Dominik Wawszczak
Student ID Number: 440014
Group Number: 3

Computational Complexity
Assignment 3

Let $X, Y \subseteq \{0,1\}^k$, where $|X| = |Y| = n$, be an instance of the Orthogonal Vectors Problem. We construct two new sets of binary vectors with dimension $d = 3k$:

$$A \;=\; \{xx0_k \;:\; x \in X\} \quad \text{and} \quad B \;=\; \{\overline{y}0_k y \;:\; y \in Y\},$$

where vu denotes the concatenation of vectors v and u, 0_l is a vector consisting of l zeros, and $\overline{v}$ is the vector v with every coordinate negated. Note that $|A| = |B| = n$.

We will prove the following equivalence:

$$\underset{x\in X}{\exists}\;\underset{y\in Y}{\exists}\; x \perp y \quad\iff\quad \underset{a\in A}{\exists}\;\underset{b\in B}{\exists}\; \mathrm{dist}_{\mathrm{Hamming}}(a,b) \leqslant k. \tag{1}$$

Assume there exist $x \in X$ and $y \in Y$ such that $x \perp y$. Take $a = xx0_k \in A$ and $b = \overline{y}0_k y \in B$. Define

$$\mathrm{cnt}_{p,q} \;=\; |\{i \;:\; x[i] = p \;\wedge\; y[i] = q\}|,$$

for any $p, q \in \{0,1\}$. We have:

$$\begin{aligned}
\mathrm{dist}_{\mathrm{Hamming}}(a,b) \;&=\; \mathrm{dist}_{\mathrm{Hamming}}(xx0_k, \overline{y}0_k y) \;=\\
&=\; \mathrm{dist}_{\mathrm{Hamming}}(x,\overline{y}) + \mathrm{dist}_{\mathrm{Hamming}}(x,0_k) + \mathrm{dist}_{\mathrm{Hamming}}(0_k,y) \;=\\
&=\; (\mathrm{cnt}_{0,0} + \mathrm{cnt}_{1,1}) + (\mathrm{cnt}_{1,0} + \mathrm{cnt}_{1,1}) + (\mathrm{cnt}_{0,1} + \mathrm{cnt}_{1,1}) \;=\\
&=\; (k - \mathrm{cnt}_{0,1} - \mathrm{cnt}_{1,0}) + (\mathrm{cnt}_{0,1} + \mathrm{cnt}_{1,0} + 2\cdot\mathrm{cnt}_{1,1}) \;=\; k + 2\cdot\mathrm{cnt}_{1,1} \;=\; k,
\end{aligned}$$

because $\mathrm{cnt}_{1,1} = 0$, as $x \perp y$. We also used the fact that $\mathrm{cnt}_{0,0} + \mathrm{cnt}_{0,1} + \mathrm{cnt}_{1,0} + \mathrm{cnt}_{1,1} = k$.

Conversely, assume there exist $a \in A$ and $b \in B$ such that $\mathrm{dist}_{\mathrm{Hamming}}(a,b) \leqslant k$. Take $x \in X$ and $y \in Y$ where $a = xx0_k$ and $b = \overline{y}0_k y$. As before, we can show that $\mathrm{dist}_{\mathrm{Hamming}}(a,b) = k + 2\cdot\mathrm{cnt}_{1,1}$ with $\mathrm{cnt}_{p,q}$ defined as earlier. Therefore, it must hold that $\mathrm{cnt}_{1,1} = 0$, which means $x \perp y$, completing the proof of the equivalence (1).

Suppose there exists a constant $\delta > 0$ such that the problem from the statement can be solved in time $\mathcal{O}\big(d^{100} \cdot n^{2-\delta}\big)$. Then, due to the equivalence (1), the Orthogonal Vectors Problem could be solved in time

$$\mathcal{O}\big(d^{100} \cdot n^{2-\delta}\big) \;=\; \mathcal{O}\big((3k)^{100} \cdot n^{2-\delta}\big) \;=\; k^{\mathcal{O}(1)} \cdot n^{2-\delta},$$

which contradicts the Orthogonal Vectors Conjecture, concluding the proof, since

$$\text{Strong Exponential Time Hypothesis} \implies \text{Orthogonal Vectors Conjecture}.$$