Contrôle Terminal BUT2 - Semestre 3

R4.04 Méthodes d'optimisation Parcours C

Nom Responsable	Godin Thibault
Date contrôle	07/04
Durée contrôle	1h30
Nombre total de pages	6
Impression	recto-verso
Documents autorisés	1 feuille A4 notes personnelles
Calculatrice autorisée	NON
Réponses	sur le sujet

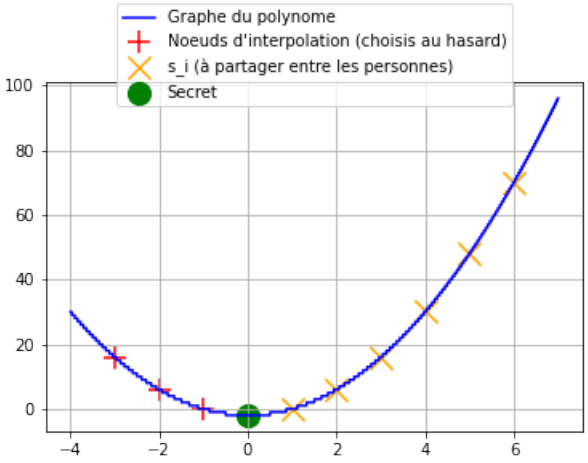
NOM Prénom : **Groupe :**

Exercice 1 : (Shamir)

On veut partager le secret $s = -2$ selon le protocole de Shamir.

Pour cela on interpole les points $(0, s), (-1, 0), (-2, 6)$ et $(-3, 16)$; et on distribue les points $(1, 0), (2, 6), (3, 16), (4, 30), (5, 48), (6, 70)$.

On demande d'expliquer en justifiant brièvement le fonctionnement de ce protocole



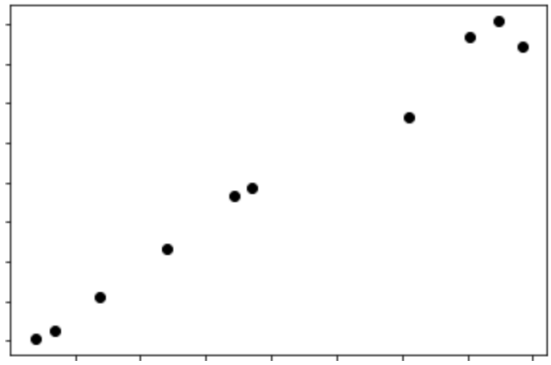
1. Quel est le degré théorique du polynôme d'interpolation utilisé ?

2. 5 personnes réunissant leurs informations peuvent-elles retrouver le secret ? Quel est le nombre théorique minimal de personnes nécessaires à la reconstruction de l'information ?

3. *Bonus* Que pensez-vous de cet exemple particulier ?

Exercice 2 : (QCM) *Entourer la ou les bonnes réponses. QCM à points négatifs.*

1. On a les données suivantes :



   a L'erreur commise en interpolant tous les points par un polynôme de Lagrange est plus petite que l'erreur commise en faisant une régression linéaire

   b L'erreur commise en interpolant tous les points par un polynôme de Lagrange est plus grande que l'erreur commise en faisant une régression linéaire

   c une régression linéaire serait plus pertinente pour prédire le prix d'un appartement connaissant sa surface

   d Une l'interpolation polynomiale serait plus pertinente pour prédire le prix d'un appartement connaissant sa surface

2. On s'intéresse à la méthode du gradient (sur la fonction dérivable autant de fois que souhaité)

   a La méthode de gradient converge toujours.

   b La méthode de gradient converge toujours si on choisi un pas assez petit.

   c Si méthode de gradient converge, on atteint un minimum local.

   d Si méthode de gradient converge, on atteint un minimum global.

NOM Prénom : **Groupe :**

Exercice 3 : (toy Reed-Solomon)

On transmet un message M avec une lettre supplémentaire pour la détection d'erreur r, selon le protocole vu TP3b. Dire en justifiant si le message avec lettre supplémentaire $[M, r]$ a été bien transmis (*cad* ne comporte pas d'erreur).

1. $[M, r] = [(0, 4), (1, 4), (2, 6), (3, 10)]$

2. $[M, r] = [(0, 1), (1, 4), (2, 6), (3, 10)]$

3. $[M, r] = [(1, 0), (4, 1), (10, 3)]$

4. $[M, r] = [(1, 0), (4, 1), (10, 0)]$

5. $[M, r] = [(1, 0), (4, 1), (10, -3)]$

On précise les évaluation de divers polynômes

$P(x)$	0	1	2	3	4	10
$1 + 3x$	1	4	7	10	13	31
$1 + \frac{11}{3}x - \frac{2}{3}x^2$	4	4	$\frac{17}{3}$	6	5	-29
$4 - x + x^2$	4	4	6	10	16	94
$-\frac{1}{3} + \frac{1}{3}x$	$-\frac{1}{3}$	0	$\frac{1}{3}$	$\frac{2}{3}$	1	3
$\frac{1}{9}(-7 + 8x - x^2)$	$-\frac{7}{9}$	0	$\frac{5}{9}$	$\frac{8}{9}$	1	-3

Exercice 4 : (Gradient) On se propose d'étudier la fonction $f(x, y) \mapsto x^2 + 2y^4 - y^3 - 4$

1. Donner le gradient (dérivées partielles) ∇f de la fonction f.

2. En déduire les points pouvant être des minimum locaux de f.

3. Appliquer les 3 premières étapes de l'algorithme, avec un pas $\delta = 0.2$ à partir du point $(2, 0)$

4. Un étudiant affirme *"Augmenter le pas δ améliore toujours le temps de convergence vers un minimum local"*. Commenter son affirmation.

NOM Prénom : **Groupe :**

Exercice 5 : (SAT)

On cherche à résoudre l'énigme "Un fermier doit passer la rivière dans une barque juste assez grande pour lui et son loup, ou lui et sa chèvre, ou lui et ses choux. Les choux seront mangés s'il les laisse seuls avec la chèvre, et la chèvre sera mangée s'il la laisse seule avec le loup. Comment faire passer tout ce monde sans dégâts ? [1]

On va se demander si on peut résoudre ce problème en T traversées. On utilise les variables $f_i, i \in \{0, \ldots, T\}$ "le fermier est sur la rive de gauche à l'instant i" (sinon il est donc sur la rive de droite) ; $g_i, i \in \{1, \ldots, P\}$ "la chèvre est sur la rive de gauche à l'instant i"" ; $l_i, i \in \{, \ldots, T\}$ "le loup est sur la rive de gauche à l'instant i" et $c_i, i \in \{0, \ldots, T\}$ "le chou est sur la rive de gauche à l'instant i"" Pour cela on va créer plusieurs clause :

- Une clause pour le début : $init = f_0 \wedge g_0 \wedge l_0 \wedge c_0$
- Une clause pour la fin : $end = \neg f_T \wedge \neg g_T \wedge \neg l_T \wedge \neg c_T$
- Une clause pour le danger : $danger_i$ si un participant peut en manger un autre
- Une clause pour le passage : $cross_i$ modélisant une traversée au temps i.

1. Écrire la formule modélisant la situation "le fermier est sur la rive gauche au temps i et sur la rive droite au temps $i + 1$"

2. Écrire la formule modélisant la situation "le fermier change de rive entre l'instant i et l'instant $i + 1$"

3. Écrire la formule modélisant la situation "le loup ne change pas de rive l'instant i et l'instant $i + 1$"

4. Écrire la clause $cross_i$ en utilisant les variables $f_i, f_{i+1}, g_i, g_{i+1}, l_i, l_{i+1}, c_i$ et c_{i+1}

5. Écrire la formule modélisant la situation "le chèvre et le loup sont sur la rive gauche à l'instant i" en utilisant les variables f_i, g_i, l_i et c_i.

1. source : `fr.wikipedia.org/` Problèmes de passage de rivière

6. Écrire la formule modélisant la situation "le chèvre et le loup sont sur la même rive à l'instant i" en utilisant les variables f_i, g_i, l_i et c_i.

7. Écrire la clause $danger_i$ en utilisant les variables f_i, g_i, l_i et c_i

8. Écrire la formule finale modélisant le problème avec exactement K traversées.

9. Expliquer brièvement l'intérêt d'un SAT solveur pour ce problème.