a_{ij}). Then there is an automorphism of $R^n \oplus R^r$ given by the matrix

$$F := \begin{pmatrix} I & 0 \\ -A & I \end{pmatrix} \tag{367}$$

indeed an inverse is given by

$$\begin{pmatrix} I & A \\ 0 & I \end{pmatrix} \tag{368}$$

Notice that F is such that $F(x_1, ..., x_n, y_1, ..., y_r) = (x_1, ..., x_n, 0, ..., 0)$. We state without proof that the Koszul complex is functorial, and so we thus have

$$K(x_1, ..., x_n, y_1, ..., y_r) \cong K(x_1, ..., x_n, 0, ..., 0) \tag{369}$$

Moreover, using Lemma B.0.15 we have $K(x_1, ..., x_n, 0, ..., 0) \cong K(x_1, ..., x_n) \otimes K(0, ..., 0) \cong K(x_1, ..., x_n) \otimes \wedge R^r$. . □

Corollary B.0.20. *Let M be any R-module, and $x_1, ..., x_n, y_1, ..., y_r$ as in Proposition B.0.19. Then*

$$H^*(M \otimes K(x_1, ..., x_n, y_1, ..., y_r)) \cong H^*(M \otimes K(x_1, ..., x_n)) \otimes \wedge R^r \tag{370}$$

and so for each i,

$$H^i(M \otimes K(x_1, ..., x_n, y_1, ..., y_r)) \cong \sum_{i=j+k} H^k(M \otimes K(x_1, ..., x_n)) \otimes \wedge^j R^r \tag{371}$$

Thus

$$H^i(M \otimes K(x_1, ..., x_n, y_1, ..., y_r)) = 0 \tag{372}$$

if and only if

$$H^k(M \otimes K(x_1, ..., x_n)) \cong 0 \textit{ for all } k \textit{ such that } i - r \le k \le i \tag{373}$$

Proof. The first statement follows from flatness of $\wedge^j R^r$ (indeed, it is free), the rest are obvious. □

B.1 Regular sequences are quasi-regular

Now, let $(f_1, ..., f_n)$ be regular in some ring R and denote by J the ideal generated by these elements. For any $m \geq 0$ the scalar multiplication by R on J^m/J^{m+1} descends to one of R/J, thus rendering J^m/J^{m+1} an R/J-module. Moreover, these scalars can be extended to $(R/J)[x_1, ..., x_n]$ by defining $x_i \cdot [r]_J = [f_i r]_J = [0]_J$. There is then an $(R/J)[x_1, ..., x_n]$-module homomorphism

$$(R/J)[x_1, ..., x_n] \to \bigoplus_{m \geq 0} J^m/J^{m+1} \tag{374}$$

defined by the rule

$$x_1^{i_1} ... x_n^{i_n} \mapsto f_1^{i_1} ... f_n^{i_n} \bmod J^{i_1 + ... + i_n + 1}$$

which is surjective.

Definition B.1.1. Such a sequence is **quasi-regular** if the above map is an isomorphism.

Indeed this is to be thought of as a weakening of the notion of regular sequences, as justified by the following Lemma:

Lemma B.1.2. *If a sequence $(f_1, ..., f_n)$ of R is regular, it is quasi-regular.*

Proof. Throughout, the notation $|I|$ where I is a sequence of natural numbers will mean $\sum_{i \in I} i$.

We proceed by induction on n. When $n = 0$ notice that the composite

$$(R/J) \overset{(368)}{\longrightarrow} \bigoplus_{m \geq 0} J^m/J^{m+1} \cong R/J$$

is the identity map, so the result clearly holds for the base case.

Now say $n \geq 1$. Let $\sum_{|I|=m} [\alpha_I]_J [f^I]_{J^{m+1}} = [0]_{J^m}$, in other words, say $\sum_{|I|=m} \alpha_I f^I$ as an element of R is in J^{m+1}. Let $\sum_{|I|=m} \alpha_I f^I = \sum_{|I'|=m+1} \beta_{I'} f^{I'}$. By substituting each $\beta_{I'}$ by $\hat{\beta}_I := \beta_{I'} f_{i_1}$, we have $\sum_{|I|=m} \alpha_I f^I = \sum_{|I|=m} \hat{\beta}_I f^I$, where each $\hat{\beta}_I \in J$. That is to say, $\sum_{|I|=m} \hat{\alpha}_I f^I = 0$ where $\hat{\alpha}_I = \alpha_I - \hat{\beta}_I$. Thus we may assume that in fact $\sum_{|I|=m} \alpha_I f^I = 0$. It remains to show that each $\alpha_I \in J$.

Next we rewrite $\sum_{|I|=m} \alpha_I f^I$ as a sum where each occurrence of f_n in f^I has been factored out. We let m' denote the largest integer such that a summand of $\sum_{|I|=m} \alpha_I f^I$ contains m' factors of f_n in the product f^I:

$$\sum_{|I|=m} \alpha_I f^I = \sum_{j=0}^{m'} \Big(\sum_{|I'|=m-j} \alpha_{I,j} f^{I',j} \Big) f_n^j = 0$$

the relabelling of α_I by $\alpha_{I,j}$ is for clarity later on. We now prove that in such a setting, we have that $\alpha_I \in J$ by induction on m'.

Denote the ideal $(f_1, ..., f_{n-1})$ by J'. If $m' = 0$ then $\sum_{|I'|=m} \alpha_I f^{I'} = 0$ where $f^{I'} \in (f_1, ..., f_{n-1})^m$ and so each $\alpha_I \in J$ by the hypothesis of induction on n.

Now say $m' \geq 1$. Then (and this is the step which takes advantage of reducing the proof to the case when $\sum_{|I|=m} \alpha_I f^I = 0$):

$$\Big(\sum_{|I'|=m-m'} \alpha_{I,m'} f^{I',j} \Big) f_n^{m'} = -\Big(\sum_{j=0}^{m'-1} \Big(\sum_{|I'|=m-j} \alpha_{I,j} f^{I',j} \Big) f_n^j \Big) \in (J')^{m-m'+1}$$

That is to say, $\Big(\sum_{|I'|=m-m'} [\alpha_{I,m'}]_J [f^{I'}]_{(J')^{m-m'+1}} \Big) [f_n^{m'}]_{(J')^{m-m'+1}} = [0]_{(J')^{m-m'+1}}$. It follows by the hypothesis of induction on n that $f_n^{m'} \alpha_I \in J'$. Now we make use of the hypothesis that $(f_1, ..., f_n)$ is regular, and indeed this is the key moment in the proof. Since $f_n^{m'}$ is not a zero divisor of R/J', we deduce that $\alpha_{I,m'} \in J' \subseteq J$. It now remains to show that the remaining $\alpha_{I,j} \in J$.

For this, we write:

$$\sum_{j=0}^{m'} \Big(\sum_{|I'|=m-j} \alpha_{I,j} f^{I',j} \Big) f_n^j = \sum_{|I'|=m-j} \Big(\alpha_{I,m'-1} f^{I',j} + f_n \alpha_{I,m'} f^{I',j} \Big) f_n^{m'-1} + \sum_{j=0}^{m'-2} \Big(\sum_{|I'|=m-j} \alpha_{I,j} f^{I',j} \Big) f_n^j = 0$$

so by the hypothesis of induction on m' we have that $\alpha_{I,m'-1} + f_n \alpha_{I,m'} \in J$ and $\alpha_{I,j} \in J$ for all $j \leq m' - 2$. The final observation to make is that since $f_n \alpha_{I,m'} \in J$ it follows that $\alpha_{I,m'-1} \in J$. □

References

[1] *Linear Logic*, J.Y. Girard. Theoretical Computer Science, Volume 50, Issue 1, Jan. 30, 1987.

[2] *Multiplicatives*, J.Y. Girard. Logic and Computer Science: New Trends and Applications. Rosenberg & Sellier. pp. 11–34 (1987).

[3] *Geometry of Interaction: Interpretation of System F*, J.Y. Girard. Categories in Computer Science and Logic, pages 69 – 108, Providence, 1989.

[4] *Geometry of Interaction II, Deadlock Free Agorithms* Part of the Lecture Notes in Computer Science book series (LNCS,volume 417). 2005.

[5] *Geometry of Interaction III, Accomodation the Additives*, J.Y. Girard. Proceedings of the workshop on Advances in linear logic. June 1995

[6] *Geometry of Interaction IV, the Feedback Equation*, J.Y. Girard. Logic Colloquium 2003, December 9.

[7] *Geometry of Interaction V*, J.Y. Girard. Theoretical Computer ScienceVolume 412Issue 20April, 2011

[8] *Linear Logic and the Hilbert Space* Advances in Linear Logic , pp. 307 - 328, Cambridge University Press, 1995.

[9] *Interaction Graphs: Multiplicatives* Annals of Pure and Applied Logic 163 (2012), pp. 1808-1837.

[10] *Interaction Graphs: Additives* Annals of Pure and Applied Logic 167 (2016), pp. 95-154.

[11] *Interaction Graphs: Nondeterministic Automata*, ACM Transactions in Computational Logic 19(3), 2018.

[12] *Interaction Graphs: Exponentials* Logical Methods in Computer Science 15, 2019.

[13] *Olivier Laurent. A Token Machine for Full Geometry of Interaction.* 2001, pp.283-297. ⟨hal-00009137⟩

[14] *Towards a Typed Geometry of Interaction* CSL 2005: Computer Science Logic pp 216–231.

[15] *From a conjecture of Collatz to Thompson's group F, via a conjunction of Girard*, `https://arxiv.org/abs/2202.04443`

[16] *The Blind Spot.* J.Y. Girard.

[17] *Normal functors, power series and lambda-calculus* Annals of Pure and Applied Logic Volume 37, Issue 2, February 1988, Pages 129-177.

[18] *Gentzen-Mints-Zucker Duality* D. Murfet, W. Troiani. `https://arxiv.org/abs/2008.10131`

[19] *An introduction to proof nets.* O. Laurent. `http://perso.ens-lyon.fr/olivier.laurent/pn.pdf`

[20] *Elimination and cut-elimination in multiplicative linear logic*, W. Troiani, D. Murfet.

[21] *Sense and Reference* G. Frege. Philosophical Review 57 (3):209-230 (1948)

[22] *Lectures on the Curry-Howard Isomorphism* Published: July 4, 2006 Imprint: Elsevier Science