Mathematics and Computation Glossary

Carlos María Rodríguez

May 3, 2021

1 Basics

Def. 1.1. *$\boldsymbol{I}$ denotes the set of all binary sequences of all lengths. $\boldsymbol{I_n}$ denotes the sequence of all binary sequences in $\boldsymbol{I}$, this is, $\boldsymbol{I_n} = \{0,1\}^n$.*

Def. 1.2. *(The class $\boldsymbol{\mathcal{P}}$).*
A function $f : \boldsymbol{I} \to \boldsymbol{I}$ is in the class $\mathcal{P}$ if there is an algorithm computing f and positive constants, A, c, such that $\forall n \in \mathbb{N}, \forall x \in I_n$, the algorithm computes $f(x)$ in at most An^c steps.

Def. 1.3. *(The class $\boldsymbol{\mathcal{NP}}$).*
The set $\mathcal{C} \in \boldsymbol{I}$ is in the class $\mathcal{NP}$ if there is a function $V_C \in \mathcal{P}$ and a constant $k \in \mathbb{R}$ such that:

- *If $x \in \mathcal{C}$, then $\exists y \in \mathbb{R}$ with $|y| \leq k|x|^k$ and $V_C(x, y) = 1$.*
- *If $x \notin \mathcal{P}$, then $\forall y$ we have $V_C(x, y) = 0$.*

The function V_C is called the *verification algorithm*, and the sequence y for which $V_C(x, y) = 1$ is called the *witness*.

Def. 1.4. *(The class **co**$\boldsymbol{\mathcal{NP}}$).*
A set $\mathcal{C} \in \boldsymbol{I}$ is in the class co$\mathcal{NP}$ iff its complement $\bar{\mathcal{C}} = \boldsymbol{I} \setminus \mathcal{C}$ is in $\mathcal{P}$.

Def. 1.5. *(Efficient reductions).*
Let $C, D \subset \boldsymbol{I}$ be two classification problems. $f : \boldsymbol{I} \to \boldsymbol{I}$ is an efficient reduction from C to D if $f \in \mathcal{P}$ and $\forall x \in \boldsymbol{I}$ we have $x \in C \iff x \in D$.
We write $C \leq D$ if such a reduction exists.

Def. 1.6. *(Hardness and completeness).*
A problem D is called $\mathcal{C}$-hard if $\forall C \in \mathcal{C}$, we have $C \leq D$. If we further have that $D \in \mathcal{C}$, then D is called $\mathcal{C}$-complete.

Def. 1.7. *(The SAT problem).*
Given a logical expression over Boolean variables (can take values in $\{0,1\}$ with connectives $\wedge, \vee, \neg$), is it satisfiable? This is, is there a boolean assignment of the variables trough which the expression evalutates to 1? The set of all such expressions is denoted by SAT.

Theorem 1.1. *SAT is $\mathcal{NP}$-complete.*

Def. 1.8. *(The $2DIO$ problem).*
Given a Diophantine equations of the form $Ax^2 + By + C = 0; A, B, C \in \mathbb{Z}$, is it solvable with positive integers?

Theorem 1.2. *$2DIO$ is $\mathcal{NP}$-complete.*

Def. 1.9. *(The $3COL$ problem).*
Given a planar map, can you color it using only 3 different colors?

Theorem 1.3. *$3COL$ is $\mathcal{NP}$-complete.*

Def. 1.10. *(The $subset - sum$ problem).*
Given a sequence $a_1, a_2, ..., a_n \in \mathbb{Z}$ and b, is there a subset J such that $\sum_{i \in J} a_i = b$?

Theorem 1.4. *$Subset - sum$ is $\mathcal{NP}$-complete.*