3.1 The Zero-Knowledge Property

a) We prove that both protocols are c-simulatable and have the (obviocdusly) polynomially-bounded challenge space \( C = \{0, 1\} \). Then, they are honest-verifier zero-knowledge, and, by Theorem 3.1 in Section 3.3.2 of the course notes, they are perfectly zero-knowledge.

Consider the a single round between \( P \) and the honest \( V \) (for either protocol). Let \( P_{TCR}(t,c,r) \) be the distribution of the triple \((t,c,r)\) they produce. To prove c-simulatability one has to show that, for both challenges \( c \in \{0, 1\} \), one can efficiently sample \( T \) and \( R \) such that \((T,R,c) \sim P_{TRC}(|\cdot|,|\cdot|,c)\).

- **Fiat-Shamir:** In an actual execution for the instance \( z = x^2 \), \( t \) is a random quadratic residue since it is chosen as \( t = k^2 \) for a random \( k \in \mathbb{Z}_m^* \), and \( r \) is computed as \( r = kx^c \). Note that \( r \) is computed bijectively from a random \( k \) and, therefore, choosing \( r \) randomly and computing \( k = rx^{-c} \) and \( t = k^2 \) results in the same distribution. To avoid having to know the witness \( x \), one simply chooses \( r \) randomly and directly computes \( t = r^2z^{-c} \).

- **Graph Isomorphism:** Let \((G,H)\) be the instance. Given \( c \in \{0, 1\} \), proceed as follows: Choose a random permutation \( \rho \). If \( c = 0 \), set \( T := \rho G \rho^{-1} \); if \( c = 1 \), set \( T := \rho H \rho^{-1} \). In both cases, the resulting triple \((T,c,\rho)\) has the desired distribution, i.e., when \( c = 0 \), then \( T = \rho G \rho^{-1} \) is a random permutation of \( G \), and when \( c = 1 \), then \( T = \rho H \rho^{-1} \) is a random permutation of \( H \) and thus of \( G \) (as in the real protocol).

b) The above argument does not work for the graph-non-isomorphism protocol, as it is not a three-round protocol. One could consider consider it a three-round protocol in which the first message of the prover is the empty message. But in this case, the challenge space would be exponentially large and, moreover, the challenge space used by the honest verifier differs from that a potentially dishonest verifier could use, which is, however, essential for the proof of Theorem 3.1.

c) The above argument fails for the Schnorr protocol, as the challenge space has size \(|G|\) which is exponential in the size of the representation of \( z \).

If one modifies the Schnorr protocol such that the challenge is chosen from any polynomially-sized set \( C \) with at least two elements, it becomes zero-knowledge and remains sound if it is repeated sufficiently often (for the original Schnorr protocol, a single round was sufficient).

d) The motivation for introducing a simulator is to state that everything the polynomially bounded \( V \) sees in an execution of the protocol he could have simulated himself, which only makes sense if the simulator is polynomially bounded as well.

---

1See also Exercise 1.3.
To illustrate this, consider the following protocol for proving that two graphs \(G\) and \(H\) are isomorphic:

\[
P \text{ computes the permutation } \pi \text{ such that } H = \pi G \pi^{-1} \text{ and sends it to } V.\]

This protocol is clearly leaks information to the verifier: he the permutation between \(G\) and \(H\), which he otherwise would not be able to do (assuming that the GI problem is hard).

However, if inefficient simulators were allowed, the protocol would be zero-knowledge as the simulator \(S\) could compute \(\pi\) itself and produce a transcript distributed identically to that of the execution of the above protocol between \(P\) and \(V\).

### 3.2 Geometric Zero-Knowledge

a) Given two angles \(\alpha\) and \(\beta\), the angle \(\alpha \pm \beta\) can be constructed as follows: Open the compass to an arbitrary angle. Draw a circle around the endpoints of both angles with the resulting radius, which results in four new points \(p_{\alpha}, p'_{\alpha}, p_{\beta}, p'_{\beta}\). Open the compass to the distance between \(p_{\alpha}\) and \(p'_{\alpha}\). Draw a circle around, say, \(p_{\beta}\) with the resulting radius and create the line \(\ell\) through \(p_{\beta}\) and \(p'_{\beta}\) as well as the intersection points \(q_{\beta}\) and \(q'_{\beta}\) of the circle and \(\ell\). Then, create a line through the endpoint of \(\beta\) and \(q_{\beta}\) or \(q'_{\beta}\), depending on whether \(\alpha + \beta\) or \(\alpha - \beta\) is to be constructed.

b) A possible protocol for this task is the following one:

\begin{align*}
\text{Peggy} & \quad \text{Vic} \\
\text{knows angles } \alpha, \beta \quad & \text{s.t. } \beta = 3\alpha \\
\text{choose random angle } \kappa & \quad \tau \\
\text{create } \tau := 3\kappa & \quad c \\
\text{choose random } c \in R \{0, 1\} & \quad \rho \\
\text{create } \rho := \kappa + c\alpha & \quad \text{check } 3\rho \equiv \tau + c\beta \\
\end{align*}

c) Completeness: One can easily verify that if Peggy is honest and knows \(\alpha\), Vic will always accept.

Proof of Knowledge: Assume Peggy knows successful answers \(\rho, \rho'\) to both challenges \(c = 0\) and \(c' = 1\) for the same first message \(\tau\). In that case,

\[
3\rho = \tau \quad \text{and} \quad 3\rho' = \tau + \beta.
\]

Thus, \(3\rho' - 3\rho = \beta = 3\alpha\), and, therefore, Peggy may compute the angle \(\alpha\) as \(\rho' - \rho\).

d) Zero-Knowledge: The protocol is \(c\)-simulatable: for a given challenge \(c \in \{0, 1\}\), choose a uniform random angle \(\rho\) and set \(\tau := 3\rho - c\beta\), which is easily checked to result in the correct distribution (along the lines of Exercise 3.1.a)). Moreover, the size of the challenge space is clearly polynomial.

Therefore, by Theorem 3.1, the protocol is perfectly zero-knowledge.

### 3.3 An Interactive Proof

a) One possible protocol for the task, which is along the lines of Schnorr’s protocol, is the following one:
Peggy knows $x, y \in \mathbb{Z}_{|G|}$
choose $k, l \in \mathbb{Z}_{|G|}$
compute $t := g^x h^l$

Vic knows $z = g^x h^y$

\[ t \]
\[ c \]

let $c \in R \subseteq \mathbb{Z}_{|G|}$

\[ (r, s) \]

check if $g^r h^s \cong tz^c$

Completeness: It is easily verified that if Peggy is honest and knows $(x, y)$, then Vic always accepts.

Proof of Knowledge: From the prover’s replies to two different challenges for the same first message $t$, one can compute values $x'$ and $y'$ such that $g^{x'} h^{y'} = z$:

Let $(t, c, (r, s))$ and $(t, c', (r', s'))$ be two accepting transcripts with $c \neq c'$. That is, $g^r h^s = tz^c$ and $g^{r'} h^{s'} = tz^{c'}$. By dividing the first equation by the second one we get:

\[ g^{r-r'} h^{s-s'} = z^{c-c'} \]

which implies that $x' = (r - r')(c - c')^{-1}$ and $y' = (s - s')(c - c')^{-1}$ are values with $g^{x'} h^{y'} = z$. Note that since $|G|$ is prime, $c - c' \neq 0$ has an inverse modulo $|G|$.

b) Zero-Knowledge: Similarly to all previous examples, the protocol is $c$-simulatable:
Choose random $r, s \in \mathbb{Z}_{|G|}$ and set $t := g^r h^s z^{-c}$, which is easily checked to result in the correct distribution (along the lines of Exercise 3.1.a)). If $C$ is chosen to be polynomially large, by Theorem 3.1, the protocol is thus zero-knowledge.