Q1

- Ch 3 : Arithmétique modulaire
- La division euclidienne
- Le modulo
- Congruences
- Ch 4 : Logique mathématique
- Propositions et prédicats
- Connecteurs logiques de base
- Formules en logique
- Calcul booléen et table de Karnaugh
- Les ensembles

Ch 3 : Arithmétique modulaire

$$ 349 = 349 * 1 $$

Les nombres premiers sont des nombres qui ne peuvent être divisé entièrement que par eux même et par 1. Par exemple 349 ne peut être divisé entièrement que par 349 et 1. Soit la seule factorisation possible de p est $p = 1 * p$. Exemples: 2, 3, 5, 7, 11, 13, 17, ...

$$ 1875 = 3 * 5 * 5 * 5 * 5 $$

N'importe quel nombre peut être factorisé en nombres premiers. Et il y a une infinité de nombres premiers.

Tester si un nombre est premier en utilisant un algorithme basique

```
def is_prime(n):
  for i in range(2,n):
    if (n%i) == 0:
      return False
  return True
```

Pour tester si un nombre est premier, on peut tester la division de tous les nombres jusqu'a $ \sqrt{n} $. Ce qui est peu efficace car on va aussi tester des nombres non premiers.

Tester si un nombre est premier en utilisant le crible d'Eratosthène

Pour calculer tous les nombres premiers $ \leq n $.

1. Lister les entiers de 2 à n
2. Pour chaque nombre plus petit que $ \sqrt{n} $ barrer tous les multiples du nombre (mais pas le nombre en lui même).

3. Tous les nombres qui restent sont des nombres premiers

Décomposer un nombre en produits de facteurs premiers

1. On divise le nombre successivement par des nombres premiers de plus en plus grand jusqu'a arriver à 1. Dans cette exemple, on va factoriser le nombre 4410.

$$ 4410 / 2 / 3 / 3 / 5 / 7 / 7 = 1 $$

2. Donc On arrive avec les valeurs suivante

$$ 4410 = 2 * 3 * 3 * 5 * 7 * 7 $$

3. Qui peut donc être simplifié de la manière suivante

$$ 4410 = 2 * 3^2 * 5 * 7^2 $$

La division euclidienne

Pour faire la division euclidienne d'un nombre je fais la division euclidienne des nombres positifs à la calculatrice.

N/D	Q	R
58/9	6	4
-58/9	$-6 - 1 = -7$	$-58 = 9 * -7 = 5$
58/-9	-6	4
-58/-9	7	5

Division euclidienne de deux polynomes

Le modulo

Trouver l'inverse modulaire

Prenons l'exemple de $9\mod80$

On peut écrire 9 et 80 dans le tableau suivant

R	9 (u)	80 (v)	Q
9	1	0	
80	0	1	

Ensuite on peut effectuer la division euclidienne des deux dernières lignes soit $9 \div 80$ et mettre le reste dans la première colonne et le quotient dans la dernière

R	9 (u)	80 (v)	Q
9	1	0	
80	0	1	
9			0

Maintenant on va multiplier chaque avant-dernière case moins chaque dernière case des deux dernières colonnes avec le quotient que l'on a trouvé

R	9 (u)	80 (v)	Q
9	1	0	
80	0	1	
9	$1-0*0=1$	$0-1*0=0$	0

Enfin on peut recommencer de nouveau depuis l'étape 2 jusqu'a arriver à un reste qui vaut 1. Si il n'y a pas de 1 et que l'on passe directement à 0, alors il n'y a pas d'inverse modulaire.

R	9 (u)	80 (v)	Q
9	1	0	
80	0	1	

R	9 (u)	80 (v)	Q
9	$1-0*0=1$	$0-1*0=0$	0
8	-8	1	8
1	$1-(-8)*1=9$	$0-1*1=-1$	1

Maintenant on peut prendre le résultat de la colonne u et :

- si celui-ci est plus grand que 80 on fait $80 - u$
- si celui-ci est plus petit que 0 on fait $80 + u$
- si celui-ci est entre les deux on le garde tel quel

Donc ici 9 est plus grand que 0 et plus petit que 80 donc le résultat est **9**

Faire le modulo d'un exposant négatif

Pour faire le $(690^{-6}) \mod 11$ on commence par faire l'inverse modulaire de 690 ce qui nous donne 7

Ensuite on fait $7^6 \mod 11$ ce qui nous donne donc 4 et c'est notre réponse finale.

Congruences

$$ 13 \mod 7 = 27 \mod 7 = 6 $$

> Deux nombres sont congrus si ils ont le même reste à la division euclidienne.

$$ a \mod n = b \mod n $$

Voici un énoncé plus court de la formule :

$$ a \equiv b (\mod n) $$

- Si a est congru à b alors $ a - b $ est divisible par n (peut être écrit comme $ a \equiv 0 (\mod n) $, 0 est le maximum donc si quelque chose n'est pas sous cette forme ce ne veut pas dire qu'il n'est pas divisible)
- Si a est congru à b et $ \alpha $ est congru à $ \beta $. Alors $ a+b $ et $ \alpha + \beta $ sont également congru, ainsi que $ a * b $ et $ \alpha * \beta $.

Ch 4 : Logique mathématique

La logique fournis des règles, des techniques permettant de décider si un raisonnement est valide ou pas.

La logique est utilisé en informatique, par exemple, pour définir les conditions qui détermineront la poursuite d'une boucle ou le choix d'une alternative au sein d'un programme, ou encore en SQL pour demander des choses à une base de donnée.

Propositions et prédicats

Proposition

Enoncé potentiel	Proposition ?	Raison	Valeur
Grand	Non	Trop ambigu	N/A
$ 4 = 9 $	Oui	N/A	Faux
8	Non	Aucune comparaison	N/A
"Je vais gagner au lotto"	Non	Pas de certitude, pas de connecteur logique	N/A
$ 7 + 9 > 11 $	Oui	N/A	Vrai

Une proposition est un énnoncé dont on peut dire avec certitude s'il il est vrai ou non. Une proposition n'est donc pas ambigue et peut avoir seulement 2 valeurs (1 (vrai) ou 0 (faux)).

Prédicats

Contrairement à une proposition un prédicat dépends d'une variable extérieure.

Connecteurs logiques de base

Minecraft logic gates
Image not found or type unknown

Sym	Nom mathématique	Electronique	Java	Minecraft
$ \neg $	Negation	NOT	!	Une torche de redstone sur un bloc avec un levier sur le bloc (inverseur)
$ \wedge $	Conjonction	AND	&&	2 torches activée par des leviers, reliées par une poudre de redstone et un inverseur
$ \vee $	Disjonction	OR	|| (ou inclusif)	Une poudre de redstone qui relie 2 leviers
$ \oplus $	Disjonction exclusive	XOR	^ (ou exclusif)	Trop compliqué à décrire
$ \iff $	Equivalence	XNOR	==	XOR avec un inverseur

La négation $ \neg $

La négation correspond à "Il est faut que P" (P étant une proposition)

Donc P prends la valeur contraire de $ \neg P $.

P	$ \neg P $	$ \neg \neg P $
0	1	0
1	0	1

Ceci est une table de vérité qui représente différentes valeurs d'énoncés par rapport à leur proposition(s).

La conjonction $ \wedge $

La conjonction est vraie si 2 propositions sont vraies.

P	Q	$ P \wedge Q $
0	0	0
1	0	0
0	1	0
1	1	1

La disjonction $ \vee $

La disjonction est vraie si une des 2 propositions sont vraie.

P	Q	$ P \vee Q $
0	0	0
1	0	1
0	1	1
1	1	1

Implication $ \implies $

$$ P \wedge Q \implies P \implies Q $$

Cet énoncé signifie que si P et Q sont vrai (AND) alors P est vrai et Q est vrai. L'implication correspond à "alors". Donc si XYZ alors ABC.

$$ \neg(x < y) \implies x = y $$

On peut par exemple imaginer une situation comme celle ci dessus, si x n'est pas plus petit que y alors x est égal à y.

P	Q	$ P \wedge Q $	$ P \implies Q $	$Q \implies P $
0	0	0	1	1
0	1	0	1	0

P	Q	$ P \wedge Q $	$ P \implies Q $	$Q \implies P $
1	0	0	0	1
1	1	1	1	1

Contrairement aux conjonctions (AND), si la première proposition (l'antécédent) est faux, alors l'implication est forcément vraie car le contraire n'a pas été prouvé.

Donc les deux propositions ne sont pas interchangables comme vu dans le tableau les colonnes 4 et 5 ne sont pas les mêmes. BB Un peu de vocabulaire :

Antécédent	Conséquent	Enoncé	Réciproque	Contraposée
P	Q	$ P \implies Q $	$Q \implies P $	$\neg Q \implies \neg P $

Equivalence $ \iff $

P	Q	$P \iff Q $	$Q \iff P $
0	0	1	1
1	0	0	0
0	1	0	0
1	1	1	1

L'équivalence est une genre d'égalité dans la logique. Cela signifie que P corresponds à Q. Les deux propositions sont interchangables.

Disjonction exclusive $ \oplus $

$$ P \oplus Q \iff (P \wedge \neg Q) \vee (\neg P \wedge Q) \iff \neg (P \iff Q) $$

La disjonction exclusive peut etre représentée par des AND, OR et NOT uniquement, c'est un genre de raccourcis. La disjonction exclusive (XOR) peut aussi être utilisée pour représenter une équivalence en ajoutant une négation (NOT).

P	Q	$ P \oplus Q $	$ P \vee Q $	$P \wedge Q $
0	0	0	0	0
1	0	1	1	0
0	1	1	1	0
1	1	0	1	1

Une disjonction exclusive (XOR) est comme une disjonction inclusive (OR) sauf que les deux propositions ne peuvent pas être vrai pour que le XOR soit vrai. Donc un XOR sera forcément faux là ou un AND sera vrai.

Quantificateurs

En plus des connecteurs logiques on peut aussi ajouter les quantificateurs :

Symbole	Signification	Exemple
$\forall$	Pour tous	« $\forall x \in N : x * 2$ est paire » → *Pour chaque valeur x dans N quand elle est multipliée par deux est paire*
$\exists$	Existe	« $\exists x \in N : x$ est paire » → *Il existe au moins un nombre dans l'ensemble N qui est pair*

Formules en logique

$$ \neg ((P \vee Q) \wedge R) $$

La formule précédente est une combinaison de connecteurs. Les parenthèses sont très importante car comme en arithmétique, les parenthèses indiquent les priorités des opérations, donc $ P \vee Q $ doit être fait avant la plus grande parenthèse, pour enfin terminer par la négation complète.

Antilogies & Tautologie

$$ \vdash P \vee \neg P $$

La formule ci-dessus signifie que $ P \vee \neg P $ donnera **toujours** 1. Ca s'appelle une tautologie. Une tautologie signifie qu'une formule sera toujours vraie.

$$ \vdash \neg (P \wedge \neg P) $$

Tandis qu'une antilogie signifie qu'une formule sera toujours fausse.

Calcul booléen et table de Karnaugh

https://www.youtube-nocookie.com/embed/buM3XxdRxU0

https://www.youtube-nocookie.com/embed/4jndJ6ADiiE

Tableau de Karnaugh

Une première manière de représenter une fonction logique avec des opérateurs booléens est d'utiliser les formes normales tel que vue au cours d'architecture des ordinateurs.

Mais pour des fonctions plus complexes, les formes normales ne sont pas très efficace pour représenter de manière concise la fonction.

Former le tableau (code binaire réfléchit)

Tout d'abord on liste les différents paramètres de la fonction. Imaginons a,b,c. On va donc avoir par exemple a et b horizontalement et c verticalement :

c/ab	?	?	?	?
?				
?				

Ensiute pour chaque groupe, on va les écrire côte à côte

```
 a   b
--- ---
   0
   1
```

Ensuite pour ajouter le chiffre suivant on va faire un "mirroir" de ce que l'on a écrit

```
 a   b
--- ---
    0
    1
-------
    1
    0
```

Et sur la colonne d'a côté on va écrire des 0 sur la première partie, et des 1 sur la deuxième

```
 a   b
--- ---
 0   0
 0   1
-------
 1   1
 1   0
```

Ce qui nous donne donc le code binaire réfléchit, et ainsi les intitulé de notre colonne → `00, 01, 11, 10`

c/ab	00	01	11	10
0				
1				

On peut donc écrire dans chaque case les valeurs de la fonction correspondante. Par exemple la deuxième case signifie que a est à 0, b est à 1 et c est à 0. On peut ainsi compléter le tableau.

Comment transformer une forme normale en tableau de karnaugh

1er forme (disjonctive)

Pour la première forme on va dire que chaque groupe (produit) correspond à un 1

$$ F(a,b,c) = \overline{a} * \overline{b} * c + \overline{a} * b * c + a * \overline{b} * \overline{c} + a * \overline{b} * c + a * b * c $$

On peut ensuite construire le tableau de karnaugh :

c/ab	00	01	11	10
00				
01				

Pour chaque groupe on peut indiquer un 1 dans le tableau, par exemple $\overline{a} * \overline{b} * c$ c'est l'équivalent de dire `a=0`, `b=0` et `c=1` on peut donc l'indiquer dans la case correspondante du tableau :

c/ab	00	01	11	10
0				
1	1			

Et ainsi de suite pour le reste du tableau, ce qui nous donne :

c/ab	00	01	11	10
0				1
1	1	1	1	1

On complète ensuite les cases restantes par des 0

c/ab	00	01	11	10
0	0	0	0	1
1	1	1	1	1

2e forme (conjonctive)

Pour la deuxième forme normale c'est un peu plus bizarre. Disons que l'on part de la forme suivante :

$$ F(a,b,c) = (a+b+c) * (\overline{a}+b+c) * (\overline{a}+b+\overline{c}) * (\overline{a}+\overline{b}+c) $$

Ensuite on inverse tous les paramètres

$$ F(a,b,c) = (\overline{a}+\overline{b}+\overline{c}) * (a+\overline{b}+\overline{c}) * (a+\overline{b}+c) * (a+b+\overline{c}) $$

Ensuite on procède exactement comme avant sauf qu'a la place d'écrire des 1 on écrit des 0.

c/ab	00	01	11	10
00	0		0	0

c/ab	00	01	11	10
01				0

Enfin on complète le reste avec des 1 :

c/ab	00	01	11	10
00	0	1	0	0
01	1	1	1	0

Simplifier un tableau de Karnaugh

Maintenant que l'on sait comment créer un tableau de Karnaugh, on va maintenant l'utiliser pour obtenir une forme plus abrégée des fonctions.

cd/ab	00	01	11	10
00	1	0	1	1
01	1	0	1	0
11	1	0	0	1
10	1	0	0	1

On peut ensuite grouper les différents éléments par puissance de 2 (donc par 1, 2, 4, 8, etc). **ATTENTION**, il faut imaginer le tableau comme une boule, les 1 sur les extrémités peuvent être reliées entre elles. Donc si par exemple il y a un 1 dans chaque coin, ils peuvent être connecté comme un seul groupe.

Par exemple voici un groupe (un peu complexe) de 1 dans tous les coins :

cd/ab	00	01	11	10
00	**1**	0	1	**1**
01	1	0	1	0
11	1	0	0	1
10	**1**	0	0	**1**

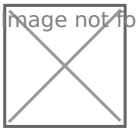
Ensuite on peut regarder quels sont les paramètres qui ne varient pas :

cd/ab	00	01	11	10
0**0**	**1**	0	1	**1**
01	1	0	1	0

cd/ab	00	01	11	10
11	1	0	0	1
1**0**	**1**	0	0	**1**

On remarque donc que dans tous les cas du groupe, *a* et *b* sont à 0. Donc l'expression en produit de notre groupe est $\overline{b} * \overline{d}$

On peut ensuite faire la même chose pour tous les groupes ce qui nous donne :



Il faut donc essayer de toujours prendre les plus grand groupes (pour avoir les plus petits produits) et d'en prendre le moins possibles (pour avoir le moins de produits possibles).

Cela va donc nous donner l'expression simplifiée suivante :

$$ F(a,b,c) = \overline{b} * \overline{d} + \overline{a} * \overline{b} + \overline{c} * a * b + \overline{b} * c $$

Les ensembles

Un ensemble est une collection non-ambigue d'objet distincts. C'est à dire que l'on peut définir ce qui relie tous les objets, et que les objets ne peuvent apparaitre qu'une seule fois dans l'ensemble.

Voici quelques exemples d'ensembles :

- Des ensembles finis de nombres : $A = \{ 0, 1, 2, 5, 9, 11 \}$
- Des ensembles finis de noms : $B = \{ Alain Dupont, Béatrice Durant, Linel Hicq, Nadine Tudor \}$
- Des ensembles infinis : $C = \{1,2,3,4,5,...\}$

On défini un ensemble par la caractéristique commune à tous les éléments

$$ A = \{x | x \in \mathbb{N}\} $$

Cette notation fait appel à la notion de préciats que l'on a vu plus tôt, voir ici, car on a un prédicat sur la variable x

$$ A = \{ x | P(x)\} $$

Quand un ensemble ne contient aucun élément on dit que c'est un ensemble "vide"

$$ B = \{\varnothing\} $$

Cardinalité des ensembles

Pour connaitre le cardinal d'un ensemble, il suffit de compter ses éléments.

- Si c'est un ensemble vide ($\varnothing$), alors le cardinal est 0
- Si c'est un ensemble qui contient d'autres ensembles, on ne fait que compter les ensembles (sans leur contenu)

Ainsi pour l'ensemble suivant :

$$ A = \{\{A\}, \{A,C\}, B, \{B,C,D,E\}, D, \{D,E\},H\} $$

Cet ensemble a un cardinal de 7.

Les relations entre les ensembles

- L'égalité. C'est à dire que a appartient à b et b appartient à a. → $\forall x \in E, (x \in A) \iff (x \in B)$

En plus de l'égalité on a aussi les opérations ensemblistes : **Attention** comme dans tous les ensembles il n'y a pas besoin de répèter les nombres.

Nom	Expression mathématique	Description
L'union	$A \cup B = \{x\|x \in A \lor x \in B\}$	soit tous les éléments qui sont dans A ou qui sont dans B
L'intersection	$A \cap B = \{x\|x \in A \land x \in B \}$	soit tous les éléments qui sont dans A et qui sont dans B
La différence	$A \setminus B$ ou $A - B = \{x\|x \in A \land x \notin B \}$	tous les éléments qui sont dans A mais pas dans B
La différence symétrique	$A \oplus B = \{ x \| (x \in A \land x \notin B) \cup (x \notin A \land x \in B) \}$	Tous les éléments qui sont uniquement dans A + tous les éléments qui sont uniquement dans B

Résoundre les diagrammes de Eulen-Venn

Pour arriver à trouver un les éléments d'un diagramme qui correspondent à une expression ensembliste, j'essaye de trouver des patterns dans l'expression.

Voici les patterns que j'ai identifiés :

- $A\cup B$ ou $A\setminus\overline{B}$ → Tous les éléments de A et tous les éléments de B (en faisant attention à ne pas répèter un même élément)
- $A\cap B$ → Les éléments communs à A et B
- $A\setminus B$ ou $A\cap\overline{B}$ → On prends les éléments de A et on retire ceux qui sont dans B
- $\overline{A}\setminus \overline{B}$ ou $\overline{A}\cap B$ → On prends les éléments de B et on retire ceux qui sont dans A
- $A\cup\overline{B}$ → Tous les éléments de B + tous les éléments qui ne sont pas dans A (en faisant attention à ne pas répèter plusieurs fois un même élément)
- $\overline{A}\setminus {B}$ ou $\overline{A} \cap \overline{B}$ → on prends tout sauf A et B