Boolean Algebra Cheatsheet 3

3.1 Definitions

- * Boolean function is a function of the form $f: \mathbb{B}^n \to \mathbb{B}$, where $n \ge 0$ is the arity of the function and $\mathbb{B} = \{0, 1\} = \{\bot, \top\} = \{F, T\}$ is a Boolean domain.
- * There are multiple ways to represent a Boolean function (all examples represent the same function):
 - 1. Truth table, *e.g.*, f = (1010), where LSB corresponds to 1, MSB to 0.

Least/Most Significant Bit

2. Analytically (as a sentence of propositional logic), e.g., $f(A, B) = \neg B$.

Propositional logic

3. Sum of minterms, e.g., $f = \sum m(0, 2) = m_0 + m_2$.

Minterms

4. Product of maxterms, e.g., $f = \prod M(1,3) = M_1 \cdot M_3$.

Maxterms

5. Boolean function number e , e.g., $f_{10}^{(2)}$ is the 10-th 2-ary function. Note that Wolfram's "Boolean operator number" is a slightly different term, which uses the reversed truth table. 10-th Boolean function $f_{10}^{(2)}$ with the truth table (1010) can be obtained via the query "5th Boolean function of 2 variables" (note: not 10th!) in WolframAlpha^[2], since $rev(1010_2) = 0101_2 = 5_{10}$.

3.2 Normal Forms

- * Disjunctive forms:
 - **Cube** is a conjunction of literals: $\mathcal{T} = \bigwedge_i \mathcal{L}_i$.
 - Formula is in **disjunctive normal form (DNF)** if it is a disjunction of terms: DNF = $\bigvee_i \mathcal{T}_{i}$.
 - **Minterm** is conjunction of literals, where *each* variable appears *once*, *e.g.*, $m_6 = (A \land B \land \neg C)$.
 - Formula is in **canonical DNF (CDNF)** if it is a disjunction of minterms: CDNF = $\bigvee_i m_i$.
- * Conjunctive forms:
 - Clause $^{\mathbb{Z}}$ is a disjunction of literals: $C = \bigvee_i \mathcal{L}_i$
 - Formula is in **conjunctive normal form** (CNF) $^{\text{LC}}$ if it is a conjunction of clauses: CNF = $\bigwedge_i C_i$.
 - **Maxterm** is disjunction of literals, where *each* variable appears *once*, *e.g.*, $M_6 = (\neg A \lor \neg B \lor C)$.
 - Formula is in **canonical CNF** (CCNF) if it is a conjunction of maxterms: CCNF = $\bigwedge_i M_i$.
- * Some other normal forms:
 - Formula is in **negation normal form (NNF)** if the negation operator (\neg) is only applied to variables and the only other allowed Boolean operators are conjunction (\wedge) and disjunction (\vee).
 - Formula f is in **Blake canonical form (BCF)** if it is a disjunction of all the prime implicants of f.
 - Formula is in **prenex normal form (PNF)** if it consists of *prefix* quantifiers and bound variables, and *matrix* quatifier-free part.
 - ∘ Formula is in **Skolem normal form (SNF)** if it is in prenex normal form with only universal first-order quantifiers.
 - **Zhegalkin polynomial** is a formula in the following form (**algebraic normal form (ANF)**):

•
$$f(X_1, \ldots, X_n) = a_0 \bigoplus_{\substack{1 \le i_1 \le \cdots \le i_k \le n \\ 1 \le k \le n}} (a_{i_1, \ldots, i_k} \wedge X_{i_1} \wedge \cdots \wedge X_{i_k})$$
, where $a_0, a_{i_1, \ldots, i_k} \in \mathbb{B}$

• $f(x_1,\ldots,x_n)=a_0\oplus (a_1x_1\oplus\cdots\oplus a_nx_n)\oplus (a_{1,2}x_1x_2\oplus\cdots\oplus a_{n-1,n}x_{n-1}x_n)\oplus\cdots\oplus a_{1,\ldots,n}x_1\ldots x_n$

3.3 Conversion to CNF/DNF

In order to convert arbitrary (i.e. any) Boolean formula to equivalent CNF/DNF:

1. Eliminate equivalences, implications and other "non-standard" operations (i.e. rewrite using only $\{\land,\lor,\neg\}$):

$$\begin{array}{ccc} \mathcal{A} \leftrightarrow \mathcal{B} & \leadsto & (\mathcal{A} \rightarrow \mathcal{B}) \land (\mathcal{B} \rightarrow \mathcal{A}) \\ \mathcal{A} \rightarrow \mathcal{B} & \leadsto & \neg \mathcal{A} \lor \mathcal{B} \\ \end{array}$$

2. Push negation downwards:

$$\neg (\mathcal{A} \lor \mathcal{B}) \rightsquigarrow \neg \mathcal{A} \land \neg \mathcal{B}$$
$$\neg (\mathcal{A} \land \mathcal{B}) \rightsquigarrow \neg \mathcal{A} \lor \neg \mathcal{B}$$

3. Eliminate double negation:

$$\neg\neg\mathcal{A} \rightsquigarrow \mathcal{A}$$

Note that after the recursive application of 1–3 the formula is in NNF.

4. Push disjunction (for CNF) / conjunction (for DNF) downward:

$$(\mathcal{A} \land \mathcal{B}) \lor C \rightsquigarrow_{\mathsf{CNF}} (\mathcal{A} \lor C) \land (\mathcal{B} \lor C)$$
$$(\mathcal{A} \lor \mathcal{B}) \land C \rightsquigarrow_{\mathsf{DNF}} (\mathcal{A} \land C) \lor (\mathcal{B} \land C)$$

5. Eliminate \top and \bot :

3.4 Functional Completeness[™]

- * A set *S* is called **closed** under some operation "•" if the result of the operation applied to any elements in the set is also contained in this set, *i.e.* $\forall x, y \in S : (x \cdot y) \in S$.
- * The **closure** S^* of a set S is the minimal *closed* superset of S.

Closure

* A set of Boolean functions F is called **functionally complete** if it can be used to express all possible Boolean functions. Formally, $F^* = \mathbb{F}$, where F^* is a *functional closure* of F, and $\mathbb{F} = \bigcup_{n \in \mathbb{N}} \{ f : \mathbb{B}^n \to \mathbb{B} \}$.

Post's Functional Completeness Theorem $^{\mbox{\sc e}}$. A set of Boolean functions F is functionally complete iff it contains:

- at least one function that does *not* preserve zero, *i.e.* $\exists f \in F : f \notin T_0$, and
- at least one function that does *not* preserve one, *i.e.* $\exists f \in F : f \notin T_1$, and
- at least one function that is *not* self-dual, *i.e.* $\exists f \in F : f \notin S$, and
- at least one function that is *not* monotonic, *i.e.* $\exists f \in F : f \notin M$, and
- at least one function that is *not* linear function, *i.e.* $\exists f \in F : f \notin L$.
- * A function f is $\mathbf{zero\text{-}preserving}^{\mathbf{L}}$ iff it is False on the zero-valuation $(\mathbb{0}=(0,0,\ldots,0))$:

$$f \in T_0 \leftrightarrow f(\mathbb{O}) = 0$$

* A function f is **one-preserving** iff it is True on the one-valuation ($\mathbb{1} = (1, 1, ..., 1)$):

```
f \in T_1 \leftrightarrow f(1) = 1
```

* A function f is **self-dual** $^{\mbox{\'e}}$ iff it is dual to itself:

$$f \in S \leftrightarrow \forall x_1, \dots, x_n \in \mathbb{B} : f(x_1, \dots, x_n) = \overline{f}(\overline{x}_1, \dots, \overline{x}_n).$$

* A function f is **monotonic** iff for every increasing valuations, the function does not decrease:

$$f \in M \leftrightarrow \forall a, b \in \mathbb{B}^n : a \leq b \rightarrow f(a) \leq f(b).$$

Comparison of valuations $a, b \in \mathbb{B}^n$ is defined as follows:

$$a \preceq b \leftrightarrow \bigwedge_{1 \leq i \leq n} (a_i \leq b_i)$$

* A function *f* is **linear** iff its Zhegalkin polynomial is linear (*i.e.* has a degree at most 1):

$$f \in L \leftrightarrow \deg f_{\oplus} \le 1$$