格与密码学的问题

1. 什么是格?
2. 格与子空间的区别是什么?
3. 欧氏空间正交化算法的输入与输出分别是什么?
4. 欧氏空间正交化算法的不变量或不变式是什么?变化的是什么？
5. 分析欧氏空间正交化算法的复杂度。
6. 比较格中最短向量问题与码中最小重量码字问题。
7. 简述Babai算法的输入、输出、设计思路。
8. 分析Babai算法的复杂度。
9. 简述GGH密码体制。
10. 简述NTRU密码体制。
11. 格基归约算法的不变式是什么？变化的是什么？