MTAT.07.003 Cryptology II
Spring 2010 / Exercise session III / Example solution

Problem. Normally, it is impossible to compute computational distance between two distributions directly, since the number of potential distinguishing algorithms is humongous. However, for really small time-bounds it can be done. Assume that all distinguishers \( A : Z_{16} \rightarrow \{0, 1\} \) are implemented as Boolean circuits consisting of NOT, AND, OR gates and the corresponding time-complexity is just the number of logic gates. For example, \( A(x_3 x_2 x_1 x_0) = x_1 \) has time-complexity 0 and \( A(x_3 x_2 x_1 x_0) = x_1 \lor \neg x_3 \land x_2 \) has time-complexity 3.

1. Let \( X_0 \) be a uniform distribution over \( Z_{16} \) and let \( X_1 \) be a uniform distribution over \{0, 2, 4, 6, 8, 10, 12, 14\}. What is \( \text{cd}_2^1(X_0, X_1) \)?
2. Find a uniform distribution \( X_2 \) over some 8 element set such that \( \text{cd}_2^1(X_0, X_2) \) is minimal. Compute \( \text{cd}_2^2(X_0, X_2) \) and \( \text{cd}_2^3(X_0, X_2) \).
3. Find a uniform distribution \( X_3 \) over some 8 element set such that the distance sum \( \text{cd}_2^1(X_1, X_0) + \text{cd}_2^1(X_0, X_3) \neq \text{cd}_2^1(X_1, X_3) \).
4. Estimate for which value of \( t \) the distances \( \text{cd}_2^1(X_0, X_1) \) and \( \text{sd}_2(X_0, X_1) \) coincide for all distributions over \( Z_{16} \).

Solution. As the statistical distance \( \text{sd}_2(X_0, X_1) = \frac{1}{2} \) and the corresponding distinguisher \( A(x_3 x_2 x_1 x_0) = x_0 \) consists of zero gates, we get \( \text{cd}_2^0(X_0, X_1) = \frac{1}{2} \).

For the second question, let \( X_\emptyset = \{x \in Z_{16} : \phi(x) = 1\} \) denote the true-set for a circuit \( \phi \) and let \( X_2 \) be some 8 element set. Then by definition

\[
\text{Adv}_{X_0, X_2}^\text{ind}(\phi) = \left| \Pr \left[ x \leftarrow X_0 : \phi(x) = 1 \right] - \Pr \left[ x \leftarrow X_2 : \phi(x) = 1 \right] \right|
\]

\[
= \frac{1}{16} \cdot ||X_\emptyset| - 2 : |X_\emptyset \cap X_2| = \frac{1}{16} \cdot ||X_\emptyset| - |X_\emptyset \setminus X_2||
\]

and minimal computational distance is achieved by the set \( X_2 \) that splits almost evenly by all possible sets \( X_\emptyset \). By considering formulae

\[
\phi_1(x) = x_0, \ldots, \phi_4(x) = x_3, \phi_5(x) = \neg x_0, \ldots, \phi_8(x) = \neg x_3,
\]

we get that a set \( X_2 \) can achieve \( \text{cd}_2^1(X_0, X_2) = 0 \) only if it contains 4 elements with the \( i \)th bit set to one and 4 elements with the \( i \)th bit set to zero. Formulae

\[
\phi_9(x) = x_0 \land x_1, \ \phi_{10}(x) = x_0 \land x_2, \ldots, \phi_{13}(x) = x_1 \land x_3, \ \phi_{14}(x) = x_2 \land x_3,
\phi_{15}(x) = x_0 \lor x_1, \ \phi_{16}(x) = x_0 \lor x_2, \ldots, \phi_{19}(x) = x_1 \lor x_3, \ \phi_{20}(x) = x_2 \lor x_3
\]

indicate that such a set must contain exactly 2 elements with \( i \)th and \( j \)th bit set to one and exactly 2 elements with \( i \)th and \( j \)th bit set to zero. A bit representation of a possible solution is depicted in Figure 1. The solution has a peculiar property: if we choose uniformly element from \( X_2 \) and observe a bit
pair \( i \) and \( j \) the corresponding bit-string has uniform distribution over \( \mathbb{Z}_4 \). Consequently, any formula consisting of two inputs is incapable from distinguishing \( X_0 \) and \( X_2 \). A formula consisting of two gates can cover three inputs and thus potential distinguishing capabilities are higher. As Figure 2 clearly shows, the distribution of bit triples \( x_0, x_2, x_3 \) is indeed different from uniform and the task of building a distinguisher simplifies considerably. In fact, we can express

\[
\text{Adv}_{X_0, X_2}^{\text{ind}}(\phi) = \frac{1}{8} |\psi(000) + \psi(101) + \psi(110) - \psi(001) - \psi(100) - \psi(111)|.
\]

for any formula \( \phi(x) = \psi(x_0x_2x_3) \). Exhaustive search reveals that the formulae

\[
x_0 \land x_2 \land x_3, x_0 \lor x_2 \lor x_3, x_0 \land x_3 \lor x_2, x_0 \land (x_2 \lor x_3)
\]

all achieve optimal advantage \( \text{Adv}_{X_0, X_2}^{\text{ind}}(\phi) = \frac{1}{8} \). For the next distance estimate, note that a three gate distinguisher can cover all 4 inputs if it does not contain Not-gates. All of such distinguishers achieve advantage \( \frac{1}{16} \) and thus cannot not be optimal. Consequently, a potential optimal 3-gate distinguisher with Not-gate must process inputs \( x_0, x_2, x_3 \). Indeed, several formulae with negation achieve again the advantage \( \frac{1}{8} \) but not more. Hence, we have shown that

\[
\text{cd}_2^3(X_0, X_2) = \text{cd}_3^4(X_0, X_2) = \frac{1}{8}.
\]

As \( \text{sd}_x(X_1, X_1) = 0 \) and \( \text{sd}_x(X_0, X_1) = \frac{1}{8} \), by taking \( X_3 = X_1 \) we get the required counter-example for the third question. Finally, note that any statistical test is a predicate. As a distinguisher with negated output works as well as the original, we must bound the gate complexity of a predicate that is satisfied by at most 8 inputs. Each of this inputs can be represented as conjunct consisting of three AND- and at most four NOT-gates. Hence, the total gate count is bounded by 64 gates, i.e., \( \text{cd}_x^{64}(X_0, X_1) = \text{sd}_x(X_0, X_1) \) for all distributions \( X_0 \) and \( X_1 \).

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Violating triples</th>
<th>sd</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x_0, x_1, x_2 )</td>
<td>No violating triples</td>
<td>0</td>
</tr>
<tr>
<td>( x_0, x_1, x_3 )</td>
<td>No violating triples</td>
<td>0</td>
</tr>
<tr>
<td>( x_0, x_2, x_3 )</td>
<td>000 ( \rightarrow ) 0.00, 001 ( \rightarrow ) 0.25, 100 ( \rightarrow ) 0.25</td>
<td>( \frac{4}{8} )</td>
</tr>
<tr>
<td>( x_1, x_0, x_1 )</td>
<td>011 ( \rightarrow ) 0.00, 110 ( \rightarrow ) 0.00, 111 ( \rightarrow ) 0.25</td>
<td>( \frac{4}{8} )</td>
</tr>
<tr>
<td>( x_2, x_3, x_4 )</td>
<td>No violating triples</td>
<td>0</td>
</tr>
</tbody>
</table>

**Figure 1:** Orthogonal array with parameters \( n = 4 \) and \( k = 2 \).

**Figure 2:** Violating triples