university of groningen / faculty of science and engineering / mathematics and applied mathematics

Conjunctions of equivalences: logic meets linear algebra

Bachelor's Project Mathematics

July 2019

Student: M.J.R. Meijering

First supervisor: Prof. dr. G.R. Renardel de Lavalette

Second assessor: Prof. dr. J. Top

Abstract

We consider fragments of classical propositional logic obtained by taking conjunctions of formulae built up using only atoms and the biconditional $\leftrightarrow$. In characterizing these fragments, we find a direct connection with linear subspaces of a vector space over the two-element field. When the logical contradiction is added to the set of propositional atoms, a connection is obtained with a more specific set of linear subspaces. It turns out that the size of the fragments that include logical contradiction can be calculated based on the size of the fragments in which it is not included.

Contents

1 Introduction **1**

2 Preliminaries **2**
2.1 Equivalences in classical propositional logic 2
2.2 Conjunctions of equivalences 4
2.3 The 2-element field 5
2.4 A vector space equipped with symmetric difference 6

3 Characterizing $\bigwedge[\mathsf{PR}, \leftrightarrow]/\equiv$ **8**
3.1 Equivalences and propositional models 8
3.2 An isomorphism with $\mathsf{CL}(\mathsf{PR})$ and determining the size 14

4 Introducing logical contradiction as an atom **17**
4.1 Determining the size of $\bigwedge[\{f, p_1, \ldots, p_n\}, \leftrightarrow]/\equiv$ 20

5 Conclusion **22**

1 Introduction

This bachelor's project is based on notes by Prof.dr. G.R. Renardel de Lavalette of the University of Groningen [5].

In this report we will discuss fragments of classical propositional logic. This logic deals with propositions, which are statements for which we can determine a truth value; either true (T) or false (F). For example, the sentences "I am wearing a hat" and "The sun is shining" are propositions, because they can be verified by taking a look. The sentence "I am wearing a hat and the sun is shining" is called a compound proposition, as it is an assembly of the two previous statements. Its truth value depends entirely on the truth values of the simpler statements of which it consists.

When studying logic, we are not so much interested in the specific statements. Instead, we like to obtain results that hold for all propositions. This is why we use propositional variables, representing arbitrary propositions of the simplest form (atoms) to which we can assign a truth value. Additionally, we have two special logical formulae, namely the tautology $\top$, which is always true, and the contradiction $\bot$, which is always false. In classical propositional logic, we apply logical connectives to the propositional variables to construct more complex propositions, but there are no predicates, non-logical objects or quantifiers involved. In this paper we make equivalences out of propositional variables by applying the biconditional operator and we then take conjunctions of these equivalences. Our main goal will be to characterize the logical fragments that are then established. In doing so, we resort to linear algebra.

In section 2 we will provide relevant definitions and notation for our specific logical fragments and the vector space in which we are interested. These are then used in section 3 to obtain results on equivalences and conjunctions of equivalences. Finally, in section 4 we will add the logical contradiction as a propositional atom and study the impact this has on our logical fragments.

2 Preliminaries

In this section, some definitions and concepts are discussed that can help us explore the fragments of conjunctions of equivalences and prove a duality. We will start with another look at propositional logic itself and fragments of equivalences. After this we can continue with conjunctions of equivalences. Then, the 2-element field will be introduced and finally we will define the vector space over this field.

2.1 Equivalences in classical propositional logic

The simplest formulae in classical propositional logic are called propositional atoms. We combine them with logical connectives to construct more complex propositions. We denote the atoms by regular lower case letters and arbitrary propositions (which may or may not be more complex) by lower case Greek letters. The logical content of propositions can be illustrated in truth tables. Since we are interested in conjunctions and biconditionals, we will show the corresponding logical formulae. For arbitrary φ and ψ, the truth values for the statements $\varphi \wedge \psi$ and $\varphi \leftrightarrow \psi$ can be found in the following truth table.

φ	ψ	$\varphi \wedge \psi$	$\varphi \leftrightarrow \psi$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	T

We consider the set $\mathsf{PR} = \{p_1, ..., p_n\}$ of propositional variables. We define the power set of PR by $\wp(\mathsf{PR}) = \{P \mid P \subseteq \mathsf{PR}\}$. We denote its elements by the upper case letters P, Q and R and call them sets. In turn, the second power set of PR is defined by $\wp(\wp(\mathsf{PR})) = \{X \mid X \subseteq \wp(\mathsf{PR})\}$. We denote its elements by the upper case letters B, C, D, X and Y and call them collections.

The fragment $[\mathsf{PR}, \leftrightarrow]$ consists of all propositional formulae generated by elements of PR and the operator $\leftrightarrow$. We call these formulae *equivalences*. Recall that $\top$ is a formula that is always true. For arbitrary formulae φ, ψ, χ the biconditional shows several properties:

$$\begin{array}{lcl} \varphi \leftrightarrow \top & \equiv & \varphi \\ \varphi \leftrightarrow \varphi & \equiv & \top \\ \varphi \leftrightarrow \psi & \equiv & \psi \leftrightarrow \varphi \\ (\varphi \leftrightarrow \psi) \leftrightarrow \chi & \equiv & \varphi \leftrightarrow (\psi \leftrightarrow \chi) \end{array}$$

where $\equiv$ denotes logical equivalence, i.e. the term on the left-hand side always has the same truth value as the term on the right-hand side. The logical tautology functions as an identity element and multiple occurrences of the same proposition cancel out in pairs. We can also conclude that the order in an equivalence and the positioning of the brackets are irrelevant modulo $\equiv$. For simplicity,

we shall therefore denote an equivalence involving the variables $\{p_1, \ldots, p_k\}$ by $p_1 \leftrightarrow \ldots \leftrightarrow p_k$ and restrict ourselves to the fragment $[\mathsf{PR}, \leftrightarrow]/\equiv$, where logically equivalent statements are considered to be the same element.

We take samples of propositional variables and put them into an equivalence by defining the function $\mathsf{eq} : \wp(\mathsf{PR}) \to [\mathsf{PR}, \leftrightarrow]/\equiv$ as follows

$$\begin{array}{lcl} \mathsf{eq}(\emptyset) & = & \top \\ \mathsf{eq}(\{p\}) & = & p \\ \mathsf{eq}(\{p_1, \ldots, p_k\}) & = & p_1 \leftrightarrow \ldots \leftrightarrow p_k. \end{array}$$

Note that the name eq is an abbreviation for "equivalence". Every equivalence in the fragment can be expressed as $\mathsf{eq}(P)$ for some P in $\wp(\mathsf{PR})$ and every set maps to a different equivalence, so we have a bijection between $\wp(\mathsf{PR})$ and $[\mathsf{PR}, \leftrightarrow]/\equiv$. Since PR is a set with n elements, its power set contains 2^n elements. Namely, when choosing a subset of PR there are n binary choices to be made; the i^{th} is either in the subset or it is not. This means that in the case of n propositional variables we have 2^n different equivalences.

We observe that an equivalence is true if and only if it contains an even number of false variables. To explain this intuitively, note that in an equivalence every pair of false formulae generates one true formula and the same holds for a pair of true formulae. On the other hand, if one formula is true and another false, the result is a false equivalence. As an example, we consider the equivalence of the variables $p_1, \ldots, p_4$ and let them be represented by their truth values. On the left we have two true variables and two false variables, while on the right three variables are false and one is true.

$$\begin{array}{ccccccc} p_1 & \leftrightarrow & p_2 & \leftrightarrow & p_3 & \leftrightarrow & p_4 \\ \mathrm{T} & \leftrightarrow & \mathrm{F} & \leftrightarrow & \mathrm{T} & \leftrightarrow & \mathrm{F} \\ \mathrm{F} & \leftrightarrow & \mathrm{F} & \leftrightarrow & \mathrm{T} & \leftrightarrow & \mathrm{T} \\ & \mathrm{T} & & \leftrightarrow & & \mathrm{T} & \\ & & & \mathrm{T} & & & \end{array} \qquad \begin{array}{ccccccc} p_1 & \leftrightarrow & p_2 & \leftrightarrow & p_3 & \leftrightarrow & p_4 \\ \mathrm{F} & \leftrightarrow & \mathrm{F} & \leftrightarrow & \mathrm{T} & \leftrightarrow & \mathrm{F} \\ \mathrm{F} & \leftrightarrow & \mathrm{F} & \leftrightarrow & \mathrm{F} & \leftrightarrow & \mathrm{T} \\ \mathrm{F} & \leftrightarrow & \mathrm{F} & \leftrightarrow & & \mathrm{F} & \\ \mathrm{F} & \leftrightarrow & & \mathrm{T} & & & \\ & \mathrm{F} & & & & & \end{array}$$

We have rearranged the equivalence such that all the Fs are on the left and then we evaluate the truth values pairwise. In the case of an even amount of Fs, they cancel each other out and make the whole equivalence true. When the amount of false variables is odd, one F remains until the end, making the equivalence as a whole false. This property will be proven formally in a different context in Lemma 1. Before this can be done, we need to introduce our interpretation of subsets of PR as propositional models.

Subsets of PR can be considered as models of the propositional language over PR. Usually, if the set P represents a model, it makes all elements in P true, and the elements of $\mathsf{PR} - P$ false. In the present context, it turns out that the opposite interpretation is more convenient. Therefore, we say that the model P

makes its own elements false and those of $\mathsf{PR}-P$ true. For an arbitrary variable p and formulae φ and ψ we say

$$\begin{array}{lll} P \models p & \text{iff} & p \notin P \\ P \models \varphi \wedge \psi & \text{iff} & P \models \varphi \text{ and } P \models \psi \\ P \models \varphi \leftrightarrow \psi & \text{iff} & (P \models \varphi \text{ iff } P \models \psi). \end{array}$$

Furthermore, we say that the formula ψ is a *logical consequence* of φ (notation $\varphi \models \psi$) if every model that makes φ true also makes ψ true, i.e.

$$\varphi \models \psi \quad \text{iff} \quad \forall P(P \models \varphi \Rightarrow P \models \psi).$$

Now that the concept of propositional models is defined, we can verify if the function eq is an isomorphism based on order preservation. We consider two sets $P, Q \in \wp(\mathsf{PR})$ and check whether the following condition holds

$$\text{if } Q \subseteq P \quad \text{then} \quad \mathsf{eq}(P) \models \mathsf{eq}(Q).$$

Based on the concept that an equivalence is true if and only if an even number of its variables is false, we can find a counterexample.

Counterexample For $P = \{p_1, p_2\}$ and $Q = \{p_1\}$ we find a model $R = \{p_1, p_2\}$ such that $R \models \mathsf{eq}(P)$, but $R \not\models \mathsf{eq}(Q)$.

Hence, the order preservation condition does not hold. In this form, the function is not an isomorphism. As a final remark for this subsection, we introduce a way of characterizing a logical formula. Every equivalence in $[\mathsf{PR}, \leftrightarrow]/\equiv$ can be uniquely represented by the set of models that make it true:

$$[\![\varphi]\!] = \{P \mid P \models \varphi\}.$$

If two formulae of the fragment have the exact same representation by models, they are logically equivalent and therefore they must be the same.

2.2 Conjunctions of equivalences

We move on the fragment $\bigwedge[\mathsf{PR}, \leftrightarrow]$ of conjunctions of equivalences. We take any sample of equivalences from $[\mathsf{PR}, \leftrightarrow]$ and put the conjunction operator in between. So

$$\bigwedge[\mathsf{PR}, \leftrightarrow] = \{\varphi_1 \wedge \cdots \wedge \varphi_k \mid \varphi_1, \ldots, \varphi_k \in [\mathsf{PR}, \leftrightarrow]\}$$

The main operator is in this case the conjunction, for which several properties can be observed. For arbitrary formulae φ, ψ, χ we have

$$\begin{array}{lll} \varphi \wedge \top & \equiv & \varphi \\ \varphi \wedge \varphi & \equiv & \varphi \\ \varphi \wedge \psi & \equiv & \psi \wedge \varphi \\ (\varphi \wedge \psi) \wedge \chi & \equiv & \varphi \wedge (\psi \wedge \chi). \end{array}$$

Once again we see that $\top$ acts as an identity element, but the second statement shows that it is not unique in doing so. Similar to the biconditional, we see that the order of the formulae and the placement of the brackets do not impact the logical content. Taking this into account, we restrict ourselves to the fragment $\bigwedge[\mathsf{PR}, \leftrightarrow]/\equiv$.

Elements of this fragment can be constructed by taking collections (containing sets that in turn contain variables) and applying a function. We define the function $\mathsf{Ceq} : \wp(\wp(\mathsf{PR})) \to \bigwedge[\mathsf{PR}, \leftrightarrow]/\equiv$ by

$$\mathsf{Ceq}(X) = \bigwedge_{P \in X} \mathsf{eq}(P).$$

The name Ceq is again an abbreviation, it shows that we are dealing with a conjunction of equivalences. The function maps elements from $\wp(\wp(\mathsf{PR}))$ to $\bigwedge[\mathsf{PR}, \leftrightarrow]/\equiv$, but it is (unlike eq) not a bijection. Specifically, injectivity does not hold, since $\mathsf{Ceq}(X) \equiv \mathsf{Ceq}(Y)$ does not imply $X = Y$. This is illustrated by the following counterexample.

Counterexample

$$\mathsf{Ceq}(\{\{p_1\}, \{p_2\}\}) = p_1 \ \wedge \ p_2 \equiv p_1 \wedge (p_1 \leftrightarrow p_2) = \mathsf{Ceq}(\{\{p_1\}, \{p_1, p_2\}\})$$

One of the goals in this report will be to find a subset of $\wp(\wp(\mathsf{PR}))$ for which Ceq is an isomorphism. This would allow us to get a better picture of the fragment $\bigwedge[\mathsf{PR}, \leftrightarrow]/\equiv$ and for example count its elements.

2.3 The 2-element field

In linear algebra, it is often the case that vector spaces are defined over the field $\mathbb{R}$ of real numbers or $\mathbb{C}$ of complex numbers. However, there are many other sets that, equipped with addition and multiplication operations, can serve as field for a vector space. In particular, the two-element field $\mathbb{Z}_2$ is an option. This is a set consisting of only two numbers, commonly called 0 and 1, with addition and multiplication given by the tables below.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

This field has certain properties that do not apply to the real numbers. For example, we have $x + x = 0$ for all $x \in \mathbb{Z}_2$, implying that the characteristic of this field is 2. We also observe $x \cdot x = x$ for every element x in $\mathbb{Z}_2$.

Scalar multiplication in a vector space over $\mathbb{Z}_2$ is defined by $1\mathbf{v} = \mathbf{v}$ and $0\mathbf{v} = \mathbf{0}$, where $\mathbf{0}$ is the identity element of addition in the vector space. We observe the property $1\mathbf{v} + 1\mathbf{v} = (1 + 1)\mathbf{v} = \mathbf{0}$, so every element of the vector space is its own inverse.

In our case, we will define a vector space over $\mathbb{Z}_2$ where the vectors are sets of propositional variables. The next subsection introduces the addition operator for this vector space and provides extra definitions that will assist in obtaining a connection with our fragments of logic.

2.4 A vector space equipped with symmetric difference

We will consider a vector space over the two-element field using subsets of PR as vectors, with the symmetric difference Δ acting as the addition operator[1].

Definition 1 The *symmetric difference* of the sets P and Q is the union of the two set differences, i.e. $P\Delta Q = (P - Q) \cup (Q - P)$, where $P - Q = \{p \in P \mid p \notin Q\}$.

Intuitively, it might be easier to interpret it in the following way: The symmetric difference of P and Q is the set of elements that are either in P or in Q, but not in both, i.e. $P\Delta Q = (P \cup Q) - (P \cap Q)$.
Some properties are given by

$$\begin{array}{lcl} P\Delta\emptyset & = & P \\ P\Delta P & = & \emptyset \\ P\Delta Q & = & Q\Delta P \\ (P\Delta Q)\Delta R & = & P\Delta(Q\Delta R) \\ P\Delta Q = P \cup Q & \Leftrightarrow & P \cap Q = \emptyset \end{array}$$

The empty set $\emptyset$ is the identity element of the vector space, since $P\Delta\emptyset$ is equal to P for all P in $\wp(\mathsf{PR})$. Linear subspaces of the vector space are collections $X \subseteq \wp(\mathsf{PR})$ that are closed under Δ, i.e. for all P and Q in X we have $P\Delta Q$ in X. Any collection can be extended in such a way that the result is closed under symmetric difference. To illustrate this, we first define the function $\mathsf{dif} : \wp(\wp(\mathsf{PR})) \to \wp(\mathsf{PR})$ as follows

$$\begin{array}{lcl} \mathsf{dif}(\emptyset) & = & \emptyset \\ \mathsf{dif}(\{P\}) & = & P \\ \mathsf{dif}(\{P_1, \ldots, P_k\}) & = & P_1\Delta \ldots \Delta P_k. \end{array}$$

Note that the dif in fact represents a linear combination of the involved vectors. We can also express a set P by putting all its elements into singletons and then taking the dif of these sets, since they are all disjoint. That is,

$$P = \mathsf{dif}\big(\{\{p\} \mid p \in P\}\big).$$

This function can now be used to describe the Δ-closure of an arbitrary collection X.

Definition 2 For any collection $X \in \wp(\wp(\mathsf{PR}))$, its Δ-*closure* is given by

$$\Delta\mathsf{cl}(X) = \{\mathsf{dif}(Y) \mid Y \subseteq X\}$$

We observe the following properties regarding the Δ-closure:

$$\begin{array}{rcl} X & \subseteq & \Delta\mathsf{cl}(X) \\ \Delta\mathsf{cl}(\emptyset) & = & \{\emptyset\} \\ \Delta\mathsf{cl}(\{P,Q\}) & = & \{\emptyset, P, Q, P\Delta Q\} \\ \Delta\mathsf{cl}(X) = X & \Leftrightarrow & \forall P, Q \in X \; P\Delta Q \in X. \end{array}$$

Now that we have found a structured way to check whether a collection is closed under Δ, we can gather all those collections into

$$\mathsf{CL}(\mathsf{PR}) = \{X \in \wp(\wp(\mathsf{PR})) \mid \Delta\mathsf{cl}(X) = X\}.$$

Opposed to the collections that are Δ-closed, we would also like to study collections that do not contain symmetric differences of any of its sets.

Definition 3 A collection X is called Δ-*independent* if

$$\forall Y \subseteq X(\mathsf{dif}(Y) = \emptyset \Rightarrow Y = \emptyset)$$

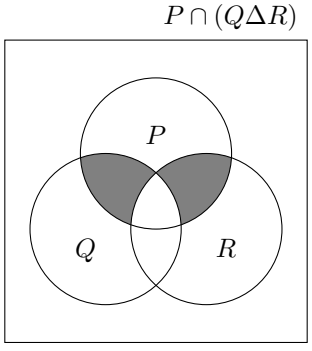
This means that a Δ-independent X does not contain an element that is the dif of a nontrivial subset $Y \subseteq X$, i.e. if $\mathsf{dif}(Y) \in X$ then $Y = \{\mathsf{dif}(Y)\}$. Since the dif represents a linear combination, this property can be used to define the basis of a subspace.

Definition 4 The collection B is called a *basis* of a subspace X if it is a Δ-independent subset of X satisfying $\Delta\mathsf{cl}(B) = X$.

In order to obtain important results in section 3, we need to equip the vector space with an additional structure, namely the operator $\cdot : \wp(\mathsf{PR})^2 \to \mathbb{Z}_2$ defined by $P \cdot Q = \#(P \cap Q) \bmod 2$. This operator is symmetric, since $P \cap Q$ is equal to $Q \cap P$. It also has the property

$$\begin{array}{rcl} P \cdot (Q\Delta R) & = & \#(P \cap (Q\Delta R)) \bmod 2 \\ & = & (\#(P \cap Q) + \#(P \cap R) - 2\#(P \cap Q \cap R)) \bmod 2 \\ & = & (\#P \cap Q) \bmod 2 + (\#P \cap R) \bmod 2 \\ & = & P \cdot Q + P \cdot R \end{array}$$

which can be verified by looking at the following picture:



This property tells us that $\cdot$ is a linear map. Since it was also symmetric, it is linear in both arguments. Therefore we call $\cdot$ a *bilinear form*. When we have $\mathsf{PR} = \{p_1\}$ we can also call it an inner product, but when the number of propositional variables is larger than one this is no longer the case. For these larger vector spaces the operator lacks positive definiteness ($P \cdot P > 0$ for all non-empty P). As a counterexample we can take $P = \{p_1, p_2\}$ and find $P \cdot P = 0$. This is due to the fact that the field $\mathbb{Z}_2$, like all finite fields, has an odd notion of positivity. The only positive element is 1, and the sum of two positive elements equals 0. Therefore we stick to the weaker term "bilinear form". We can use this bilinear form to define orthogonality.

Definition 5 The sets P and Q are *orthogonal* when $P \cdot Q = 0$, i.e. $\#(P \cap Q)$ is even. We denote this by $P \perp Q$.

We can characterize a collection X by listing the sets Q such that Q is orthogonal to every set in X. We call this the *orthogonal complement* $X^\perp$ of X and define it formally by

$$X^\perp = \{Q \mid \forall P \in X \; Q \perp P\}.$$

Note that since a set can be orthogonal to itself, a collection may overlap with its orthogonal complement.

3 Characterizing $\bigwedge[\mathsf{PR}, \leftrightarrow]/\equiv$

Now that we have provided the necessary definitions and notation, we can obtain relevant results concerning the fragments of equivalences and conjunctions of equivalences.

3.1 Equivalences and propositional models

We consider the function eq once more. We concluded in section 2.1 that it was not an isomorphism based on order preservation. However, since then we have introduced the symmetric difference operator Δ acting on the power set of PR. Just like the biconditional, it makes propositional variables cancel out in pairs. We find

$$\mathsf{eq}(P \Delta Q) = \mathsf{eq}(P \cup Q - P \cap Q) \equiv \mathsf{eq}(P \cup Q) \leftrightarrow \mathsf{eq}(P \cap Q) \equiv \mathsf{eq}(P) \leftrightarrow \mathsf{eq}(Q)$$

where the first logical equivalence holds since $P \cap Q$ is a subset of $P \cup Q$ and in this way we preserve the fact that the elements of $P \cap Q$ can be canceled out. The last logical equivalence is just a matter of changing the order of the variables.

Keeping in mind that the function was already bijective, we conclude that by adding the symmetric difference operator we have turned the function eq into an isomorphism.

Now, we take another look at propositional models and how they relate to the vector space with symmetric difference. Subsets P and Q of PR are considered orthogonal when their intersection contains an even number of elements. We find a similar result when P and Q are considered as propositional models.

Lemma 1 Let P and Q be subsets of PR. Then

$$P \models \mathsf{eq}(Q) \quad \text{iff} \quad \#(P \cap Q) \text{ is even.}$$

Proof. To prove the statement, we apply induction over the number of elements of Q. When $\#Q = 0$, we have $Q = \emptyset$. In this case, $\#(P \cap Q)$ is always even, as it is equal to zero. We have $\mathsf{eq}(Q) = \mathsf{eq}(\emptyset) = \top$, so $P \models \mathsf{eq}(Q)$ always holds and we can conclude that the statement is true for $\#Q = 0$.

Now, suppose that the statement holds for sets Q containing k elements. For any Q with $k+1$ elements we can take some $q \in Q$ since it is nonempty. We define $Q' = (Q - \{q\})$ and observe $\#Q' = k$. Hence, we know that the statement is true for Q'. We then have

$$\begin{array}{lll} P \models \mathsf{eq}(Q) & \Leftrightarrow & P \models (q \leftrightarrow \mathsf{eq}(Q')) \\ & \Leftrightarrow & P \models q \quad \text{iff} \quad P \models \mathsf{eq}(Q') \\ & \Leftrightarrow & P \models q \quad \text{iff} \quad \#(P \cap Q') \text{ is even} \\ & \Leftrightarrow & q \notin P \quad \text{iff} \quad \#(P \cap Q') \text{ is even} \\ & \Leftrightarrow & \#(P \cap Q) \text{ is even} \end{array}$$

The last step holds because there are two possible cases. On the one hand we have the case where $\#(P \cap Q')$ is even. Then P does not contain q, which results in the fact that $(P \cap Q) = (P \cap Q')$. On the other hand, there is the case where $\#(P \cap Q')$ is odd. We then have that q is an element of P and thus $(P \cap Q) = (P \cap Q') \cup \{q\}$. The intersection of P and Q has an even amount of elements in both cases.

We conclude that by induction, the statement is true for every subset Q. $\square$

As the structure $\cdot$ on the vector space $\wp(\mathsf{PR})$ is symmetric, it is trivial that we have $P \perp Q$ if and only if $Q \perp P$. The translation of this property into logic is also implied by Lemma 1, since taking $P \cap Q = Q \cap P$ yields the next result.

Corollary 1 Let P and Q be subsets of PR. Then

$$P \models \mathsf{eq}(Q) \quad \text{iff} \quad Q \models \mathsf{eq}(P)$$

Lemma 1 also allows us to obtain a result on the model representation of a conjunction of equivalences. Recall that

Lemma 2 Let X be an element of $\wp(\wp(\mathsf{PR}))$. Then

$$[\![\mathsf{Ceq}(X)]\!] = X^{\perp}$$

Proof. The result follows from Lemma 1 and the definitions of orthogonality and propositional models:

$$\begin{array}{rcl} [\![\mathsf{Ceq}(X)]\!] & = & \{P \mid P \models \mathsf{Ceq}(X)\} \\ & = & \{P \mid P \models \mathsf{eq}(Q)\ \forall Q \in X\} \\ & = & \{P \mid \#(P \cap Q) \text{ is even } \forall Q \in X\} \\ & = & \{P \mid P \perp Q\ \forall Q \in X\} \\ & = & X^{\perp} \end{array}$$

□

Now that we arrive at conjunctions of equivalences again, we will take another look at the function Ceq. In section 2.2 we found that it is not an injection from $\wp(\wp(\mathsf{PR}))$ to the fragment of conjunctions of equivalences modulo $\equiv$. The counterexample shows that $\mathsf{Ceq}\Big(\Big\{\{p_1\},\{p_2\}\Big\}\Big) \equiv \mathsf{Ceq}\Big(\Big\{\{p_1\},\{p_1,p_2\}\Big\}\Big)$. We note that the collections $\Big\{\{p_1\},\{p_2\}\Big\}$ and $\Big\{\{p_1\},\{p_1,p_2\}\Big\}$ have the same Δ-closure, namely $\Big\{\emptyset,\{p_1\},\{p_2\},\{p_1,p_2\}\Big\}$. If we would only consider sets that are itself Δ-closed, this problem would not occur. Therefore, we decide to change the domain to $\mathsf{CL}(\mathsf{PR})$. In order to show that the function is injective when $\mathsf{CL}(\mathsf{PR})$ is the domain, we want to prove that $(X^{\perp})^{\perp} = X$ for Δ-closed X. We will use the concept of bases to obtain this in Lemma 4. First, we have to pave the way with an intermediate result.

Lemma 3

1. Every Δ-closed collection has a basis.
2. If X is Δ-closed, then $\#X = 2^k$ for some k

Proof.

1. Let X be Δ-closed. A basis B of X is obtained by the non-deterministic algorithm

   $B \leftarrow \emptyset$
   while $\Delta\mathsf{cl}(B) \neq X$ **do**
   $P \leftarrow$ some element of $X - \Delta\mathsf{cl}(B)$
   $B \leftarrow B \cup \{P\}$

2. Let B be a basis of X; it suffices to show $\#X = 2^{\#B}$. We have

   $$\begin{array}{rcl} X = \Delta\mathsf{cl}(B) & = & \{\mathsf{dif}(Y) \mid Y \subseteq B\} \\ & = & \{\mathsf{dif}(Y) \mid Y \in \wp(B)\} \end{array}$$

   Similarly to what we discussed in section 2.1, the power set of B contains $2^{\#B}$ different elements Y. Since B is Δ-independent, this results in $2^{\#B}$ different outputs for $\mathsf{dif}(Y)$. We conclude $\#X = 2^{\#B}$.

□

If a basis of X consists of k sets, there must also be at least k variables involved. We would like each set in the basis to contain an exclusive element, so we introduce the concept of a *good* basis.

Definition 6 We call a basis B of X *good* if every $P \in B$ has an *exclusive* element, i.e. an element that distinguishes it from all other elements of B. Let $B^P = \bigcup_{P \in B} (B - \{P\})$, then

$$\forall P \in B \; P - B^P \neq \emptyset$$

This concept will be useful when we interpret the proof of $(X^\perp)^\perp = X$ in our specific vector space. However, this result can be proven in a much more general fashion. We will do so in the next Lemma, after which an example will be given for this general case. Subsequently, the result will be applied to the vector space equipped with symmetric difference.

Lemma 4 Let V be an n-dimensional vector space such that vectors can be represented by n-tuples. Let V be equipped with the dot product acting as a bilinear form. Then, for any linear subspace X of V we have $(X^\perp)^\perp = X$.

Proof. We express the elements of V as row vectors of length n with scalar entries. Every k-dimensional subspace X of V has a basis consisting of k elements, represented by a k-by-n matrix. Gaussian elimination can be performed to create a basis B, which is in reduced row echelon form. We assume here that the first k columns form an identity matrix. If this is not the case, one can swap some columns to obtain such a matrix, then apply the following process and swap the columns back afterwards to get the same result.

We have

$$B = \begin{bmatrix} \mathbf{b_1} \\ \vdots \\ \mathbf{b_k} \end{bmatrix} = \begin{bmatrix} I_k & B_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & \cdots & 0 & b_{1,k+1} & \cdots & b_{1,n} \\ 0 & 1 & \cdots & 0 & b_{2,k+1} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & b_{k,k+1} & \cdots & b_{k,n} \end{bmatrix}$$

We find a set of vectors that are orthogonal to the row vectors of B by defining the $(n-k)$-by-n matrix

$$C = \begin{bmatrix} \mathbf{c_1} \\ \vdots \\ \mathbf{c_{n-k}} \end{bmatrix} = \begin{bmatrix} -B_1^{\mathrm{T}} & I_{n-k} \end{bmatrix} = \begin{bmatrix} -b_{1,k+1} & \cdots & -b_{k,k+1} & 1 & 0 & \cdots & 0 \\ -b_{1,k+2} & \cdots & -b_{k,k+2} & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_{1,n} & \cdots & -b_{k,n} & 0 & 0 & \cdots & 1 \end{bmatrix}$$

since for arbitrary vectors $\mathbf{b_i}$ and $\mathbf{c_j}$ we have

$$\mathbf{b_i} \cdot \mathbf{c_j} = -b_{i,k+j} + b_{i,k+j} = 0.$$

The dot product is a bilinear form, so we have

$$X = \mathsf{span}(B) \subseteq (\mathsf{span}(C))^{\perp} \tag{1}$$

$$\mathsf{span}(C) \subseteq (\mathsf{span}(B))^{\perp} = X^{\perp}. \tag{2}$$

Consider an arbitrary vector $\mathbf{d} = \begin{bmatrix} d_1 & d_2 & \dots & d_n \end{bmatrix} \in X^{\perp}$. Because we have $\mathbf{d} \cdot \mathbf{b_i} = 0$ for $i = 1, \dots, k$ and the left part of B is an identity matrix, we can express the first k elements of $\mathbf{d}$ as follows

$$d_i = -(b_{i,k+1}d_{k+1} + \cdots + b_{i,n}d_n) = -\sum_{j=1}^{n-k} b_{i,k+j}d_{k+j} \qquad \text{for } i = 1, \dots, k$$

We will now check if $\mathbf{d}$ can be expressed as a linear combination of the row vectors of C. Note that the right hand side of C consists of an $n-k$ identity matrix. In order to match the last $n-k$ elements with $\mathbf{d}$ we must take

$$\begin{aligned}
& d_{k+1}\mathbf{c_1} + \dots + d_n\mathbf{c_{n-k}} \\
= \; & \sum_{i=1}^{n-k} d_{k+i} \begin{bmatrix} -b_{1,k+i} & \cdots & -b_{k,k+i} & \mathbf{e_i} \end{bmatrix} \\
= \; & \begin{bmatrix} -\sum_{j=1}^{n-k} b_{1,k+j}d_{k+j} & \cdots & -\sum_{j=1}^{n-k} b_{k,k+j}d_{k+j} & d_{k+1} & \cdots & d_n \end{bmatrix} \\
= \; & \begin{bmatrix} d_1 & \cdots & d_k & d_{k+1} & \cdots & d_n \end{bmatrix} \\
= \; & \mathbf{d}
\end{aligned}$$

where $\mathbf{e_i}$ is the i^{th} row vector of I_{n-k}. Since $\mathbf{d}$ was chosen arbitrarily, we conclude that every element of $X^{\perp}$ is also an element of $\mathsf{span}(C)$, so

$$X^{\perp} \subseteq \mathsf{span}(C). \tag{3}$$

In a similar way, it can be shown that an arbitrary element $\mathbf{a}$ from $(\mathsf{span}(C))^{\perp}$ is in X by taking $a_1\mathbf{b_1} + \cdots + a_k\mathbf{b_k} = \mathbf{a}$. Consequently, we have

$$(\mathsf{span}(C))^{\perp} \subseteq X. \tag{4}$$

Combining equations (1) through (4), we find $X = (\mathsf{span}(C))^{\perp} = (X^{\perp})^{\perp}$. □

In order to clear up the process, we will discuss an example which is set in a 4-dimensional vector space over the field of real numbers $\mathbb{R}$.

Example The vectors [2 4 6 4] and [3 6 9 1] form a basis for a subspace X. If we put them in a matrix and apply Gaussian elimination, we obtain

$$B = \begin{bmatrix} 1 & 2 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

We now swap the second and last column, so that we have a matrix of the desired form. We call it B' and let C' be the matrix with orthogonal row vectors:

$$B' = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 0 & 1 & 0 & 0 \end{bmatrix} \text{ and } C' = \begin{bmatrix} -3 & 0 & 1 & 0 \\ -2 & 0 & 0 & 1 \end{bmatrix}.$$

By swapping the columns back we define

$$C = \begin{bmatrix} -3 & 0 & 1 & 0 \\ -2 & 1 & 0 & 0 \end{bmatrix}.$$

By computing the dot products, one can check that the vectors of C are orthogonal to the vectors of B. This means that equation (1) and (2) are satisfied. Also, for any vector $\mathbf{d}$ in the orthogonal complement of X, we have $\mathbf{d} \cdot \mathbf{b_1} = d_1 + 2d_2 + 3d_3 = 0$ and $\mathbf{d} \cdot \mathbf{b_2} = d_4 = 0$. Therefore, d_1 can be expressed as $-2d_2 - 3d_3$. We observe that $\mathbf{d}$ is a linear combination of the vectors of C by taking

$$d_3\mathbf{c_1} + d_2\mathbf{c_2} = \begin{bmatrix} -2d_2 - 3d_3 & d_2 & d_3 & 0 \end{bmatrix} = \begin{bmatrix} d_1 & d_2 & d_3 & d_4 \end{bmatrix} = \mathbf{d}.$$

In turn, any vector $\mathbf{a}$ in the orthogonal complement of $\mathsf{span}(C)$ has the properties $a_3 = 3a_1$ and $a_2 = 2a_1$. We take

$$a_1\mathbf{b_1} + a_4\mathbf{b_2} = \begin{bmatrix} a_1 & 2a_1 & 3a_1 & a_4 \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \end{bmatrix} = \mathbf{a}.$$

Now that we have provided clear reasoning for this result, a correct interpretation can be given for the vector space with symmetric difference such that it fits the necessary conditions.

Corollary 2 Let the vector space $\wp(\mathsf{PR})$ over $\mathbb{Z}_2$ be equipped with the symmetric difference operator Δ and the bilinear form $\cdot$ given by $P \cdot Q = \#(P \cap Q) \bmod 2$. Then, for any linear subspace X it holds that $(X^\perp)^\perp = X$

Proof. The elements of the vector space can be denoted by n-tuples with binary entries. Here, a zero at the i^{th} entry represents the absence of p_i in the set, whereas a one represents the presence of p_i. For example, for $n = 3$, we have the sets $\{p_1, p_3\}$ and $\{p_2, p_3\}$ which translate to the vectors $\begin{bmatrix} 1 & 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 & 1 \end{bmatrix}$, respectively.

Consider the arbitrary vectors $\mathbf{a}, \mathbf{b} \in \wp(\mathsf{PR})$ represented by the n-tuples $\begin{bmatrix} a_1 & \dots & a_n \end{bmatrix}$ and $\begin{bmatrix} b_1 & \dots & b_n \end{bmatrix}$. Recall the addition and multiplication tables from section 2.3. The vector $\mathbf{a} + \mathbf{b} = \begin{bmatrix} a_1 + b_1 & \dots & a_n + b_n \end{bmatrix}$ has the following property:

$$(\mathbf{a} + \mathbf{b})_i = a_i + b_i = \begin{cases} 0 & \text{if } a_i = b_i \\ 1 & \text{if } a_i \neq b_i. \end{cases}$$

This means that p_i is an element of $\mathbf{a}\Delta\mathbf{b}$ exactly when it is either in $\mathbf{a}$ or $\mathbf{b}$, but not in both. This is in accordance with the symmetric difference operator.

The dot product of the vectors is given by $\mathbf{a} \cdot \mathbf{b} = \sum_{i=1}^{n} a_i b_i$.We know that the scalar product $a_i b_i$ only equals 1 if both a_i and b_i are 1, i.e. if p_i is an element of both sets. Hence, the dot product sums $\#(\mathbf{a} \cap \mathbf{b})$ ones and the remaining terms are zero. Since the dot product maps to the field $\mathbb{Z}_2$, we are using addition modulo 2, so the dot product is equivalent to the bilinear form we introduced: $\sum_{i=1}^{n} a_i b_i = \#(\mathbf{a} \cap \mathbf{b}) \bmod 2$. This shows that our interpretation works. □

If we follow the proof of Lemma 4 with the new interpretation in mind, we observe how to obtain a basis of $X^{\perp}$ in our specific vector space. We will clarify the process with an example.

For $n = 6$, we consider the collection $\Big\{\{p_1, p_3, p_5, p_6\}, \{p_3, p_5\}, \{p_4, p_6\}\Big\}$, which form a basis for a subspace X. It is not a good basis, since the set $\{p_3, p_5\}$ does not contain an exclusive element. We transform it into a good basis by replacing the first set with the symmetric difference of the first two sets. So, we have the good basis $B = \Big\{P_1, P_2, P_3\Big\} = \Big\{\{p_1, p_6\}, \{p_3, p_5\}, \{p_4, p_6\}\Big\}$. We say that p_1, p_3 and p_4 are the *exclusive* elements, and we call p_2, p_5 and p_6 the *other* elements (note that p_5 could also have been picked as an exclusive element, but we restrict ourselves to one exclusive element per set). A basis C for the orthogonal complement of X can now be constructed by setting $C = \Big\{Q_{p_2}, Q_{p_5}, Q_{p_6}\Big\}$, where Q_{p_i} consists of the element p_i and the exclusive elements of the sets in B that contain p_i. So in our example we have $C = \Big\{Q_{p_2}, Q_{p_5}, Q_{p_6}\Big\} = \Big\{\{p_2\}, \{p_3, p_5\}, \{p_1, p_4, p_6\}\Big\}$.

The lemmas that we have obtained so far contain a lot of information about the vector space $\wp(\mathsf{PR})$ equipped with Δ and its connection with the logical fragments. They also provide us with the necessary properties to prove that the function Ceq is an isomorphism, which contributes greatly in characterizing the fragments of conjunctions of equivalences.

3.2 An isomorphism with $\mathsf{CL}(\mathsf{PR})$ and determining the size

Theorem 1 $\mathsf{CL}(\mathsf{PR})$ is isomorphic to $\bigwedge[\mathsf{PR}, \leftrightarrow]/\equiv$

Proof. This requires that we show three properties of the restriction of Ceq to $\mathsf{CL}(\mathsf{PR})$:

1. injectivity: if $X, Y \in \mathsf{CL}(\mathsf{PR})$ and $\mathsf{Ceq}(X) \equiv \mathsf{Ceq}(Y)$ then $X = Y$;
2. surjectivity: for every $X \subseteq \wp(\mathsf{PR})$ there is a $Y \in \mathsf{CL}(\mathsf{PR})$ with $\mathsf{Ceq}(X) \equiv \mathsf{Ceq}(Y)$;
3. order preservation: if $X, Y \in \mathsf{CL}(\mathsf{PR})$ and $X \subseteq Y$ then $\mathsf{Ceq}(Y) \models \mathsf{Ceq}(X)$.

The reasoning for (1) is as follows: if $\mathsf{Ceq}(X) \equiv \mathsf{Ceq}(Y)$ then

$$X = (X^{\perp})^{\perp} = [\![\mathsf{Ceq}(X)]\!]^{\perp} = [\![\mathsf{Ceq}(Y)]\!]^{\perp} = (Y^{\perp})^{\perp} = Y$$

where the first equation holds due to Corollary 2 and the second equation due to Lemma 2.

For (2), we take $Y = \Delta\mathsf{cl}(X)$ and use

$$[\![\mathsf{Ceq}(X)]\!] = X^\perp = (\Delta\mathsf{cl}(X))^\perp = Y^\perp = [\![\mathsf{Ceq}(Y)]\!]$$

where the second equation holds due to the linearity of $\cdot$. Since $\mathsf{Ceq}(X)$ and $\mathsf{Ceq}(Y)$ are true for the exact same collection of models, we conclude that they are logically equivalent.

Finally, for (3) we reason that if X is a subset of Y, then for all P we have

$$\begin{array}{lcll} P \models \mathsf{Ceq}(Y) & \Leftrightarrow & P \models \mathsf{eq}(Q) & \forall Q \in Y \\ & \Rightarrow & P \models \mathsf{eq}(Q) & \forall Q \in X \\ & \Leftrightarrow & P \models \mathsf{Ceq}(X) & \end{array}$$

□

Now that we have established the fact there is a duality, we can consider the amount of different conjunctions of equivalences by looking at $\#\mathsf{CL}(\mathsf{PR})$. Recall from Lemma 3 that a Δ-closed X has 2^k elements, where k is the number of elements of the bases of X. If we can find an expression for the number of subspaces X with $\#X = 2^k$ for arbitrary k, we can take the sum over all values of k to find $\#\mathsf{CL}(\mathsf{PR})$ and therefore the number of different conjunctions of equivalences.

We define

$$\begin{array}{lcl} \mathsf{D}(n) & = & \mathsf{CL}(\{p_1, \ldots, p_n\}) \\ \mathsf{D}(n,k) & = & \{X \in \mathsf{D}(n) \mid \#X = 2^k\} \end{array}$$

The *Gaussian binomial coefficients* are given by

$$\binom{n}{k}_q = \prod_{i=0}^{k-1} \frac{q^{n-i} - 1}{q^{i+1} - 1}$$

for $0 < k \leq n$ and $\binom{n}{0}_q = 1$ (by [4][3]). In the following paragraph we will show that $\#D(n,k)$ is equal to the Gaussian binomial coefficient with $q = 2$. This proof is based on [2].

Since every X in $\mathsf{D}(n,k)$ has a basis (Lemma 3), we can count the elements of $\mathsf{D}(n,k)$ by considering bases. We will count how many different bases with k elements exist in the vector space $wp(\mathsf{PR})$ and then divide by the number of different bases for a given collection X with 2^k elements. For the special case $k = 0$, there is exactly one element, which is its own basis. We have $\#\mathsf{D}(n,0) = \#\{\{\emptyset\}\} = 1$. For $k > 0$, a basis can be constructed using the algorithm from the proof of Lemma 3. In the vector space $\wp(\mathsf{PR})$, we obtain a basis

$B = \{P_1, \ldots, P_k\}$, where P_i is the i^{th} element that is added. The number of choices

- for P_1 is $2^n - 1$ (any element except $\emptyset$),
- for P_2 is $2^n - 2$ (any element except those of $\Delta\mathsf{cl}(\{P_1\})$),
  $\vdots$
- for P_k is $2^n - 2^{k-1}$ (any element except those of $\Delta\mathsf{cl}(\{P_1, \ldots, P_{k-1}\})$).

Consequently, the number of different bases with k elements in the n-dimensional vector space is

$$(2^n - 1)(2^n - 2) \cdots (2^n - 2^{k-1})$$

In order to find the amount of different bases for a given subspace X, we apply the same process, with k instead of n. This means that the number of elements of $\mathsf{D}(n, k)$ is given by

$$\#\mathsf{D}(n,k) = \frac{(2^n - 1)(2^n - 2) \cdots (2^n - 2^{k-1})}{(2^k - 1)(2^k - 2) \cdots (2^k - 2^{k-1})}$$

We divide both the numerator and the denominator by $(2^1)(2^2) \cdots (2^{k-1})$ and find that for $0 < k \leq n$

$$\begin{aligned} \#\mathsf{D}(n,k) &= \frac{(2^n - 1)(2^{n-1} - 1) \cdots (2^{n-k+1} - 1)}{(2^k - 1)(2^{k-1} - 1) \cdots (2^1 - 1)} \\ &= \prod_{i=0}^{k-1} \frac{2^{n-i} - 1}{2^{i+1} - 1} \end{aligned}$$

We can conclude that for all k, we have

$$\#\mathsf{D}(n,k) = \binom{n}{k}_2$$

and thus the total number of subspaces is given by

$$\#\mathsf{D}(n) = \sum_{k=0}^{n} \binom{n}{k}_2$$

which also represents the number of different conjunctions of equivalences for a given number of propositional variables n. Some values of $\#\mathsf{D}(n,k)$ and $\#\mathsf{D}(n)$

are given by

$n=0$	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$	$n=7$	
1	1	1	1	1	1	1	1	$k=0$
	1	3	7	15	31	63	127	$k=1$
		1	7	35	155	651	2667	$k=2$
			1	15	155	1395	11811	$k=3$
				1	31	651	11811	$k=4$
					1	63	2667	$k=5$
						1	127	$k=6$
							1	$k=7$
1	2	5	16	67	374	2825	29212	$\sum_k$

The bottom sequence is listed in the Online Encyclopedia of Integer Sequences as entry A006116.

4 Introducing logical contradiction as an atom

The concept of negation appears very often in logic. But since we are interested in conjunctions of equivalences, we cannot simply add the logical connective $\neg$ to our fragment. However, the same effect can be created by considering the logical contradiction (falsum) as a propositional atom. In the introduction we denoted it by its usual symbol $\bot$, but we have already used this notation extensively in the last section, where it represented orthogonality. Instead, we will now denote falsum by the lower case f, as it is a propositional atom which always has truth value F.

An equivalence containing falsum has the following property:

$$\varphi \leftrightarrow f \;\equiv\; \neg\varphi.$$

where $\neg\varphi$ is the negation of φ. Its truth value can be derived from the truth table

φ	$\neg\varphi$
T	F
F	T

Note that we do not introduce the negation operator to our fragments, but we create the possibility to obtain the same logical content by adding f. For a given set P, we know that $\mathsf{eq}(P)$ is true if and only if an even amount of elements of P is false. The set $P \cup \{f\}$ translates to the negation of $\mathsf{eq}(P)$, as

$$\mathsf{eq}(P \cup \{f\}) = \mathsf{eq}(P) \leftrightarrow f \equiv \neg\mathsf{eq}(P).$$

This equivalence is true if and only if an odd amount of elements of P is false.

We will study the fragment $[\mathsf{PR} \cup \{f\}, \leftrightarrow]$ of equivalences. We start by checking if the function eq is still bijective. Surjectivity holds from the definition of the fragment, but injectivity needs some verification. It is easy to check that $\mathsf{eq}(P \cup \{f\})$ is not logically equivalent to any element of $[\mathsf{PR}, \leftrightarrow]$. Namely, if we assign the truth value T to all propositional variables in PR, the number of false elements in P is zero and therefore even. This means that $\mathsf{eq}(P \cup \{f\})$ is false, while $\mathsf{eq}(Q)$ is true for all Q in $\wp(\mathsf{PR})$ due to the absence of false propositional variables.

Now suppose that $\mathsf{eq}(P \cup \{f\})$ is logically equivalent to some $\mathsf{eq}(Q \cup \{f\})$. Then, we have

$$\begin{array}{rcl} \mathsf{eq}(P \cup \{f\}) \equiv \mathsf{eq}(Q \cup \{f\}) & \Rightarrow & \neg\mathsf{eq}(P) \equiv \neg\mathsf{eq}(Q) \\ & \Rightarrow & \mathsf{eq}(P) \equiv \mathsf{eq}(Q) \\ & \Rightarrow & P = Q \end{array}$$

From this we can conclude that the function is indeed injective.

Moving on to the fragment $\bigwedge[\mathsf{PR} \cup \{f\}, \leftrightarrow]/\equiv$, we observe that a conjunction of equivalences that contains the single element f as an equivalence will always get truth value F. We would like to discover a similar duality to what we found before, but this seems to be an obstacle. It is illustrated by the subspaces $X = \{\emptyset, \{p_1\}, \{f\}, \{p_1, f\}\}$ and $Y = \{\emptyset, \{p_2\}, \{f\}, \{p_2, f\}\}$, for which the counterparts are logically equivalent:

$$\mathsf{Ceq}(X) = \top \wedge p_1 \wedge f \wedge (p_1 \leftrightarrow f) \equiv f \equiv \top \wedge p_2 \wedge f \wedge (p_2 \leftrightarrow f) = \mathsf{Ceq}(Y)$$

We avoid this problem by leaving every collection X such that $\{f\} \in X$ out of consideration, except for $\wp(\mathsf{PR} \cup \{f\})$. We keep the latter collection so that there is exactly one subspace X that maps to falsum. Note that by removing the other subspaces that contain the singleton $\{f\}$, we automatically remove self-contradicting collections. Namely, if X contains an arbitrary P (translating to $\mathsf{eq}(P)$) and the set $P \cup \{f\}$ (translating to $\neg\mathsf{eq}(P)$), then by Δ-closedness we must have $P\Delta(P \cup \{f\}) = \{f\}$ in X.

We define the set $\mathsf{DN}(n)$ as

$$\mathsf{DN}(n) = \left\{ X \in \mathsf{CL}(\{f, p_1, \ldots, p_n\}) \mid \{f\} \notin X \right\} \cup \left\{ \wp(\{f, p_1, \ldots, p_n\}) \right\}$$

Now that falsum is added as a propositional atom, there is a condition for propositional models. Recall that a model P makes all its elements false and the remaining elements true. Since f is by definition false, it must be contained in every model. Because of this, we do not have $X^\perp = [\![\mathsf{Ceq}(X)]\!]$ anymore. Since this was a vital part of the injectivity proof for Theorem 1, we have to make an adjustment in order to derive an isomorphism. Note that the collection $[\![\mathsf{Ceq}(X)]\!]$ is now given by all sets in $X^\perp$ that contain f.

As a step in fixing the injectivity proof for the isomorphism, we make another statement about a general n-dimensional vector space and its subspaces. After this, we can apply the result to the vector space based on symmetric difference.

Lemma 5 Let V be an n-dimensional vector space such that vectors can be represented by n-tuples. Let V be equipped with the dot product acting as a bilinear form. Furthermore, let the collection $M \subseteq V$ be given by $M = \left\{ \begin{bmatrix} a_1 & \cdots & a_n \end{bmatrix} \mid a_1 \neq 0 \right\}$. If X is a linear subspace of V such that $\begin{bmatrix} a_1 & 0 & \cdots & 0 \end{bmatrix} \notin X$ for nonzero a_1, then we can find a basis D of $X^\perp$ such that $D \subseteq M$.

Proof. Take a basis B of X in reduced row echelon form. Without loss of generality, we can assume that B is of the form $\begin{bmatrix} I_k & B_1 \end{bmatrix}$. The first row vector of B is given by

$$\mathbf{b_1} = \begin{bmatrix} 1 & 0 & \cdots & 0 & b_{1,k+1} & \cdots & b_{1,n} \end{bmatrix}.$$

Because of our condition on X, we know that there is a j such that $b_{1,k+j} \neq 0$. Now, if we create a basis C of $X^\perp$ according to the proof of Lemma 4, the j^{th} row vector of C is given by

$$\mathbf{c_j} = \begin{bmatrix} -b_{1,k+j} & \cdots & -b_{k,k+j} & \mathbf{e_j} \end{bmatrix}$$

where $\mathbf{e_j}$ is the j^{th} row vector of I_{n-k}. We know that the first element of $\mathbf{c_j}$ is nonzero, so $\mathbf{c_j}$ is an element of M.

We define the matrix D by

$$D = \begin{bmatrix} \mathbf{d_1} \\ \vdots \\ \mathbf{d_{n-k}} \end{bmatrix} \qquad \text{with } \mathbf{d_i} = \begin{cases} \mathbf{c_i} & \text{if } \mathbf{c_i} \in M \\ \mathbf{c_i} + \mathbf{c_j} & \text{if } \mathbf{c_i} \notin M. \end{cases}$$

This definition provides certain properties. Firstly, every vector of D has a nonzero first element, so D is a subset of M. Also, we notice that the vectors of D are linear combinations of the vectors of C in such a way that they are linearly independent. Namely, we have n vectors such that every vector of C is a linear combination. From this we can conclude that $\mathsf{span}(D) = \mathsf{span}(C)$, so D is also a basis of $X^\perp$. □

We can use Lemma 5 in our specific case by letting the first entry of the vector be an indicator function for the presence of falsum.

Corollary 3 Let the vector space $\wp(\{f, p_1, \ldots, p_n\})$ over $\mathbb{Z}_2$ be equipped with the symmetric difference operator Δ and the bilinear form $\cdot$ given by $P \cdot Q = \#(P \cap Q) \bmod 2$. Furthermore, let the collection $M \subseteq \wp(\{f, p_1, \ldots, p_n\})$ be given by $M = \{P \in \wp(\{f, p_1, \ldots, p_n\}) \mid f \in P\}$. If X is a linear subspace such that $\{f\} \notin X$, then

1. We can find a basis D of $X^\perp$ such that $D \subseteq M$.

2. $(X^\perp \cap M)^\perp = X$.

Proof. 1. We again interpret the vectors as n-tuples. In this case, the first entry indicates the presence of f in the set and the $(i+1)^{\text{th}}$ entry indicates the presence of p_i in the set. By Lemma 5 we can find a basis D of $X^\perp$ such that every set in D contains falsum, so $D \subseteq M$.

2. We have $D \subseteq (X^\perp \cap M) \subseteq X^\perp = \Delta\mathsf{cl}(D)$. Since $X^\perp$ is itself closed under Δ, we know that $\Delta\mathsf{cl}(X^\perp \cap M) = X^\perp$. Then, by linearity of $\cdot$, we can conclude that $(X^\perp \cap M)^\perp = (X^\perp)^\perp = X$.

□

The second statement of the corollary turns out to be the missing link to prove our final isomorphism.

Theorem 2 $\mathsf{DN}(n)$ is isomorphic to $\bigwedge[\{f, p_1, \ldots, p_n\}, \leftrightarrow]/\equiv$

Proof. We again need the properties injectivity, surjectivity and order preservation. The latter can be proven in the exact same way as for Theorem 1. The proof for injectivity is similar to that of the previous theorem, but with a small adjustment. If $X, Y \in \mathsf{DN}(n)$ and $\mathsf{Ceq}(X) \equiv \mathsf{Ceq}(Y)$, then we have

$$X = (X^\perp \cap M)^\perp = [\![\mathsf{Ceq}(X)]\!]^\perp = [\![\mathsf{Ceq}(Y)]\!]^\perp = (Y^\perp \cap M)^\perp = Y.$$

Finally, the proof for surjectivity is given as follows. There are two cases. For every $X \subseteq \wp(\{f, p_1, \ldots, p_n\})$ such that $\{f\} \notin \Delta\mathsf{cl}(X)$ we have $Y = \Delta\mathsf{cl}(X) \in \mathsf{DN}(n)$ such that

$$[\![\mathsf{Ceq}(X)]\!] = X^\perp \cap M = (\Delta\mathsf{cl}(X))^\perp \cap M = Y^\perp \cap M = [\![\mathsf{Ceq}(Y)]\!]$$

and for every $X \subseteq \wp(\{f, p_1, \ldots, p_n\})$ such that $\{f\} \in \Delta\mathsf{cl}(X)$ we have $Y = \wp(\{f, p_1, \ldots, p_n\}) \in \mathsf{DN}(n)$ such that

$$[\![\mathsf{Ceq}(X)]\!] = \emptyset = [\![\mathsf{Ceq}(Y)]\!].$$

In both cases we find $[\![\mathsf{Ceq}(X)]\!] = [\![\mathsf{Ceq}(Y)]\!]$ and thus $\mathsf{Ceq}(X) \equiv \mathsf{Ceq}(Y)$. □

4.1 Determining the size of $\bigwedge[\{f, p_1, \ldots, p_n\}, \leftrightarrow]/\equiv$

Finally, we can count $\#\bigwedge[\{f, p_1, \ldots, p_n\}, \leftrightarrow]/\equiv$ by counting the number of subspaces in $\mathsf{DN}(n)$. Recall the definition of $\mathsf{DN}(n)$:

$$\mathsf{DN}(n) = \left\{ X \in \mathsf{CL}(\{f, p_1, \ldots, p_n\}) \mid \{f\} \notin X \right\} \cup \left\{ \wp(\{f, p_1, \ldots, p_n\}) \right\}.$$

We can calculate $\#\mathsf{DN}(n)$ by taking $\#\mathsf{CL}(\{f, p_1, \ldots, p_n\})$, subtracting $\#\{X \in \mathsf{CL}(\{f, p_1, \ldots, p_n\}) \mid \{f\} \in X\}$ and adding 1 (since we let $\wp(\{f, p_1, \ldots, p_n\})$ be contained in $\mathsf{DN}(n)$). We note that in the vector space $\wp(\{f, p_1, \ldots, p_n\})$, falsum does not have any special properties and can therefore be regarded as the $n{+}1^{\text{th}}$ atomic element. Therefore we can say $\#\mathsf{CL}(\{f, p_1, \ldots, p_n\}) = \#\mathsf{D}(n)$.

For every subspace $X \in \mathsf{CL}(\{f, p_1, \ldots, p_n\})$ that contains the singleton $\{f\}$ we can obtain a basis $B = \Big\{\{f\}, P_1, \ldots, P_n\Big\}$ with $f \notin P_i$ for all $i = 1, \ldots, n$ by the algorithm

$B \leftarrow \{\{f\}\}$
while $\Delta\mathsf{cl}(B) \neq X$ **do**
    $P \leftarrow$ some element of $X - \Delta\mathsf{cl}(B)$ that does not contain f
    $B \leftarrow B \cup \{P\}$

From this basis we can remove the singleton $\{f\}$. The collection $B - \{\{f\}\}$ is a basis for a subspace $Y \in \mathsf{D}(n)$ (where falsum is not a propositional atom). In turn, we can also take any subspace $Y \in \mathsf{D}(n)$, add the singleton $\{f\}$ and then take the Δ-closure, resulting in a subspace $X \in \mathsf{CL}(\{f, p_1, \ldots, p_n\})$. That is, $\Delta\mathsf{cl}(Y \cup \{\{f\}\}) = X \in \mathsf{CL}(\{f, p_1, \ldots, p_n\})$. We note that for every $Y \in \mathsf{D}(n)$ this results in a different subspace X, so the number of subspaces X that contain the singleton $\{f\}$ is given by $\#\mathsf{D}(n)$.

This means that the calculation for $\#\mathsf{DN}(n)$ boils down to

$$\#\mathsf{DN}(n) = \#\mathsf{D}(n+1) - \#\mathsf{D}(n) + 1.$$

Some values for $\#\mathsf{DN}(n)$ and therefore for $\#\bigwedge[\{f, p_1, \ldots, p_n\}, \leftrightarrow]/\equiv$ are given by

	$n=0$	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$
$\#\mathsf{DN}(n) =$	2	4	12	52	308	2452	26388.

This is not a known sequence according to the Online Encyclopedia of Integer Sequences, so it could perhaps be added as a result of this report.

5 Conclusion

We have studied the fragments of equivalences and conjunctions of equivalences in classical propositional logic. We have discussed some of the properties of the propositional formulae themselves, but the most remarkable results were obtained by finding dualities by means of linear algebra. There is a one-to-one connection between the fragment of equivalences and a vector space over the 2-element field equipped with the symmetric difference operator. Also, there is an isomorphism between the fragment of conjunctions of equivalences and the set of subspaces of such a vector space. As a result of this, the number of different conjunctions of equivalences could be calculated. It is given by the sum of the Gaussian binomial coefficients with $q = 2$ and can be found as the entry A006116 of the Online Encyclopedia of Integer Sequences.

Finally, when the logical contradiction falsum is added as a propositional atom, we find another isomorphism. The fragment of conjunctions of equivalences then has a direct connection with a particular set of subspaces. We have determined the size of this fragment, namely in the case of $n = 0, 1, 2, 3, 4, 5, 6, \ldots$ propositional variables it is given by the sequence 2, 4, 12, 52, 308, 2452, 26388, ...

References

[1] J. Alama. "The Vector Space of Subsets of a Set Based on Symmetric Difference." In: *Formalized Mathematics* 16.1 (2008), pp. 1–5. DOI: https://doi.org/10.2478/v10037-008-0001-7.

[2] P.J. Cameron. *MT5821 Advanced Combinatorics course module, chapter 6*. University of St. Andrews. 2014. URL: http://www-groups.mcs.st-andrews.ac.uk/~pjc/Teaching/MT5821/1/l6.pdf.

[3] G. Critzer. "Combinatorics of Vector Spaces over Finite Fields". MA thesis. Emporia State university, 2018.

[4] K.E. Morrison. "Integer Sequences and Matrices over Finite Fields". In: *Journal of Integer Sequences* 9.2 (2006), pp. 1–28. URL: https://cs.uwaterloo.ca/journals/JIS/VOL9/Morrison/morrison37.pdf.

[5] G.R. Renardel de Lavalette. *Conjunctions of equivalences: logic meets linear algebra*. University of Groningen. 2018.