Exercise 15 [Typo corrected 2025-12-04]

Analysis of Boolean Functions, Autumn 2025, University of Chicago
Instructor: William Hoza (williamhoza@uchicago.edu)

Submission. Solutions are due **Friday, December 5** at 11:59pm Central time. Submit your solutions through Gradescope. You are encouraged, but not required, to typeset your solutions using a LaTeX editor such as Overleaf.

The policies below can also be found on the course webpage.

Collaboration. You are encouraged to collaborate with your classmates on exercises, but you must adhere to the following rules.

- Work on each exercise on your own for at least five minutes before discussing it with classmates.
- Feel free to explain your ideas to your classmates in person, and feel free to use whiteboards/chalkboards/etc. However, do not share any written/typeset solutions with your classmates for them to study on their own time. This includes partial solutions.
- Write your solutions on your own. While you are writing your solutions, do not consult any notes that you might have taken during discussions with classmates.
- In your write-up, list any classmates who helped you figure out the solution. The fact that student A contributed to student B's solution does not necessarily mean that student B contributed to student A's solution.

Permitted Resources for Full Credit. In addition to discussions with me and discussions with classmates as discussed above, you may also use the course textbook, any slides or notes posted in the "Course Timeline" section of the course webpage, and Wikipedia. If you wish to receive full credit on an exercise, you may not use any other resources.

Outside Resources for Partial Credit. If you wish, you may use outside resources (ChatGPT, Stack Exchange, etc.) to solve an exercise for partial credit. If you decide to go this route, you must make a note of which outside resources you used when you were working on each exercise. You must disclose using a resource even if it was ultimately unhelpful for solving the exercise. Furthermore, if you consult an outside resource while working on an exercise, then you must not discuss that exercise with your classmates.

In this exercise, you will prove that every $(0.51 \cdot n)$-wise uniform generator has seed length at least $n - O(1)$.

Exercise 15 (10 points)**.** Let D be a k-wise uniform distribution over $\{0,1\}^n$. Let $p\colon \{0,1\}^n \to [0,1]$ be the probability mass function of D. Let X, X' be two independent samples from D.

(a) Prove that $\Pr[X = X'] = 2^{-n} + 2^n \cdot W^{>k}[p]$.

(b) Prove that $\Pr[d(X,X') = 1] = n \cdot 2^{-n} + 2^n \cdot \sum_{|S|>k} \widehat{p}(S)^2 \cdot (n - 2|S|)$, where $d(\cdot,\cdot)$ denotes Hamming distance.

(c) Use part (b) to prove that if $2k + 2 > n$, then

$$W^{>k}[p] \leq \frac{n \cdot 2^{-2n}}{2k + 2 - n}.$$

(d) Assume $k \geq 0.51 \cdot n$. Use parts (a) and (c) to prove that $\Pr[X = X'] \leq O(2^{-n})$.

(e) Assume $k \geq 0.51 \cdot n$. ~~Let $G\colon \{\pm 1\}^r \to \{\pm 1\}^n$,~~ Let $G\colon \{0,1\}^r \to \{0,1\}^n$, and assume $G(U_r) = D$. Use part (d) to prove that $r \geq n - O(1)$.