

PEUT-ON ÊTRE CERTAIN DE L'INCERTITUDE?



Projet d'étudiants de 1^{ère} année
Nathan Azoulay, Anas Barakat et Adrien Cohen-Olivar
Encadrés par Lirida Naviner et You Wang

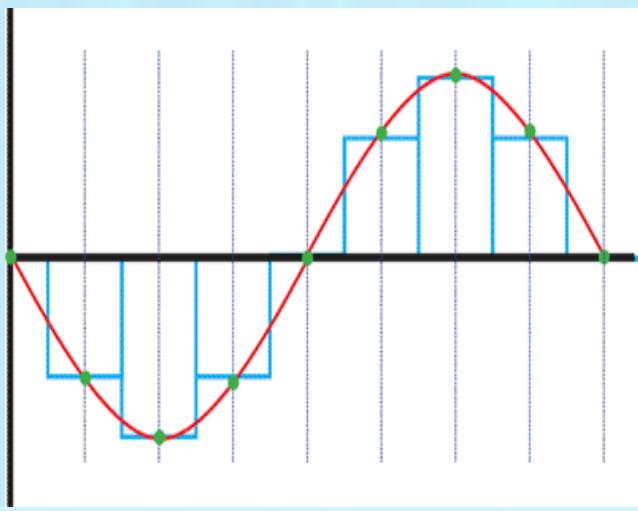
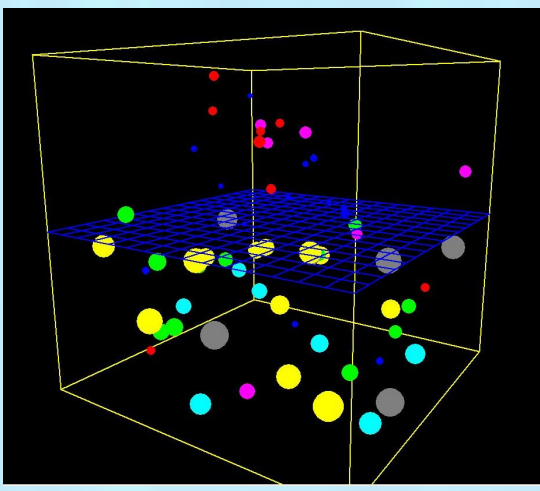
PAF
15 jours
chrono!

1- Problématique

01111000011101110110101...100
Est-ce vraiment une séquence aléatoire?

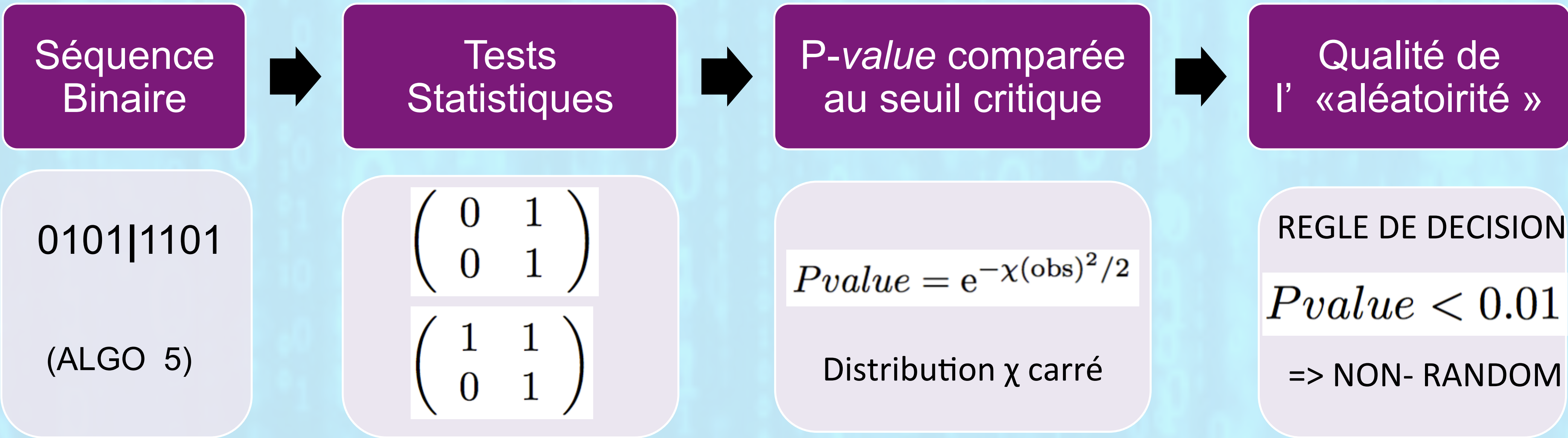
- Testeur, Qualité, Aléatoire, PRNG

2- Applications



Simulation Échantillonnage Cryptologie

3- Principe des tests



4- Algorithmes de Tests *



1 – Test de Fréquence

100101010

Combien de 1 ?

≈ 50 %

sinon



2 – Test de Fréquence par bloc

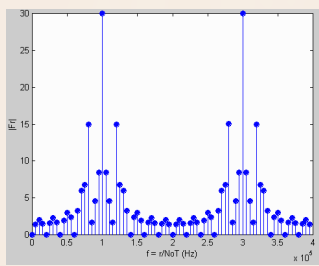
100|101|010

100
101
010

Test de Fréquence
Test de Fréquence
Test de Fréquence

5 - Test à Transformée de Fourier Discrète

100101010



Détection de motifs périodiques

7 –Test de détection de motifs redondants sans chevauchement

100101010
motif: 110

Comptage de la redondance

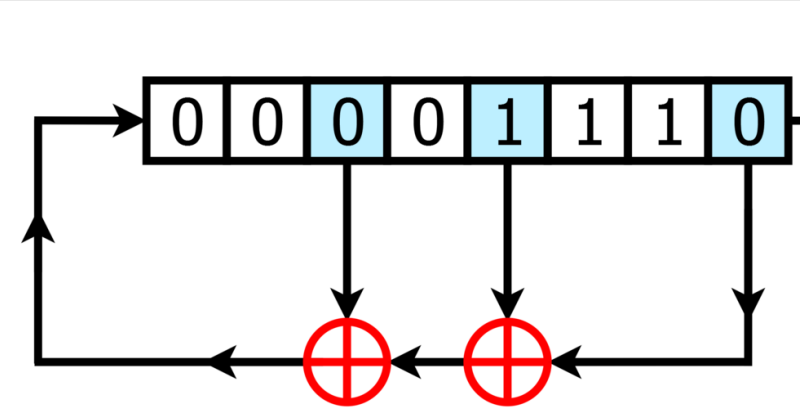
Si correspondance
100101010
Sinon
100101010

8 –Test de détection de motifs redondants avec chevauchement

Toujours décalage d'un bit

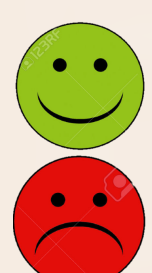
10 – Test de Complexité Linéaire

LFSR

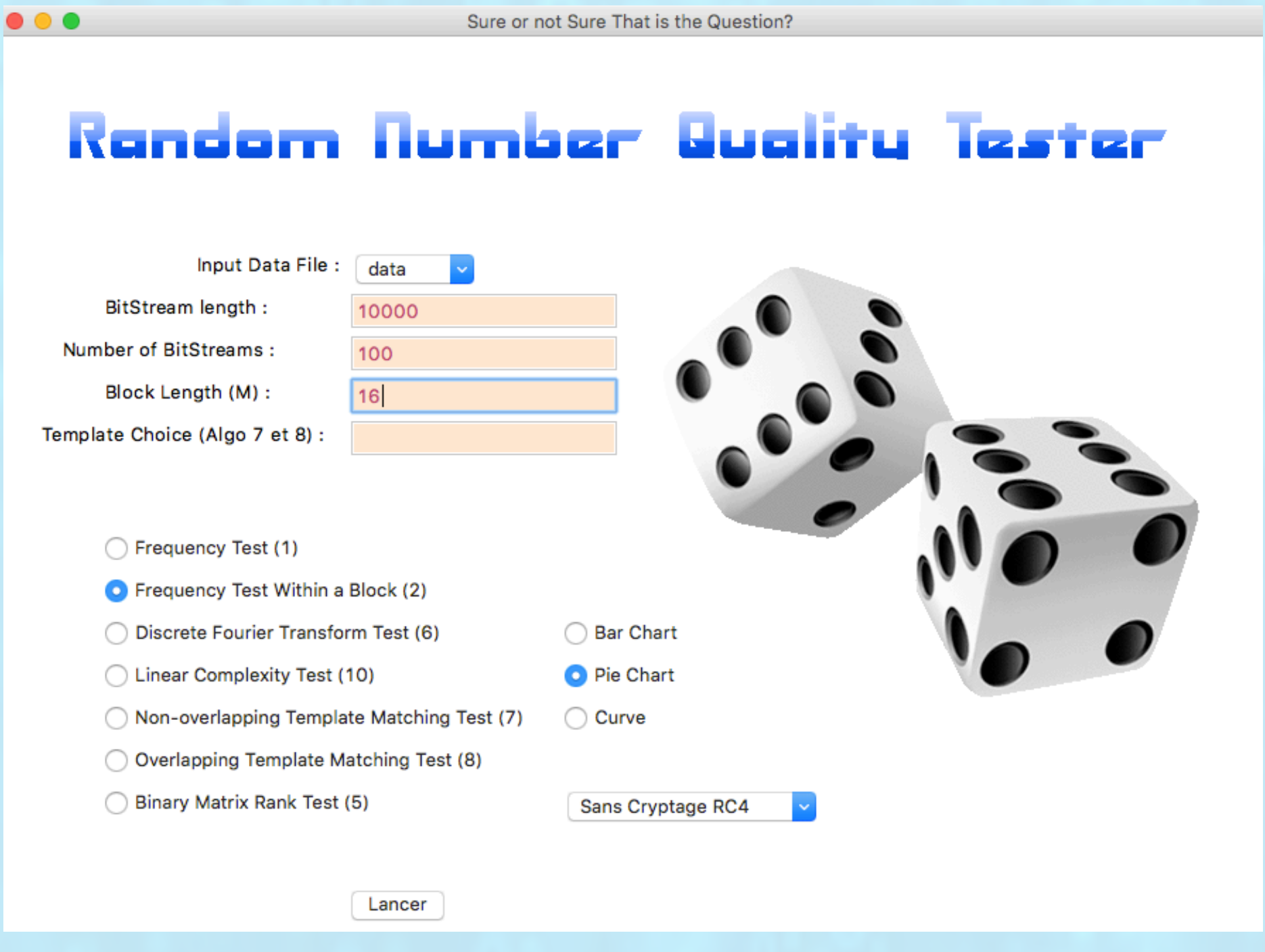


Algo de
Berkelamp-
Massey

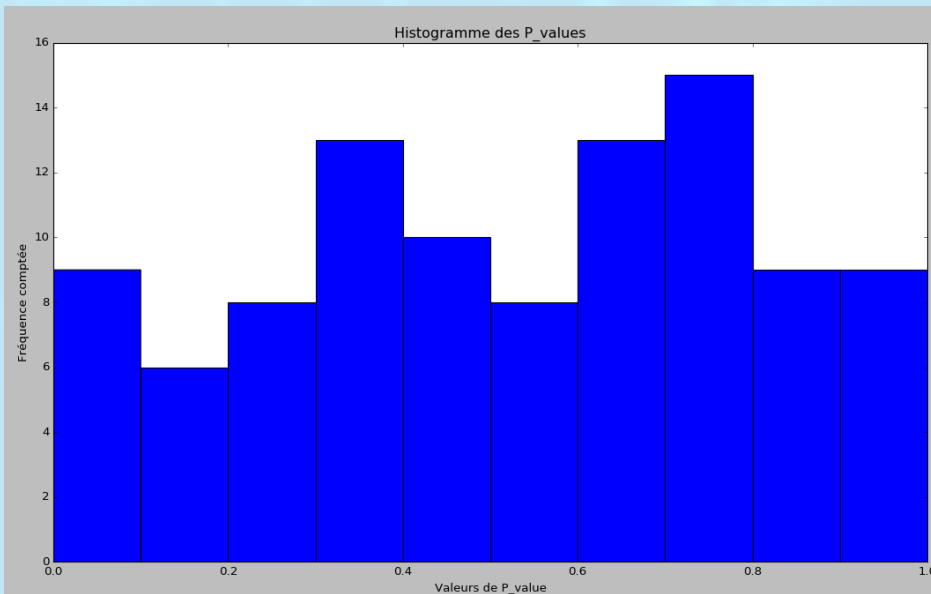
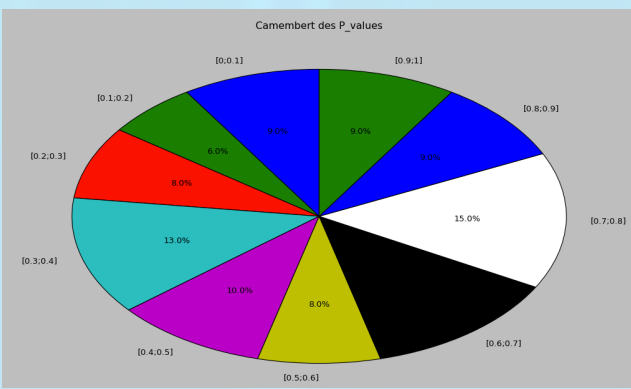
Complexité linéaire
grande
Petite



5- Interface graphique (Tkinter)



6- Résultats



Distribution uniforme des P_value sur [0,1] avec 100 tests

7-Conclusion

- **Réalisation:** implémentation des algorithmes, GUI, codage RC4
- **Qualité:** fonctionnels
- **Pour aller plus loin:** génération de nombres