量子计算理论基础与软件系统实验报告

课程名称：	量子计算理论基础与软件系统
作业名称：	Lab 3 Shor and Grover Algorithm
姓　　名：	周楠
学　　号：	3220102535
电子邮箱：	3220102535@zju.edu.cn
联系电话：	19858621101
指导教师：	卢丽强

2024 年 11 月 22 日

一. 实验目的和要求

本次实验中，我们将使用 ‘qiskit‘ 框架实现 Shor 算法和 Grover 算法，并通过量子电路的模拟运行加深对这两个核心量子算法的理解。

二. 实验环境

```
conda create -n quantum python=3.10
conda activate quantum
conda deactivate
conda env remove -n quantum
```

三. 实验流程

3.1 Shor 算法代码分析

1. 补全 ‘mod_circuit‘ 函数中量子门 U 对应的酉矩阵定义，以构造量子门 U。

```python
def mod_circuit(a, N, n_v):
    """
    Create a quantum circuit for modular multiplication: |x  -> |
        ax mod N
    """
    matrix = np.zeros((2 ** n_v, 2 ** n_v), dtype=complex)

    # Fill the matrix with the modular multiplication results
    for x in range(2 ** n_v):
        # 如果x小于N, 则计算(a*x) mod N
        if x < N:
            y = (a * x) % N
            matrix[y, x] = 1
            # matrix[x, y] = 1
        else:
            matrix[x, x] = 1

    # Create and return a unitary gate from the matrix
    return UnitaryGate(matrix)
```

2. 运行补全的代码，取 $a = 7$，分解整数 $N = 15$，观察输出的计数结果，验证分解结果是否正确。

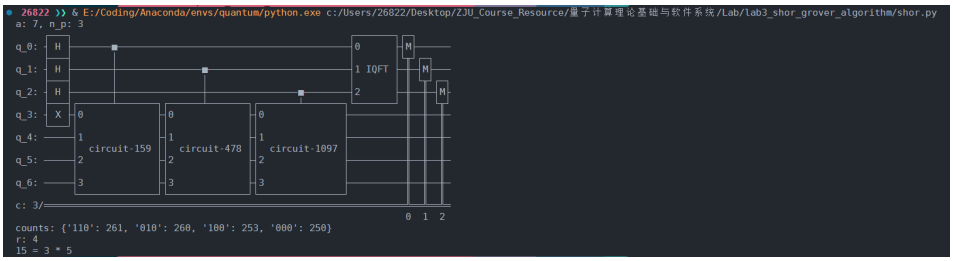

图 1: Shor 算法结果

3. 修改代码中的部分参数，选取合适的 a，分解整数 $N = 21$。采用遍历 a 和 n_p 的方法，观察输出结果，验证分解结果是否正确。

```
for a in range(2, N):
    if np.gcd(a, N) == 1:
        for n_p in range(2, 5):
            print(f"a: {a}, n_p: {n_p}")
            qc = shor_circuit(N, a, n_p, n_v)
            print(qc.draw())
            ...
```

最终发现当 $a = 8$ 时，$n\_p = 2$ 或者 $n\_p = 3$ 时，$N = 21$ 可以被分解为 3×7。

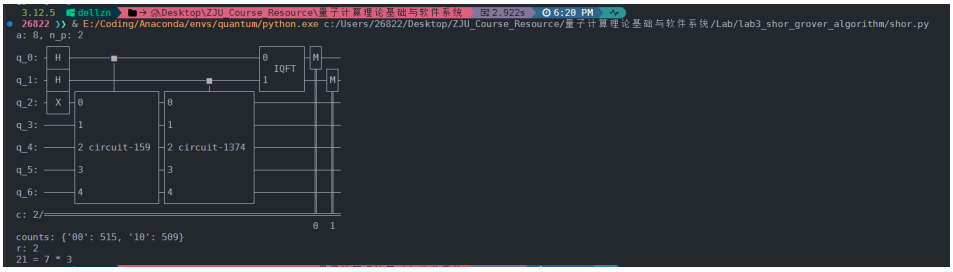

图 2: Shor 算法结果

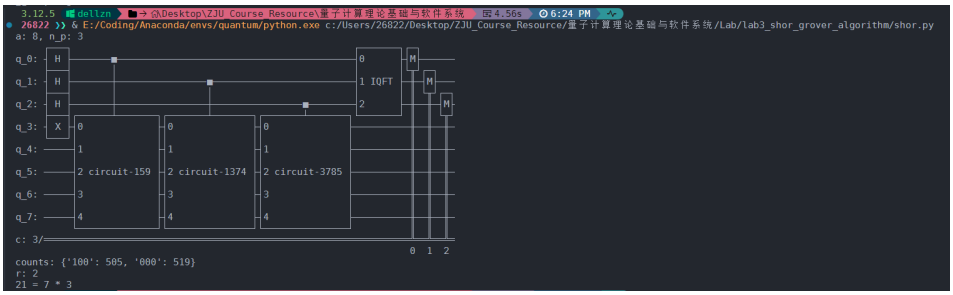

图 3: Shor 算法结果

四. 遇到的困难及解决方法

在对 $N=21$ 进行分解时，发现当 $a=2$ 时，理想状态下，希望得到 $r=6$, 这样就能实现 $2^6 \mod 21=1$，从而分解 21。但是实际运行时，不管如何设置 n_p，都无法得到 $r=6$。

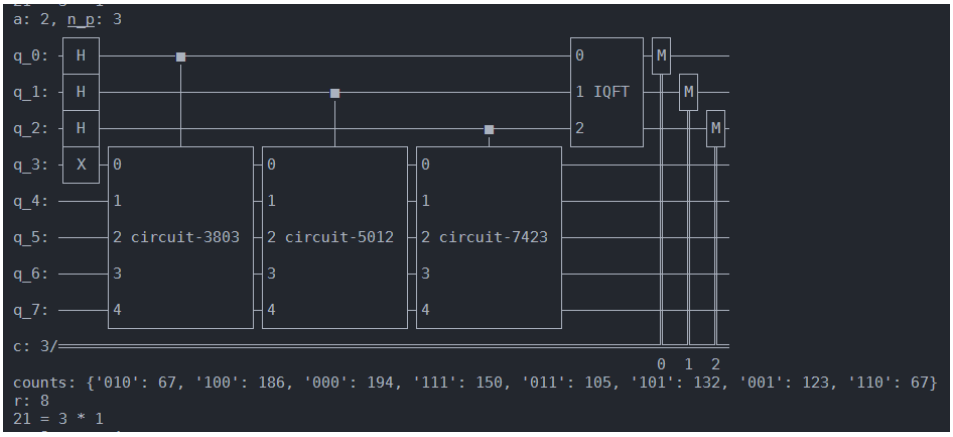

图 4: Shor 算法结果

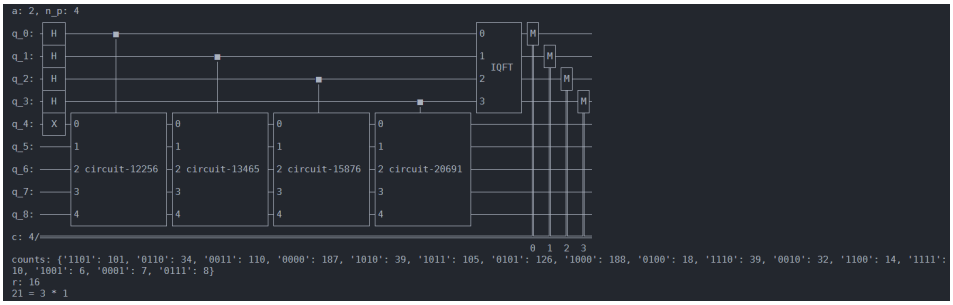

图 5: Shor 算法结果

我一度怀疑是自己算法写错了，但为了多次测试，我才用循环遍历 a 和 n_p 的方法，最终发现当 $a=8$ 时，$n\_p=2$ 或者 $n\_p=3$ 时，$N=21$ 可以被分解为 3×7。成功解决问题。

五. 总结与心得

本次实验也算是实操了 Shor 算法，原先对 Shor 算法只是停留在理论层面，只是听说过使用量子 shor 算法能够加快质因数分解。后面在理论的学习中，原来量子 shor 算法加快的是求解阶的问题，根据计算出来的阶，就能分解整数。也算是在实操中加深了对 Shor 算法的理解。