数据库设计说明书

一、引言

1.1 编写目的

1、本数据库设计说明书是关于图书挂阅读打卡数据库设计，主要包括数据逻辑结构设计、数据字典以及运行环境、安全设计等。

2、本数据库设计说明书读者：用户、系统设计人员、系统测试人员、系统维护人员。

3、本数据库设计说明书是根据系统需求分析设计所编写的。

4、本系统说明书为开发软件提供了一定基础。

1.2 背景

高校学生去图书馆的频率两极分化，通过问卷调查我们发现增加图书馆打卡功能可以促进学生多去图书馆多阅读，形成良好的习惯，而利用微信小程序来做这个功能，把常用的 app 微信和本校图书馆结合起来，是很方便用户的事情。既有当今时代大数据、云计算的现代感，又时刻提醒我们不要忘记静心读书。图书馆打卡小程序--悦读打卡主要有有登录注册、打卡提醒、定位打卡、打卡周报、打卡排行榜几个功能，可以很好地提高学生用户对图书馆的利用率。

1.3 定义

本文件中绝大多数字段为驼峰式命名法。

1.4 参考资料

1.数据库表结构设计的几条准则

https://www.cnblogs.com/wyq178/p/8549715.html

2.数据库表设计（一对多、多对多）

https://blog.csdn.net/fighteryang/article/details/82848505

3.数据库设计说明书-国家标准格式

https://wenku.baidu.com/view/fcccbc331688848686 62d625.html

二、外部设计：

2.1 标识符和状态

数据库软件的名称：MySQL

数据库的名称为：悦读打卡

2.2 使用它的程序

微信小程序

2.3 约定

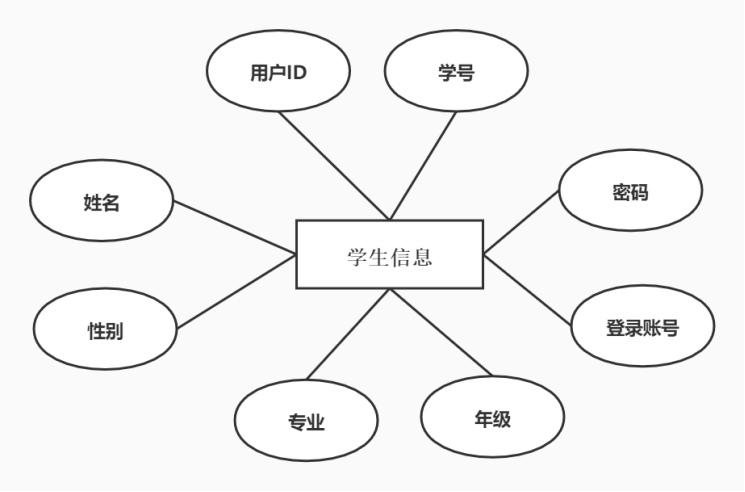
命名约定：所以的数据库命名都是以模块的具体表的英文词汇组成,这样能够统一数据库表的命名，也能够更好的规范数据库表命名的作用。

设计约定：在本系统中，数据库的设计采用面向对象的设计方法，首先进行对象实体的设计，最后将对象持久化到数据库中。所有数据表第一个字段都是系统内部使用主键列，自增字段，不可空，名称为 id。

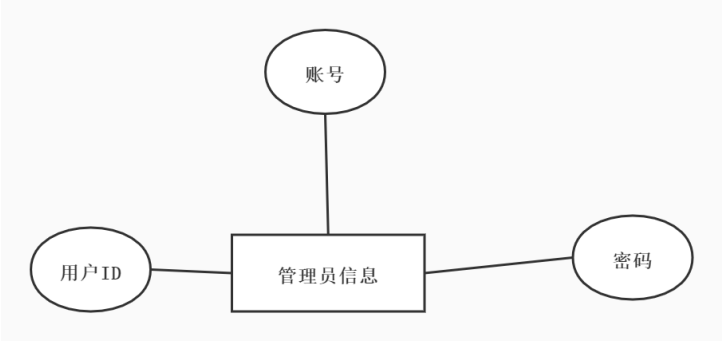
三、结构设计

3.1 概念结构设计

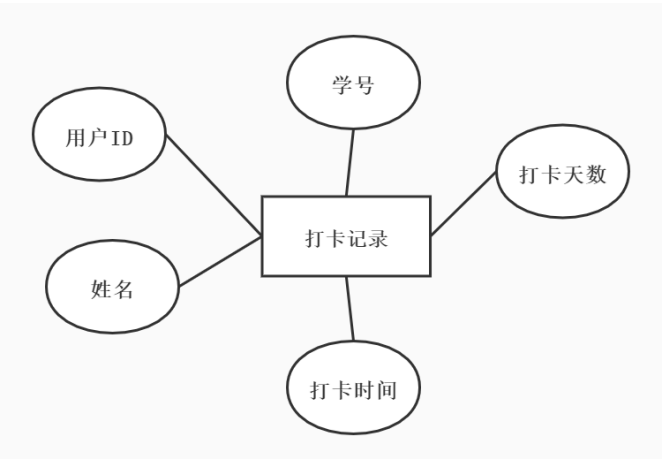
学生信息(用户 ID、学号、姓名、性别、专业、年级、登录账号、密码)



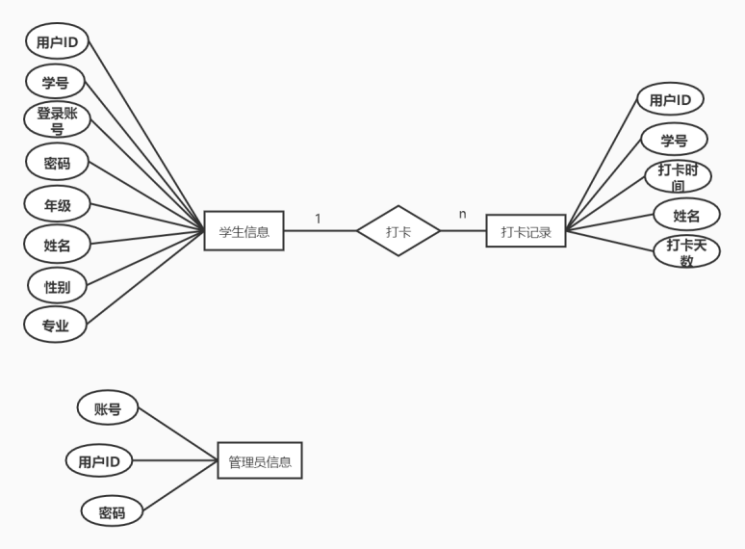
管理员信息（用户 ID、账号、密码）



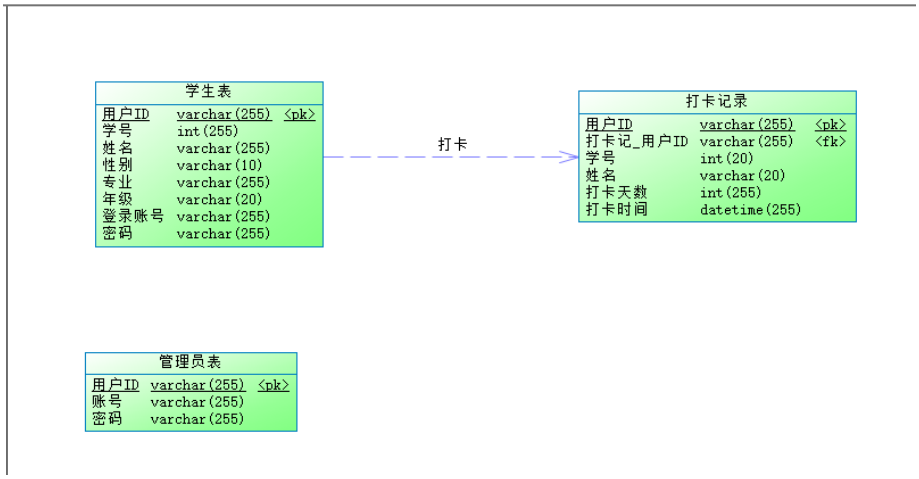
打卡记录（用户 ID、打卡天数、姓名、学号、打卡时间）



完整 E-R 图

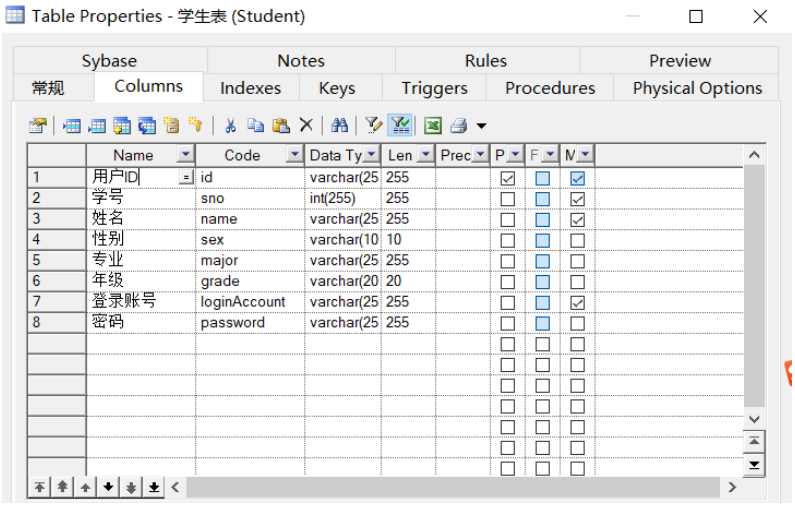


3.2 逻辑结构设计

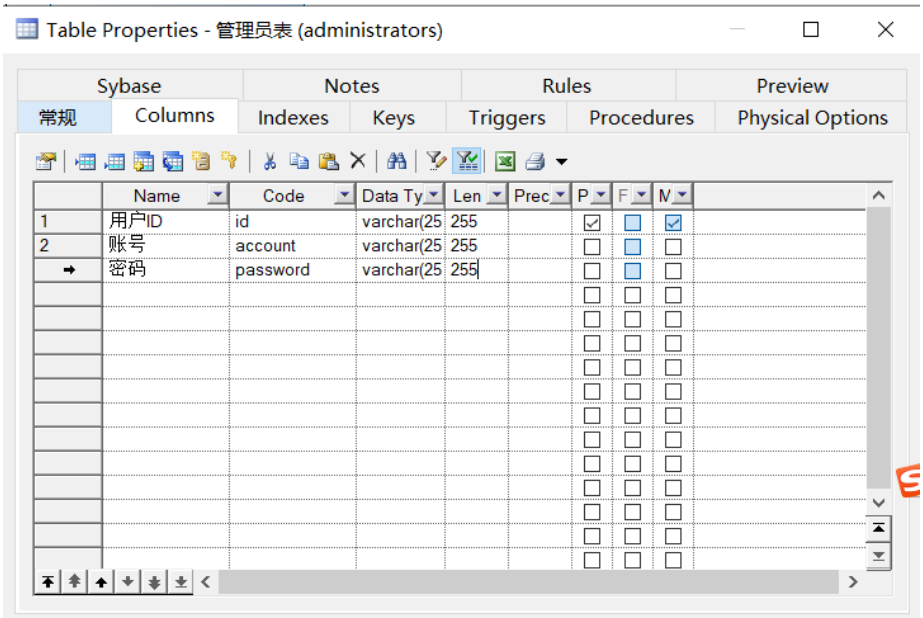


3.3 物理结构设计

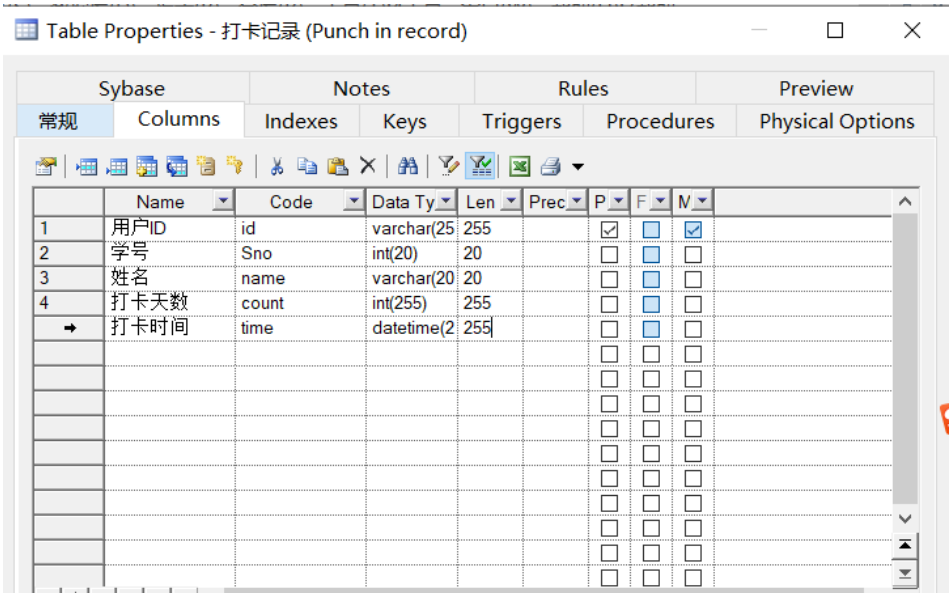
学生物理结构设计



管理员物理结构设计



打卡记录



四、运用设计

4.1 安全保密设计

只允许有资格的指定用户去访问数据库中指定的表或数据，主要通过数据库系统的存取控制来实现。此要求的目的是将用户权限等级到数据字典中。用户只访问他有权访问的数据。每当用户进行数据的增删改查等操作时，先对其进行操作权限的检查，若此用户的操作权限超出了系统定义的权限，系统将拒绝用户执行此操作。

不同类型的用户授予不同的数据管理权限。我们将允许操作的权限分为三类：

1、数据库登录权限类：有数据库登录权限的用户可以进入数据库管理系统，进入管理系统后，可以使用数据库管理系统所提供的各类工具和实用程序。同时，数据库的主人

可以授予此类用户数据查询、建立视图等权限。这类用户只能进行数据库信息的查询，不能对信息做出任何的改动。

2、资源管理权限类：具有资源管理权限的用户，拥有上一类的用户所拥有的所有权限，除此之外，还有创建数据库表、索引等数据库的权限，可以在权限允许的范围内修改、查询数据库，还能将自己拥有的权限授予其他用户。

3、数据库管理员权限类：具有数据库管理员权限的用户将具有数据库管理的一切权限，包括访问用户的所有数据，授予或回收用户的各种权限，创建各种数据库，完成数据库的整库备份、装入重组等工作。这类用户的权限是数据库用户的最高权限，一般只有数据库的管理人员可以有。

五、数据库验证验收标准

5.1 数据库数据体的验收

1. 保证每列的原子性，即要符合第一范式。
2. 表中记录应该有唯一的标识符。
3. 尽量只存储单一实体类型的数据。

5.2 数据库安全性的验收

1. 用户识别和鉴别：该方法由系统提供一定的方式让用户标识自己的 ID，每次用户进入系统时，由系统进行核对，鉴定通过后才能提供系统的使用权。
2. 存取控制:通过用户权限定义和合法权检查确保只有合法权限的用户访问数据库，所有未被授权的人员无法存取数据。
3. 视图机制:为不同的用户定义视图，通过视图机制把要保密的数据对无权存取的用户隐藏起来，从而自动地对数据提供一定程度的安全保护。
4. 审计:建立审计日志,把用户对数据库的所有操作自动记录下来放人审计日志中，DBA 可以利用审计跟踪的信息，重现导致数据库现有状况的一系列事件,找出非法存取数据的人、时间和内容等。
5. 数据加密:对存储和传输的数据进行加密处理，从而使得不知道解密算法的人无法获知数据的内容。