Electronic Colloquium on Computational Complexity, Comment 2 on Report No. 62 (2006)

On page 6 we want to calculate $\Pr[f(x) = f(y)]$. Knowing that $f(x) = \sum_{A_i \in \mathcal{A}} \lambda_i f_i(x)$, this probability is equal to $\Pr[\sum_{A_i \in \mathcal{A}} \lambda_i (f_i(x) - f_i(y)) = 0]$.

Then I don't understand the line $\Pr[f(x) = f(y)] = \prod_{i=1}^{m} (\Pr[f_i(x) = f_i(y) | \lambda_i \neq 0] \Pr[\lambda_i \neq 0])$.

As far as I understand, we have, due to the linearly independance of the f_i :

$\Pr[f(x) = f(y)] = \prod_{i=1}^{m} \Pr[\lambda_i (f_i(x) - f_i(y)) = 0]$

Thus we have

$\Pr[f(x) = f(y)] = \prod_{i=1}^{m} (\Pr[\lambda_i (f_i(x) - f_i(y)) = 0 | \lambda_i = 0] \Pr[\lambda_i = 0] + \Pr[\lambda_i (f_i(x) - f_i(y)) = 0 | \lambda_i \neq 0] \Pr[\lambda_i \neq 0])$

Which leads to

$\Pr[f(x) = f(y)] = \prod_{i=1}^{m} (\Pr[\lambda_i = 0] + \Pr[f_i(x) = f_i(y) | \lambda_i \neq 0] \Pr[\lambda_i \neq 0])$

An then, because the λ_i were chosen randomly uniformly

$\Pr[f(x) = f(y)] = \prod_{i=1}^{m} (\frac{1}{q} + \Pr[f_i(x) = f_i(y)] \frac{q-1}{q})$

$\Pr[f(x) = f(y)] = \frac{1}{q}^m \prod_{i=1}^{m} (1 + \Pr[f_i(x) = f_i(y)](q-1))$

Which is not exactly the same. And assuming that the line I don't understand is true, then I still don't understand why the probability that $\lambda_i \neq 0$ would be equal to $\frac{1}{q}$ and not $\frac{q-1}{q}$

And the same thing about conditional probabilities is done on next page (page 7). The authors ensure that $\Pr[f_i(x) = f_i(y)] \leq \Pr[f_i(x) = f_i(y) | r, r' \notin L(modq)] \Pr[r, r' \notin L(modq)]$.

And I'd rather say that it's greater or equal, not less or equal. Because I think that the correct equality is

$\Pr[f_i(x) = f_i(y)] = \Pr[f_i(x) = f_i(y) | r, r' \notin L(modq)] \Pr[r, r' \notin L(modq)] + \Pr[f_i(x) = f_i(y) | rorr' \in L(modq)] \Pr[rorr' \in L(modq)]$.

In the proof of the last inequality, I truly don't understand how we can fix both m and q. We have $m \log q = s$, so if I correctly understood, fixing m to $\frac{2n + \log n - 1 + \log q}{\log q}$ and fixing q to $\sqrt[3]{n}$ implies that

$2n + \frac{4}{3} \log n - 1 = s$ which is not always true.

Also I won't write down all the little typing error but one of them, on page 3, is quite

ISSN 1433-8092

important, it's written

Since $\Pr[|S^{(0)}| \neq |S^{(1)}|]$ is very high

instead of

Since $\Pr[|S^{(0)}| = |S^{(1)}|]$ is very high

Finally, the paper implicitly says that the random constraint $f(x) = b$ can be put in CNF, but do we have a polynomial algorithm that does it ? It's not clear to me how to make this constraint into a CNF.

Thank you very much for the time you spent reading this and I hope I'll receive an answer that will make me understand better this paper.

ECCC ISSN 1433-8092

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