//

COMPRESSION

Compression sans perte d'information

- Arithmetic coding - Code arithmétique
- Burrows-Wheeler transform - BWT - Algorithme de tri utilisé comme pré-traitement pour améliorer une compression.
- Byte pair encoding
- Context Tree Weighting - CTW - Algorithme de compression utilisé pour les fichiers textes

- Deflate - Algorithme de compression de données utilisée par ZIP.
- Dynamic Markov compression - DMC - Technique de compression par encodage arithmétique adaptative et statistique.

- Elias Delta coding - Algorithme de compression de données. Compression des séquences qui apparaissant fréquemment.

- Elias Gamma coding - Encodage universel des entiers positifs.

- Elias Omega coding - Encodage universel des entiers positifs.

- Embedded Zerotree Wavelet - EZW - Codage progressif pour comprimer une image en une suite de bits, avec une précision progressive. Peut être utilisé en compression avec perte pour un résultat plus spectaculaire.
- Even-Rodeb Code -

- Fibonacci coding - Encodage d'entiers positifs en mots binaires.
- Golbach Codes

- Golomb coding - Codage optimal pour les alphabets suivant une distribution géométrique.
- Huffman coding - Assigne des codes aux symboles de sorte que la longueur des codes

corresponde à la probabilité des symboles .

- Incremental encoding - Delta encoding appliqué à des séquences de chaînes.
- Interpolative Coding

- Kraft-McMillan Inequality

- Laplacian Pyramid - LP -

- LZ77 - La base des déclinaisons à venir en LZ Lempel-Ziv (LZ78, LZW, LZSS, LZMA, LZO, ROLZ Reduced Offset Lempel Ziv). Tous sont basés sur un c ode utilisant un dictionnaire .

- LZ78 - Code utilisant un dictionnaire.
- LZSS - Code utilisant un dictionnaire.

- Lempel-Ziv-Welch - LZW - Successeur de LZ78. Construit une table de translation à partir des données à compresser. Est utilisé par le format graphique GIF.

- Lempel-Ziv-Markov chain-Algorithm - LZMA
- Lempel-Ziv-Oberhumer - LZO - Algorithme axé sur la vitesse.
- Levenstein Code

- Move to Front - MTF - Algorithme de tri utilisé comme pré-traitement pour améliorer une compression.
- Phased-In Codes

- Prediction by Partial Matching - PPM - Prédiction par correspondance partielle. Technique de compression adaptative et statistique.
- Range encoding - Même principe que le codage arithmétique, mais avec un procédé différent.

- Redundancy Feedback Coding - RF -

- Recursive Phased-In Codes

- Recursive Bottom-Up Coding - RBUC -

- Recursive Range Reduction

- Rice codes - Codage optimal pour les alphabets suivant une distribution géométrique.

- Run-length encoding - RLE - Algorithme primaire remplaçant une séquence uniforme par

le nombre d'occurrences
- Schalkwijk's Coding

- Self-Delimiting Codes

- Shannon-Fano coding - Construit des codes préfixes basés sur un ensemble de symboles et probabilités.
- Subexponential Code

- Sequitur - Algorithme qui décompose une chaîne en vocabulaire (ou grammaire incrémentale).
- Stout Codes
- Taboo Codes

- Ternary Comma Code

- Tjalkens-Willems V-to-B Coding

- Teuhola-Raita - Algorithme qui exploite la redondance des caractères.

- Tunstall code

- Truncated binary encoding - Un encodage normalement utilisé pour une distribution uniforme avec un alphabet fini. Améliore le codage binaire.
- Unary coding - Représente un nombre n avec n autres suivis par un zéro.
- Universal Codes

- Wang's Flag Code

- Yamamoto Flag Code

- Zeta coding - Algorithme utilisé en compression des graphes.

Compression avec perte d'information

- Algebraic code-excited linear prediction - ACELP

- A-law algorithm - Compression utilisée dans le domaine de la téléphonie.
- Fractal compression - Compression d'images utilisant les fractales.

- Karhunen–Loève theorem - KLT -

- Linear predictive coding - LPC - Utilise l'enveloppe spectrale sous forme compressée du

signal digital de la voix.

- Mu-law algorithm - Compression de signal analogique.
- Set Partitioning In Hierarchical Trees - SPIHT -

- Transform coding - Utilisé pour les données de type audio ou photos.
- Vector quantization - Technique utilisée dans la compression avec perte.
- Wavelet compression - Type de compression convenant bien aux images et à l'audio.
- Warped linear predictive coding - WLPC -

COMPILATION

Allocation de mémoire

- Boehm garbage collector - Gestionnaire de mémoire.
- Buddy memory allocation - Allocation de mémoire en réduisant la fragmentation.
- Generational garbage collector - Gestionnaire de mémoire rapide qui se base sur l'ancienneté des enregistrements.
- Mark and sweep
- Reference counting - Gestionnaire d'allocation simple qui compte le nombre de liens sur une donnée et récupère l'espace quand il vaut zéro.

Systèmes distribués

- Lamport ordering - Un ordonnateur d'évènement basé sur la relation happened-before (arrivé avant).
- Snapshot - C'est la sauvegarde de l'état global du système.
- Vector clocks - Ordonnancement total des évènements.
- Marzullo - Synchronisation distribuée selon le temps alloué.
- Intersection - Autre algorithm basé sur le temps alloué.

Systèmes d'exploitation

- Banker - Algorithme pour éviter les plantages.

- Page replacement - Sélection de pages à sacrifier quand la mémoire manque.
- Bully - Sélection d'un poste prioritaire.

Algorithmes de contrôle de disque

- Elevator - Planification de disque fonctionnant comme un ascenceur.
- Shortest seek first - Planification du disque pour réduire le temps d'accès.

Algorithmes de synchonization de processus

- Peterson - Permet à deux processus de partager une même ressource sans conflit, grâce à l'emploi d'une mémoire commune pour communiquer.
- Lamport's Bakery - Améliore la robustesse de la gestion de plusieurs processus en multi-tâches au moyen d'exclusions mutuelles.
- Dekker - Algorithme de programmation concurrente.

Algorithmes de minutage (scheduling)

- Earliest deadline first scheduling - Quand un évènement survient (fin de tâche, nouvelle tâche, etc...) on recherche dans la liste le processus à terminer au plus tôt.

- Fair-share scheduling - Partage le temps processeur entre les groupes ou utilisateurs. On appelle récursivement pour cela un autre algorithme pour gérer le partage entre processus.

- Least slack time scheduling - Least Laxity First affecte les priorités selon les différences temporelles pour les processus. date limite, le moment où on est prêt, le temps d'exécution.

- List scheduling - A partir d'une liste de processus dotés de priorités, affecte d'abord aux plus prioritaires les ressources disponibles. Stratégies possibles. chemin critique, plus long chemin, plus haut niveau d'abord, plus long temps de traitement.

Multi level feedback queue

- Rate-monotonic scheduling - Algorithme optimal, préemptif, à priorité statique. Priorité

donnée selon un principe de taux monotonique (le premier à finir est le premier traité).

- Round-Robin scheduling - Le plus simple, assigne des tranches de temps à chaque processus sans priorité.
- Shortest job next - Exécute ensuite le processus en attente qui a le temps d'exécution le plus court, sans préemption.
- Shortest remaining time - Une version de minutage du plus court processus à venir, qui termine la tâche en court avant d'en choisir une autre.

CRYPTOGRAPHIE

Cryptographie à clé secrète (symétrique)

Utilise une clé secrète ou une paire de clés liées, à la fois pour l'encryptage et le décryptage.

- Advanced Encryption Standard - AES est égalementconnu sous le nom de Rijndael.
- Blowfish - Conçu par Schneir comme algorithme d'usage général, pour remplacer le DE vieillissant.
- Data Encryption Standard (DES) - Anciennement DE Algorithm.
- IDEA - nternational Data Encryption Algorithm, anciennement IPES, remplace aussi DES. Utilisé par PGP (Pretty Good Privacy). Effectue des transformations sur les données découpées en bloc, en utilisant une clé.
- RC4 (or ARC4) - Chiffrage de flux très utilisé, notamment par le protocole SSL pour le traffic Internet et WEP pour les réseaux sans fil.
- Tiny Encryption Algorithm - Algorithme sur blocs de données facile à implémenter, utilisant quelques formules.

Cryptographie à clé publique (asymétrique)

Utilise une paire de clés, dites clé publique et clé privée. La clé publique crypte le message,

seule la clé privée permet de le décrypter.

- DSA (Digital Signature Algorithm). Génère des clés avec des nombres premier et aléatoires. Etait utilisée par les agences US, et maintenant dans le domaine public.
- ElGamal. Basé sur Diffie-Hellman, utilisé par GNU Privacy Guard software, PGP, et autres systèmes de cryptographie.
- RSA(Rivest, Shamir, Adleman). Largement utilisé dans le commerce éléctronique. Utilise des nombres premiers.
- Diffie-Hellman (Merkle) key exchange (ou échange exponentiel key). Méthode et algorithme pour échanger du contenu secret par un canal de communication non protégé. Utilisé par RSA.
- NTRUEncrypt. Utilise des anneaux polynomiaux avec multiplications convolutives.

Générateur de code

- MD5. Utilisé pour tester les images ISO des CD ou DVD.
- RIPEMD (RACE Integrity Primitives Evaluation Message Digest). Basé sur les principes de MD4 et similaire à to SHA-1.
- SHA-1 (Secure Hash Algorithm 1). Le plus utilisé dans l'ensemble des fonctions de hachâge cryptographique SHA. A été conçu par l'agence américaine NSA.
- HMAC. Authentication de message par clés de hachage.
- Tiger (TTH). Utilisé dans le hachage "Tiger tree".

Cryptographie sécurisé utilisant des nombres aléatoires

- Secret sharing - Secret Splitting, Key Splitting, M of N.
- Shamir's secret sharing - C'est une formule basée sur une interpolation polynomiale.
- Blakley's secret sharing - Est géométrique, le secret est un point dans un espace à m dimensions.

Autres techniques de cryptographie

- Algorithme de Shor - Algorithme quantique supposé capable de décrypter un code basé sur les fonctions asymétriques tel que RSA.
- Maximum de Vraisemblance à Posteriori - MVP - Technique permet de traduire un code arithmétique.

- Subset sum. Un ensemble d'entiers étant donné, y a-t'il un sous-ensemble dont la somme fasse zéro? Utilisé en cryptographie.
- Arithmétique modulaire

Générateurs de nombres aléatoires

- Blum Blum Shub. Basé sur une formule utilisant des nombres premiers.
- Mersenne twister. Par Matsumoto Nishimura, rapide, a une périodicité très longue.
- Lagged Fibonacci generator. Améliore le générateur à congruence linéaire en utilisant la séquence de Fibonacci.
- Linear congruential generator. Un des plus anciens, non le meilleur, génère une séquence à partir de trois nombres.
- Yarrow algorithm. Par Bruce Schneier, John Kelsey, and Niels Ferguson. Générateur cryptographiquement sûr, peut être utilisé pour générer des nombres réellement aléatoires à partir d'entrées de périphériques analogiques.
- Fortuna. Présenté comme une amélioration de l'algorithem de Yarrow.
- Linear feedback shift register. Registre à décalage dont l'entrée est une fonction linéaire de son contenu précédent. Le contenu initial est le "seed" (grain).

CALCUL SCIENTIFIQUE

- Algorithms for Recovery and Isolation Exploiting Semantics.
- Unicode Collation. Fournit un moyen standard de placer des noms, mots ou chaines de caractères dans une séquence donnée.
- CHS conversion. Conversion entre les systèmes d'addressages sur disques.
- Cyclic redundancy check. Calcul de mots de contrôle.
- Parity control. Technique de detection d'erreur élémentaire. un nombre est-il pair ou impair?

Geométrie

- Gift wrapping. Détermine l'enveloppe convexe d'un ensemble de points.
- Gilbert-Johnson-Keerthi distance. Trouve la plus courte distance entre deux formes convexes.
- Graham scan. Détermine l'enveloppe convexe d'un ensemble de points sur un plan.
- Line segment intersection. Trouve quelles lignes sont en intersection avec une ligne imaginaire.
- Points dans un polygone.
- Ray/Plane intersection. Intersection de rayons avec un plan.
- Line/Triangle intersection. Cas particulier de Ray/Plane.
- Polygonisation de surfaces implicites. Approxime une surface implicite par une représentation en polygones.
- Triangulation. Méthode pour évaluer une distance ou déterminer les propriétés d'un espace topologique.

Graphes

- Bellman-Ford - Calcule les plus courts chemins dans un graphe.
- Canonisation de graphes. Consiste à trouver la forme canonique d'un graphe de sorte qu'il soit isomorphique à un autre graphe. S'utilise en chémoinformatique.
- Dijkstra's algorithm. Calcule les plus courts chemins dans un graphe sans arc de valeur négative.
- Perturbation methods. Calcules les plus courts chemins dans un graphe.
- Floyd-Warshall. Résoud le problème de plus court chemin dans un graphe orienté et valué.
- Floyd's cycle-finding. Algorithme itératif qui détecte les cycles.
- Hopcroft–Karp algorithm. A partir d'un graphe bipartie, retourne le maximum de cotés sans points communs. Les alternatives sont les algos breadth-first et depth-first.

- Johnson. Plus court chemin dans un graphe orienté valué.
- Kruskal. Trouve l'arbre de parcours minimum d'un graphe.
- Prim. L'algorithme de Robert Prim trouve l'arbre de parcours minimum d'un graphe. Aussi appelé DJP , Jarník ou Prim–Jarník.
- Boruvka. Comme Kruskal.
- Ford-Fulkerson. Calcule le flot maximum passant dans un graphe.
- Edmonds-Karp. Implémentation de Ford-Fulkerson.
- Nonblocking Minimal Spanning Switch. Echanges téléphoniques.
- Woodhouse-Sharp. Trouve l'arbre de parcours minimum d'un graphe.
- Spring based. Algorithme de dessin de graphe.

- Hungarian. Trouve une correspondance parfaite.

Coloration d'un graphe

- Nearest neighbour. Recherche du plus proche voisin.
- Topological sort. Classement d'un graphe orienté acyclique de façon que chaque noeud précède les noeuds auxquels il est lié (selon le sens des arcs).
- Tarjan's off-line least common ancestors algorithm. Calcule les ancêtres communs les plus proches à des paires de noeuds dans un arbre.

SIMULATEUR

Graphisme

- Bresenham's line. Utilise des variables de décision pour afficher un ligne entre deux points.
- Colorisation. Procédé pour colorer une image ou une vidéo en noir et blanc, avec quelques traits pour marquer les couleurs. Exemples.
- Depixélisation. Sous le nom original de "Depixelizing Pixel Art", cet algorithme de lissage convertit une image en pixels grossiers en une image réaliste. (Johannes Kopf et Dani Lischinski). Démonstration. Archive des démos.

Landscape

- DDA line algorithm. Utilise les mathématiques en virgule-flottante pour dessiner une ligne entre deux points.

- Flood fill. Colorie une zone délimitée par par une ligne fermée.
- Image Restoring. Restore des photos, améliore des images.
- Xiaolin Wu's line algorithm. Algorithm d'anti-aliasing de ligne.
- Painter's algorithm. Détecte les parties visibles d'une scène en 3D.
- Ray tracing. "Rendering", tracé d'image réaliste.
- Phong shading. En 3D, crée un éclairage.
- Gouraud shading. Simule les effets de liumière et couleurs sur la surface d'un objet en 3D.

- Scanline rendering. Construit une image en déplaçant une ligne imaginaire.
- Global illumination. Reconstitue l'éclairage direct et réfléchi par d'autres objets.
- Interpolation. Construit de nouveau point sur une image agrandie.
- Resynthesizer. Enlève un objet sur une photo en reconstituant le fond. Utilisé par Photoshop et The Gimp. Tutoriel resynthesizer.
- Slope-intercept algorithm. C'est une implémentation de la formule slope-intercept pour dessiner une ligne.
- Spline interpolation. Réduit les erreurs avec le phénomène de Runge.
- 3D Surface Tracker Technology. Procédé pour ajouter des images sur les murs dans une vidéo en tenant compte des surfaces cachées.

CHAMPION DU MONDE

Intelligence artificielle

- Alpha-beta. Alpha max plus beta min. Utilisé pour les jeux de tableaux notamment.
- Analyse des syntiments. En fait une combinaison des algorithmes de Bayes, entropie maximale et SVM (machine à support de vecteur).
- Colonies de fourmis. Ensemble d'algorithmes basés sur le comportements des fourmis qui parviennent à une optimisation pour résoudre un problème.
- DE (Differential evolution). Résoud le problème polynomial de Chebyshev.
- Semi-Supervised Recognition of Sarcastic Sentences in Online Product Reviews. Un algorithme qui reconnaît le sacarsme ou l'ironie dans un tweet ou un document en ligne. Un tel algorithme sera aussi essentiel pour la programmation des robots humanoïdes.

Vision par ordinateur

- Epitome. Représente une image ou une vidéo par une plus petite.
- Compte d'objets dans une image. Utilise l'algorithme des composants connectés pour définir d'abord chaque objet, et compter les objets.
- Algorithme de O'Carroll. A partir d'une conversion en mathématique de la vision des insecte, cet algorithme évalue comment se déplacer en évitant les objets.

Algorithmes génétiques

- Fitness proportionate selection. Nommé aussi roulette, sélectionne des solutions.
- Truncation selection. Sélectionne des solutions classées par pertinence.
- Tournament selection. Sélectionne la meilleur solution par une sorte de tournoi.
- Stochastic universal sampling. Les individus sont associés aux éléments contigus d'une ligne de sorte que chacun ait une taille qui lui corresponde.

Réseaux de neurones

- Réseau de Hopfield. Réseau neuronal récurrent qui fonctionne comme une mémoire adressable binaire. Il converge vers un état stable.
- Backpropagation. Technique d'apprentissage aidée pour entraîner des réseaux de neurones artificiels.
- Self-organizing map (Kohonen map). Réseaux de neurones entraînés en utilisant un apprentissage autonome pour produire une représentation en basse dimensions (2D, 3D) des exemples donnés à apprendre.