COCOON 2021 (subreviewer)

Review Request

You have already submitted your review. The review and the information about this request are shown below.

Your Review

Review 2

Paper:	103
Title:	Sharp indistinguishability bounds from non-uniform approximations
Authors:	Christopher Williamson
PC member:	Ling-Ju Hung
Reviewer:	Chuang-Chieh Lin <josephcclin@gmail.com>
Time:	Aug 06, 04:05
Overall evaluation:	**-1**: (weak reject) This paper considers the problem of distinguishing between two symmetric probability distributions by observing k bits of sample, yet subject to the constraint that all (k-1)-wise marginal distributions of the two distributions are identical. The authors provide upper bound and lower bound on the maximal statistical distance that holds for all k. This work is motivated from cryptographic secret sharing schemes in a minimal setting: j-wise indistinguishability guarantees that any coalition of size bounded by j of colluding parties can learn nothing about the secret from the joint shares. Their technique is to decompose an arbitrary statistical test into a small Boolean basis Q_w that observes k bits and accepts iff the observed Hamming weights is exactly w. To approximate a high-degree polynomial, a low-degree polynomial approximation is used and such an approximation need not to be uniform due to the discrete domain of Q_w. Overall, I don't think the manuscript is ready. It's difficult for readers, especially the ones who are unfamiliar with this issue, to follow. I am also concerned about the correctness of the proofs (e.g., the one for Lemma 1). Errors and other comments: Line 10 of the paragraph of "Approximate degree motivation": 2\epsilon-distinguishability is not defined. Does it mean 2\epsilon-wise distinguishability? Line 2 of Theorem 1, page 3: the statistical distance is not defined. Line -4, page 6: Should the product starts from i=1? Otherwise, the right-hand side of the equality should start with n^k/(k-1)! and the fractional inside the square root is supposed to end with (k^2-1/4)/(n^2-k^2). Line -7, page 8: "perfectly k-wise indistinguishable" is not defined.

	Line 11, page 9: |x| is not defined. Is it the Hamming weight of x (i.e., the number of 1's in x)?
Reviewer's confidence:	**2**: (low)
Confidential remarks for the program committee:	
Special issue invitation?:	

Submission Information

Submission 103	
Title:	Sharp indistinguishability bounds from non-uniform approximations
Paper:	(Jun 30, 17:59 GMT)
Author keywords:	randomness polynomial approximation bounded indistinguishability
EasyChair keyphrases:	non uniform approximation (126), wise indistinguishable distribution (126), sharp indistinguishability bound (110), discrete chebyshev (106), discrete chebyshev polynomial (95), statistical distance (90), symmetric distribution (90), approximate degree (90), boolean function (80), polynomial approximation (70), linear programming duality (63), discrete chebyshev basis (63), hamming weight (60), wise indistinguishable (60), statistical test (60), k wise marginal (47), symmetric boolean function (47), discrete chebyshev representation (47), central binomial coefficient (47), univariate polynomial (40), low degree polynomial approximation (40), symmetric function (40), uniform approximation (40), reconstruction advantage (40)
Abstract:	We study the problem of distinguishing between two symmetric probability distributions over n bits by observing k bits of a sample, subject to the constraint that all (k-1)-wise marginal distributions of the two distributions are identical to each other. Previous works of Bogdanov et al. and of Huang and Viola have established approximately tight results on the maximal statistical distance when k is at most a small constant fraction of n and Naor and Shamir gave a tight bound for all k in the case of distinguishing with the OR function. In this work we provide sharp upper and lower bounds on the maximal statistical distance that hold for all k. Upper bounds on the statistical distance have typically been obtained by providing uniform low-degree polynomial approximations to certain higher-degree polynomials; the sharpness and wider applicability of our result stems from the construction of suitable non-uniform approximations.
Submitted:	Jun 30, 17:44 GMT
Last update:	Jun 30, 17:44 GMT

Authors

first name	last name	country	affiliation	Web page	corresponding?
Christopher	Williamson	Hong Kong	Independent researcher		✓

Emails

Below you will find the email exchange between you and Ling-Ju Hung concerning this paper. All times are GMT.

Time:	Aug 04, 08:20
Who:	Ling-Ju Hung->you
Subject:	COCOON 2021 submission review request

Dear Chuang-Chieh,

I am a PC member of COCOON 2021. Could you please write
a review for me on the following paper submitted to COCOON 2021:

Paper id: 103
Title: Sharp indistinguishability bounds from non-uniform approximations
---

The instructions on how to answer this review request
can be found at the bottom of this letter.

I need to receive the review by August 9, 2021.

If you cannot review this paper, could you please suggest names and
email addresses of 2-3 possible reviewers?

Best regards,
Ling-Ju Hung <ljhung@ntub.edu.tw>

Time:	Aug 04, 09:44
Who:	you->Ling-Ju Hung
Subject:	Your review request for COCOON 2021 submission 103

OK.