1 Zero Knowledge Proofs in Geometry

a) The constructions are simple and we show here for example how to bisect an angle. First we open the compass in an arbitrary angle and draw a circle around the endpoint of the angle. We label the intersection points of the circle and the angle as $A$ and $B$. We draw a circle around the point of $A$ and $B$. And we construct a line between the endpoint of the angle and the intersection of the (newly constructed) circles.

b) The following example is one of the possible protocols:

<table>
<thead>
<tr>
<th>ZKP in Geometry</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Peggy</td>
<td>Vic</td>
</tr>
<tr>
<td>knows $\alpha, \beta = 3\alpha$</td>
<td>knows $\beta$</td>
</tr>
<tr>
<td>create random angle $\gamma$</td>
<td></td>
</tr>
<tr>
<td>construct $\tau = 3\gamma$</td>
<td>send over $\tau$</td>
</tr>
<tr>
<td>send over $c$</td>
<td>choose randomly $c \in {0, 1}$</td>
</tr>
<tr>
<td>create $\rho = \gamma + c\alpha$</td>
<td>send over $\rho$</td>
</tr>
<tr>
<td>check $3\rho = \tau + c\beta$</td>
<td></td>
</tr>
</tbody>
</table>

- **Completeness.** One can easily see that if Peggy is honest and knows $\alpha$, Vic always accepts. More concretely, in the last step $3\rho = 3(\gamma + c\alpha) = 3\gamma + 3c\alpha = \tau + c\beta$.

- **Soundness.** We show that if Peggy can answer both challenges then she really knows $\alpha$. Assume Peggy can answer for both challenges $c = 0$ and $c' = 1$ correctly with $\rho = \gamma + 0 \cdot \alpha = \gamma$ and $\rho' = \gamma + \alpha$. Then it follows that Peggy can compute $\alpha = \rho' - \rho$. In other words, if she doesn’t know $\alpha$ she can at most answer one of the challenges, and fail at the other challenge. That is, Peggy can correctly answer in one round only with probability $1/2$, and therefore $n$ rounds only with probability $1/2^n$.

- **Zero Knowledge.** The main idea is to show that the same transcript that Victor has after the protocol could be generated by himself (without knowing $\alpha$). During the protocol the transcript contains the triples $(\tau, c, \rho)$ and can be produced as follows. For each challenge $c$, generate a random $\rho$ and construct $\tau = 3\rho - c\beta$.

---

1 You may have a look at the following video about these constructions and the impossibility of trisecting an angle, if desired: [https://youtu.be/O1sPvUrOfDU](https://youtu.be/O1sPvUrOfDU)

2 With the same distribution; in case of random values.
Note. The soundness and zero knowledge property may sound contradictory to each other but they are not. Even though the transcript has "no information about α" after the protocol, Victor is convinced that Peggy knows α because she was able to answer to the challenges during the protocol. In particular, first τ is constructed and only then based on the challenge c, ρ is constructed.

2 MPC with Secret Sharing

a) One can easily see that each party after summing locally holds a share of the polynomial \( f(x) = f_1(x) + f_2(x) \) (since the degree of the polynomial by summing doesn’t change and \( t \) points uniquely define a polynomial of degree \( t - 1 \)). It follows, \( s = f(0) = f_1(0) + f_2(0) = s_1 + s_2 \). Hence, if the polynomial is reconstructed and evaluated at point 0, it will result to the sum of \( s_1 \) and \( s_2 \).

b) Dave can just continue the same way as other participants:

Alice

Choose \( r \)

\[
\begin{align*}
    m_1 &= a + r \\
    m_2 &= b + m_1 \\
    m_3 &= c + m_2 \\
    m_4 &= d + m_3
\end{align*}
\]

Send \( s = m_4 - r \) to everyone

\[\hline\]

Carol

Dave

\[\hline\]

\[\hline\]

\[\hline\]

c) Alice and Carol can easily compute the salary of Bob as follows. Since Carol has \( m_2 = b + m_1 \) and Alice has \( m_1 \) they can compute \( b = m_2 - m_1 \). The same technique can be used for Dave as well, namely \( d = m_4 - m_3 \).

d) The main idea is to use secret sharing and the fact that they are linear. Each party shares their salary by using \( (n,n) \) Shamir secret sharing, compute locally the sum of each share (namely the share of each salary), and in the end reconstruct the sum only.

2