1.1 Exercises

1.1.1 Test of commutativity

Problem

Input

• Group G

• Function $\circ$ gives the product of two elements.

• n elements of G $h_1, h_2, ..., h_n$ and H, the generated group.

Output ACCEPT iff H is a commutative group

Complexity Number of operations involving $\circ$.

Naive solution Checking all possible couples $(i, j) \in G^2$ requires $O(n^2)$ operations.

Algorithm

• Draw $k, l$ with Sampling at random from H.

• Accept iff. $k \circ l = l \circ k$

Complexity One call to Sampling, two calls to $\circ$

Performance One sided error :

• H commutative group $\Rightarrow$ ACCEPT always

• H non commutative group $\Rightarrow$ ACCEPT with probability inferior to 3/4

Property H is commutative iff $\forall i, j; h_i \circ h_j = h_j \circ h_i$ (the generators commute)

Lemma 1.1. if H is not commutative then

• $\exists i, j$ for which $h_i \circ h_j \neq h_j \circ h_i$

• $\mathbb{P}_{k, l \in H} (k \circ l \neq l \circ k) \geq 1/4$
Proof: the center of H is defined as follow:
\[ Z(H) = \{ k \in H | \forall l \in H, k \circ l = l \circ k \} \]
Moreover,
\[ S(k) = \{ l \in H | k \circ l = l \circ k \} \]
So if \( S(k) = H \) then \( k \in Z(H) \).
\( Z(H) \) is a strict sub group of \( H \), so using the Lagrange theorem:
\[ |Z(H)| \leq \frac{1}{2} |H| \]
Therefore,
\[ \mathbb{P}_{k \in H} (k \in Z(H)) \leq \frac{1}{2} \]
Let \( k \in H \setminus Z(k) \)
Also, \( S(k) \) is a strict sub group of \( H \),
\[ |S(k)| \leq \frac{1}{2} |H| \]
Therefore,
\[ \mathbb{P}_{l \in H} (l \in S(k)) \leq \frac{1}{2} \]
Finally,
\[ \mathbb{P}_{k, l \in H} (k \circ l \neq l \circ k) = \mathbb{P}_{k, l \in H} (k \circ l \neq l \circ k \cap k \notin Z(H)) \]
\[ = \mathbb{P}_{k, l \in H} (k \notin Z(H) \cap k \notin S(k)) \]
\[ \mathbb{P}_{k, l \in H} (k \circ l \neq l \circ k) = \mathbb{P}_{k, l \in H} (k \notin Z(H)) \cdot \mathbb{P}_{k, l \in H} (k \notin S(k) | k \notin Z(H)) \]
\[ = \mathbb{P}_{k, l \in H} (k \circ l \neq l \circ k) \geq \frac{1}{2} \cdot \frac{1}{2} \]
\[ \geq \frac{1}{4} \]
CQFD

Note We have demonstrated that the algorithm is a Monte-Carlo algorithm, with a one sided error of 1/4.
We still have to explain the Sampling process, which choose randomly \( k, l \in H \)

Weak Sampling
- Draw \( r \) uniformly from \( \{0, 1\}^n \)
- Calculate and return \( h_1^r \cdot \ldots \cdot h_n^r \)
Example

- \( n = 4 \)
- draw 0110
- return \( h_2 \cdot h_3 \)

Complexity  \( n \) group operation \( \circ \)

Lemma 1.2. If \( K \) is a strict subgroup of \( G \), and \( h_1 \ldots h_n \) the generators of \( K \) then

\[
\mathbb{P}_{h \text{ with Weak Sampling}}(h \in K) \leq 1/2
\]

Proof: Since \( K \neq G \), \( \exists \ i \) such as \( h_i \notin G \)

Remember : we draw \( r \) uniformly from \( \{0, 1\}^n \).

\[ h = h_1^{r_1} \cdot \ldots \cdot h_n^{r_n} \]

Fix \( r \) except \( r_i \)

Suppose \( i = 1 \)

\[ \beta = h_2^{r_2} \cdot \ldots \cdot h_n^{r_n} \]

\[ \mathbb{P}_{r_i \in \{0,1\}} (h \in K) = \mathbb{P}_{r_i \in \{0,1\}} (h_1^{r_1} \cdot \beta \in K) \]

- \( \beta \in K \)
  - \( r_1 = 1 \Rightarrow h_1 \cdot \beta \notin K \) (if \( h_1 \cdot \beta \in K \) then \( h_1 \in K \Rightarrow \) Contradiction)
  - \( r_1 = 0 \Rightarrow h = \beta \in K \)

\[ \mathbb{P}_{r_i \in \{0,1\}} (h \in K | \beta \in K) = 1/2 \]

- \( \beta \notin K \)
  - \( r_1 = 1 \Rightarrow \) unknown
  - \( r_1 = 0 \Rightarrow h = \beta \notin K \)

\[ \mathbb{P}_{r_i \in \{0,1\}} (h \in K | \beta \notin K) \leq 1/2 \]

Consequently

\[ \mathbb{P}_{r_i \in \{0,1\}} (h \in K |) \leq 1/2 \]

To generalize to all \( i \), take

\[ i = \min \{ j, h_j \notin K \} \]

Set \( \eta = h_1^{r_1} \cdot \ldots \cdot h(j-1)^{r_{j-1}} \) and adapt the proof.

Finally, using the conditional probability on \( r_1, \ldots, r_n \) except \( r_j \), we reach the conclusion :

\[ \mathbb{P}_{r_i \in \{0,1\}^n} (h \in K) \leq 1/2 \]

CQFD
Complexity Finally the algorithm requires $O(n)$ against the $O(n^2)$ of the naive method.

1.1.2 Determinist Algorithm to Probabilistic Algorithm

Problem

Input

- Deterministic algorithm $P$ which return the product of two matrix

$$P(A,B) \neq A \cdot B \leq 1/9$$

- $\delta$

Output Probabilistic algorithm $P_2$ such as

$$\text{Err}(P) = \mathbb{P}_{A,B \text{ matrix modulo } N}(P_2(A,B) \neq A \cdot B) \leq \delta$$

Complexity The algorithm must require $O(n^2)$ additions/multiplications and $(O(\log \delta))$ call to $P$

Questions

1. Prove that $\forall R,S$ matrix modulo N

$$A \cdot B = (A - R) \cdot (B - S) + (A - S) \cdot S + R \cdot (B - S) + R \cdot S(*)$$

2. Deduce the probabilistic algorithm

3. Write an algorithm which requires $O(n^2)$ additions/multiplications and $(O(\log \delta))$ call to $P$ such as

   - If $\text{Err}(P) = 0$ then $\mathbb{P}(\text{Algo accept}) = 1$
   - If $\text{Err}(P) \leq 1/11$ then $\mathbb{P}(\text{Algo accept}) \geq 1 - \delta$
   - If $\text{Err}(P) \geq 1/9$ then $\mathbb{P}(\text{Algo reject}) \geq 1 - \delta$
   - If $1/11 \leq \text{Err}(P) \leq 1/9$ then non specified

Answers

1. Develop

2. Choose uniformly at random two matrix $R$ and $S$ modulo $N$

   - Calculate and return $(*)$ with $P$
Proof:

\[ \mathbb{P}(\mathcal{P}(\mathcal{*}) = A \cdot B) = \mathbb{P}(P(A - R, B - S) \neq (A - R) \cdot (B - S)) \]

or \( (P(A - R, S) \neq (A - R) \cdot S) \)

or \( (P(R, B - S) \neq R \cdot (B - S)) \)

or \( (P(R, S) \neq R \cdot S)) \)

\[ \mathbb{P}(\mathcal{P}(\mathcal{*}) = A \cdot B) \leq 4\text{Err}(P) \]

\[ \mathbb{P}(\mathcal{P}(\mathcal{*}) = A \cdot B) \leq 4/9 \]

\[ \square \]

**Note** Choosing randomly \( R \) and \( S \) is the same thing as choosing randomly \( A-R \) and \( B-S \) because we work modulo \( N \)

3. • Do \( k \) times:
   - Choose \( A, B \) randomly
   - Verify \( P(A, B) = A \cdot B \) with Friedvalds algorithm done multiple times
   - \( X_i = 0 \) if there is no mistake
   - \( X_i = 1 \) if any mistake

• if \( \sum X_i \leq \frac{k}{10} \) then ACCEPT
  else REJECT

**Proof:** Try using the Chernoff Bound