Electronic Colloquium on Computational Complexity, Comment 1 on Report No. 62 (2006)

ECCC

Comments on "Unique-k-SAT is as Hard as k-SAT"

Chris Calabro

May 29, 2006

Abstract

The paper "Unique k-SAT is as Hard as k-SAT", by Subhas Kumar Ghosh [Gho], has many flaws, both technical and academic, and some invalidate the proof of the main result. The following comments describe some of the errors. It is assumed that the reader is intimately familiar with the paper.

1 Academic errors

The format of the paper closely mirrors that of [CIKP] using the same or minor variants of introductory explanation, section titles, theorems, and proofs. Portions of many paragraphs are directly copied from [CIKP] without permission. For example, paragraph 1 of section 1 is just a slight modification of a subset of the sentences from the first 2 paragraphs of section 1.1 of [CIKP].

In light of the author's claims, some of these duplicated sections are no longer relevant; e.g. all of section 3 is a nearly verbatim analogue of section 3.1 of [CIKP], but is no longer needed.

On page 2, paragraph 3, the author claims that [CIKP] show that Unique-k-SAT is as hard as k-SAT. They did not show this.

2 Minor technical errors

The author confuses big-Oh and little-Oh, and states some incorrect bounds. E.g. in lemma 1.1, $n^{o(1)}$ should be $O(n^2)$. Lemma 1.1 also gives the wrong probability bound: it's $\Omega(1/n)$, not $1/4$. On page 4, paragraph 2, $\Omega(s^{o(1)})$ does not makes sense, mixing little-Oh and big-Omega. Perhaps the author meant $s^{O(1)}$. On page 3, item 1, $n^{o(1)}$ should be $O(nk)$.

Page 3, item 2, is literally false. If $|S|$ is odd then $Pr(|S^{(0)}| = |S^{(1)}|)$ is not high, it's 0. Even if $|S|$ were even, the probability may still be low. Perhaps the author meant that the probability that $|S^{(0)}|$ is approximately $|S^{(1)}|$ is high.

In lemma 2.1, q in the statement plays no role. Also ϵ plays no role and might as well be chosen as a constant, say $(\ln 2)/3$, to force $k' = k$. Also the

ISSN 1433-8092

probability $1/2$ is too large; the construction admits to making a guess that only has $1/n$ chance of succeeding, so the success probability can't be any better than $1/n$.

In proposition 2.1, $\mathbb{F}^n$ is not a field and should be simply $\mathbb{F}$. (If one tries to interpret $\mathbb{F}^n$ as the field of order q^n, then the first sentence of the proof of proposition 2.1 makes no sense, since e.g. x^2 is not x when x is a nonzero element of the field.)

The proof of claim 2.2 is invalid, but can be fixed. First strengthen claim 2.1 to the following revised claim 2.1: there is no nontrivial combination of $f_1, \ldots, f_m$ that evaluates to 0 on all of $\mathcal{A}$. (This implies that $f_1, \ldots, f_m$ are linearly independent, but this stronger statement is what we actually will use.) Then we go back to the proof of claim 2.2 and note that if $\sum \lambda_i \hat{f}_i = 0$, then this sum is 0 when restricted to $\mathcal{A}$ as well, and so (by revised claim 2.1) $\sum \lambda_i f_i = 0$, which implies that the λ_i are all 0. So the $\hat{f}_i$ are linearly independent.

3 Major error

Claim 2.3 is the main source of the paper's improvement but is false, which we now show. First notice that the conclusion does not depend on ϵ. Later the author chooses $t = q - 1$, $m = \frac{s}{\lg q}$, $q = n^{1/3}$. So the probability expression $(\frac{t}{\sqrt{2}q^2})^{2m}$ is much less than $\frac{1}{q^2}$, at least when $s > \frac{1}{3}\lg n$.

Let $C \subseteq \{0,1\}^n$ be a distance $r = \lceil \epsilon n \rceil$ code with exactly $q+1$ points. Then, by the pigeonhole principle and the union bound,

$$
\begin{aligned}
1 &= Pr(\exists x, y \in C, x \neq y \; f(x) = f(y)) \\
&\leq \binom{q+1}{2} Pr(f(x) = f(y)) && \text{for some fixed } x, y \in C \text{ with } x \neq y \\
&\leq \binom{q+1}{2} \left(\frac{t}{\sqrt{2}q^2}\right)^{2m} && \text{assuming claim 2.3} \\
&< 1,
\end{aligned}
$$

a contradiction.

References

[CIKP] C. Calabro, R. Impagliazzo, V. Kabanets, R. Paturi, The complexity of unique k-SAT: an isolation lemma for k-CNFs, Proc. 18th IEEE Conference on Computational Complexity, 2003, pp 135–141

[Gho] Subhas Kumar Ghosh, Unique k-SAT is as Hard as k-SAT, Electronic Colloquium on Computational Complexity, Report TR06-062, 2006

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/