des résultats convaincants avec des logiciels comme `Maple`, `Sage` ou `XCas`.

6.4 Option C : Algèbre et Calcul formel

Généralités

La qualité générale des exposés tend à baisser. La préparation de l'exposé, à l'instar de la compréhension du texte, devrait être un passage incontournable de la préparation, là où l'on voit de nombreux candidats arriver sans s'être posé la question de la restitution de ce qu'ils ont étudié et compris – avec pour conséquence qu'ils restent beaucoup trop près du texte. Même s'il est permis de garder le texte en main, on ne saurait trop conseiller aux candidats de le laisser sur la table lors de l'oral...

S'il est parfaitement légitime de ne pas vouloir aborder tous les aspects d'un texte, la stratégie, adoptée cette année par certains très bons candidats, d'en rester au premier tiers et de refuser d'entrer dans les mathématiques avancées, ne permet pas, sauf exception, d'obtenir une excellente note.

Enfin, l'oral de l'option C n'est pas un problème, ou une suite d'exercices, d'algèbre. La ligne directrice du calcul formel est la recherche de l'*effectivité*, puis de l'*efficacité* (souvent en temps, parfois en espace) du calcul algébrique, en allant des aspects les plus élémentaires (calcul avec les entiers, les polynômes, les entiers modulo, les séries formelles) aux aspects plus avancés (élimination, géométrie effective, codes correcteurs d'erreur). Se poser ces questions permet, dans de très nombreux cas, de mieux comprendre la ligne directrice des textes, et d'en proposer un exposé éclairant ; par exemple d'expliquer, au-delà de ce que le texte fait, *pourquoi* il le fait.

Les candidats ayant le réflexe de se saisir, seuls, d'une question de complexité, sont perçus très positivement par le jury. Pour prendre un exemple, quand le texte parle de cryptographie, comparer le coût du système proposé et le coût d'une attaque, même naïve, est une initiative intéressante et actuellement inexistante. Une telle étude est beaucoup plus à sa place qu'un exposé détaillé de RSA plaqué sur un texte qui n'en parle pas – la mention rapide de RSA dans un texte introduisant un système de chiffrement pour comparer des complexités restant bien sûr pertinente. Plus largement, une réflexion minimale sur les ordres de grandeur (est-ce qu'un calcul faisable représente $10^1, 10^{10}, 10^{100}, 10^{1000}$ opérations élémentaires) permettrait souvent de mieux situer les problèmes soulevés par un texte, ou de proposer des valeurs de paramètres réalistes quand ce sujet n'est pas évoqué par le texte.

Aspects mathématiques

Les remarques de l'année 2012 s'appliquent intégralement à la session 2013, et on renvoie le lecteur à ce rapport, en ajoutant ici quelques remarques complémentaires.

- L'algèbre linéaire n'est toujours pas l'acquis solide qu'elle devrait être, ses aspects effectifs peuvent encore progresser. Le réflexe "pivot de Gauss / n^3" en réponse aux questions effectives d'algèbre linéaire est devenu plus répandu, avec parfois des surprises : pour certains candidats, il peut permettre de calculer le rang, mais pas le déterminant, ou seulement de résoudre des systèmes linéaires, *etc.* Aussi, il est bon d'avoir fait un pivot entier à la main pour s'être posé la question de la "remontée", par exemple pour le calcul de l'inverse : on ne décide pas soudainement d'opérer sur les colonnes, contrairement à une idée répandue. Les questions de valeurs propres, en particulier la différence entre sous-espace propre et sous-espace caractéristique, restent mal comprises.
- Le résultant reste la terreur des candidats. Beaucoup surcompensent des lacunes en infligeant au jury un extrait de lecon d'algèbre sur le sujet, avec des hypothèses (trop) générales, et sans le résultat souvent utile, voire central, dans le contexte de l'option C, *i.e.* celui concernant la spécialisation d'une variable, faisant apparaître la condition de non-annulation simultanée des termes de tête. Ces remarques sur le résultant s'appliquent également à d'autres sujets ; rappelons donc que le jury n'accordera **a**ucune valeur

à un exposé de leçon généraliste sur une notion du texte, et qu'on se limitera, au plus, à l'énoncé du théorème pertinent dans le contexte étudié.
- Pour ce qui est de l'arithmétique, le point noir reste l'algorithme d'Euclide étendu, qui reste assez peu formalisé dans l'esprit des candidats ; les connaissances sur les corps finis progressent, tout en restant fragiles. En particulier, le fait que l'endomorphisme de Frobenius permet, partant d'une racine d'un polynôme, d'obtenir toutes les autres, n'est pas connu des candidats. Un certain nombre de candidats se lancent dans une discussion sur l'algorithme de Berlekamp (un peu à tout propos, d'ailleurs). Outre qu'une telle discussion est souvent hors sujet, l'algorithme (difficile) est en général compris de manière tellement superficielle que ça n'a, cette année, jamais été une bonne idée.
- Les codes correcteurs sont une partie limitée du programme, et très peu de connaissances sont exigibles (et exigées). Néanmoins, il est bon de s'y être un peu frotté pour se familiariser avec les problématiques sous-jacentes, typiquement qu'un bon code correcteur se décrit de façon compacte (et est donc en général linéaire), a une grande dimension et grande distance minimale (par rapport à sa longueur) et, aussi et surtout un algorithme de décodage efficace – rappelons que ce second point n'est pas vrai d'un code linéaire "quelconque". Il faut s'être confronté à ces faits pour comprendre les questions que se pose presque tout texte sur les codes...
- Sur les aspects complexité, rappelons qu'il est toujours pertinent de dire ce qu'on compte, car c'est souvent ambigu en calcul formel : opérations sur les éléments du corps, ou de l'anneau de base ; ou (préférable, mais parfois trop difficile) opérations "élémentaires" sur des petits entiers. L'exemple de l'algorithme d'Euclide est éclairant : la complexité linéaire du nombre de divisions euclidiennes oublie un fait important : soit le nombre d'étapes est petit, soit les quotients sont petits en moyenne, et le coût total est quadratique là où on l'attendrait, naïvement, cubique. La mise en regard de ces deux complexités est un élément important sur l'algorithme. Sur ces aspects complexité, relevons aussi une confusion fréquente et pourtant élémentaire entre opérations consécutives (on ajoute les complexités) et opérations imbriquées (on les multiplie), qui conduit à des aberrations (complexités de l'ordre de $n!$ ou n^n quasi-systématiques).

Enfin, tout cela n'a de sens qu'une fois la question de la représentation des objets réglée : entiers, polynômes mais aussi séries formelles et réels. Pour ces derniers, de loin les plus délicats, signalons que les connaissances attendues sur les flottants sont très limitées (essentiellement une prise de conscience des problèmes liés à la perte de précision catastrophique lors de la soustraction de deux nombres proches), et qu'on attend surtout une réflexion sur les limites de l'approximation et la différence, du point de vue algébrique, entre monde réel et monde approché (pgcd de deux polynômes à coefficients réels, par exemple, ou encore les 0.999999999 ou 1.000000001 affichés par les logiciels).

Informatique

La qualité de l'illustration informatique semble inexorablement en baisse, la réflexion associée est bien pauvre, et le commentaire de l'illustration presque inexistant. Ce n'est pas le cas des attentes du jury sur ce sujet, et ce hiatus finira nécessairement par conduire à un durcissement de l'évaluation sur ce point. Les remarques des années passées continuent à s'appliquer : en particulier, on ne découvre pas un logiciel le jour de l'oral, mais on en connaît les capacités et, surtout, les limites avant.

6.5 Option D : Modélisation et Analyse de Systèmes Informatiques

Commentaires généraux

Le jury a apprécié le travail accompli pour la préparation de cette épreuve par les meilleurs candidats. Il a interrogé les candidats dans le même esprit que dans les autres options et les critères d'évaluation étaient