1 Exemples

Dans une base de données, **l'information est stockée dans des fichiers**, mais ceux-ci ne sont en général pas lisibles par un humain : ils nécessitent l'utilisation d'un **Système de Gestion de Bases de Données Relationnelles (SGBD)** pour les exploiter.

Parmi les logiciels de gestion de bases de données les plus connus, on trouve :

Dans le domaine du libre :
- mariaDB / mySQL
- postgreSQL

Dans le monde propriétaire, les plus connus sont :
- IBM DB2
- Oracle Database
- Microsoft SQL Server

Ce sont de très gros logiciels, fonctionnant en mode client/serveur, assez complexes à mettre en œuvre et à utiliser. Ils sont conçus pour gérer plusieurs millions d'enregistrements de manière fiable et sécurisée. Leur architecture côté serveur est prévue pour être répartie sur plusieurs machines et ainsi permettre une tenue en charge lorsqu'un grand nombre de requêtes parviennent.

En ce qui nous concerne, nous utiliserons cette année un outil libre simple à mettre en œuvre mais permettant tout de même de se familiariser avec la gestion des bases de données et le langage SQL : **SQLite**. Nous exploiterons aussi **DB Browser** qui offre une interface graphique d'exploitation d'une base au format SQLite.
Des outils Online sont aussi disponibles.

2 Rôles d'un SGBD

Le rôle d'un SGBD est évidemment de permettre la consultation et la mise à jour d'une base de données, mais de façon tout aussi importante son rôle est d'**assurer l'intégrité de la base** et d'**optimiser** son exploitation.

Les SGBD permettent en particulier :
- de **lire, écrire, modifier, effacer**, **mettre en relation** des données dans les différentes tables.
- de gérer les **utilisateurs** ayant accès aux données.
- de gérer les **droits d'accès** aux différentes données.
- d'assurer la **sécurité et l'intégrité des données** y compris lorsque plusieurs utilisateurs accèdent simultanément aux mêmes données, ou en cas de pannes.

Compléments : on pourra lire la BD manga sur les bases de données (dispo au CDI) pour avoir plus de détails sur ces fonctionnements.

2.1 Persistance des données

L'importance des données peut être évidemment capitale (ex : base de données d'une banque) et les données contenues dans la base ne doivent pas être perdues en cas de fausse manipulation ou de pannes. Des dispositifs de **sauvegardes pour la persistance des données** doivent donc être assurés par le SGBD.

2.2 Gestion des accès concurrents

Plusieurs utilisateurs sont en général susceptibles d'interagir avec une base de données.
Il peut y avoir des accès concurrents à la base : 2 utilisateurs cherchent à effectuer des modifications simultanément sur les mêmes données de la base. Si ces accès ne sont pas trop gênants en lecture, ils seraient dramatiques en écriture ! Un ensemble d'opérations effectuées sur une base s'appelle une **transaction** et le SGBD, en s'appuyant sur un **système de verrous**, permet d'assurer que 2 transactions concurrentes ne peuvent être validées en même temps.

2.3 Efficacité de traitement des requêtes

Les requêtes pour interagir avec une base sont effectuées dans le langage SQL [*voir P2.IV*]. Ces requêtes sont assez proches d'un langage naturel mais plusieurs algorithmes d'interaction avec la base peuvent être mis en œuvre pour répondre à une requête donnée. En fonction de la nature de la requête et de l'état de la base, certains algorithmes sont plus efficaces que d'autres. C'est le rôle du SGBD de s'**assurer d'une optimisation du traitement des requêtes**.

Remarque : Pour l'accès rapide aux données certains algorithmes s'appuient sur la construction d'index, implémentés sous formes d'arbres ou de tables de hachage.

2.4 Sécurisation des accès

Puisque différents utilisateurs peuvent interagir avec la base, le SGBD doit **définir les droits d'accès en lecture ou écriture aux différentes données de la base** (des accès partiels sont possibles) pour **augmenter la sécurité** et limiter les risques de corruption de la base.

Exemple : L'administrateur de la base de données d'une banque ne doit pas avoir les mêmes droits qu'un client de la banque. Et un certain client ne doit pas pouvoir accéder aux données concernant un autre client !