Conditional Inapproximability and Limited Independence – Addenda and Errata

Per Austrin

November 25, 2008

Acknowledgment I am grateful to Ryan O'Donnell for spotting many of these errors and pointing me towards some additional literature.

Page 11: definition of $||f||_\infty$ only makes sense for Ω finite. For infinite Ω it should be the essential supremum of $|f(x)|$.

Page 13, Definition 2.2.5: the same notion of correlation between probability spaces appears in [1], Chapter 10, for the case of Gaussian spaces.

Page 18: it should be pointed out that all the material in Section 2.3.3 is very basic material which can be found in many places, see e.g. [3].

Page 22: the "relaxed influence conditions", i.e., that at least three different functions must have a common influential coordinate, is not part of [2], Theorem 6.6. See [2], Lemma 6.9 for this.

Pages 36-37, Theorem 3.5.2 and Proposition 3.5.3: the pairwise independent distributions whose existences are asserted are also balanced.

Page 39, end of proof of Proposition 3.6.1: "taken care of." should be "taken care of similarly."

Pages 54-55, definition of the verifier: X is used both for the left vertex set of the Unique Label Cover instance and the random matrix picked by the verifier. This shows up also in the proof of soundness. It should in each case be clear from context which X is referred to, but just to make it clear: on line (1) in Algorithm 1 and in the first two paragraphs of the proof of soundness X refers to the left vertex set, the other occurences on pages 54-55 refer to the matrix.

Page 76, bottom: "any $v \in V$" should be "any $v \in V_{\text{good}}$".

Page 87, "curve of Figure 6.3 is indeed convex", should be concave.

Page 96, Theorem 7.1.2: the hypercontractivity estimates of Wolff are exactly optimal as a function of α (i.e., not just essentially optimal).

Page 96, regarding the estimates in Corollaries 7.1.3 and 7.1.4: better estimates are given already in [4], and mentioned in the paper of Wolff as well.

Page 96: Corollaries 7.1.3 and 7.1.4 both use that if f is (p, q, η)-hypercontractive then f is (p, q, η')-hypercontractive for every $0 < \eta' \leq \eta$ (see e.g. [3]).

Page 96, proof of Corollary 7.1.3: the third expression should be $\frac{1}{A^{1/3}+A^{-1/3}}$, not $\frac{1}{A^{1/3}-A^{-1/3}}$.

Page 97, Theorem 7.1.5: $p \geq 2$.

Page 97, Theorem 7.1.6: $p \geq 2$.

Page 99, Proof of Theorem 7.2.2: having μ as the expected value of $|f|$ was an exceptionally bad choice. The distribution μ appearing in the statement of the theorem never appears in the proof, so all μ's appearing in the proof refer to the expected value of $|f|$.

Page 108: L should be l in the end of the proof of Lemma 8.4.3, and $||x||$ should be $||\overline{x}||$ in the last equation.

Page 109: in the expression $\max_{a \in [-1,1]^m} \sum_{i=1}^m a_i \left\langle v, x_i^{:\leq 2:} \right\rangle_{\mathbb{R}}$, it would have been more appropriate to use sup instead of max, but it is clear that the maximum is attained.

Page 110, the expression $L \exp(-\tau m) = \exp(-\tau m + \ln(5/\epsilon)|D_2|)$: should be $\leq$ rather than $=$.

Page 110: "provided m is a sufficently large multiple of $|D_2|$". $|D_2|$ should be $|D_2| \ln(5/\epsilon)$ (as we eventually chose ϵ as a function of c_3, this ends up being a sufficiently large multiple of $|D_2|$).

Page 110, end of proof of Lemma 8.4.2: $c_3/2m$ should be $c_3/(2m)$.

Page 111: "closes to f in..." $\rightarrow$ "closest to f in..."

Page 112, Theorem 8.6.1: there are some errors in the bound on m and on the error probability. The bound on m should be $m \leq \frac{n^k}{2^k q^{k^2} k^{2k}}$. The bound on the error probability should be $\exp(-n/(2kq^k)) =$

$\exp(-\Theta(n/c^k))$ for $c = 2q$ (say). These should also be the bounds in Lemma 8.6.2. Also, the last step is a bit hasty. With the appropriate bounds, and a middle step added for clarity, it becomes

$$1 - m\exp\left(-\frac{n}{2kq^k}\right) \geq 1 - n^k\exp\left(-\frac{n}{2kq^k}\right) \geq 1 - \exp(-\Theta(n/c^k)),$$

provided k is, say, at most a small multiple of $\log_q n$ (note that if k is not bounded by a small multiple of $\log_q n$ we have $m \leq 1$ and Theorem 8.6.1 is trivially true).

Page 119: "...by $(1/\alpha)^{|T|/2}$ Plugging this...", should be a period before "Plugging".

Page 119, second last equation of proof of Lemma 9.1.2: the $(1/\alpha)^{|T|/2}$ factor is temporarily lost.

Page 119, discussion after Lemma 9.1.2 about complex basis: Equation (9.1) is not the right equation, it should be the unnumbered equation at the top of page 119.

Page 120, Corollary 9.2.1: "largest non-zero Fourier coefficient" is somewhat misleading, "largest non-empty Fourier coefficient" is a better wording.

Page 120-121: Corollary 9.2.2 contains many mistakes. See the section below for complete details.

Page 122: "adding T_ρ does not change...". The word "adding" here was not a good choice—"applying T_ρ to the f_i's" would have been better.

Page 125: the identity $|\operatorname{Supp}(\mu)| = q^2(2^k - 1)$ for noisy arithmetic progressions is under the assumption that $q \geq 3$ and $k \geq 3$.

Corollary 9.2.2

There are many errors in Corollary 9.2.2, both in the statement and more seriously in the proof. Below are the correct statement and proof, in their entirety. There are five changes in the statement (here listed in decreasing order of significance):

1. The assumption $||f_i||_2 \leq 1$ has been replaced by the stronger condition $f_i(x) \in [0, 1]$ for every x.
2. d and δ also depend on $D := \deg_{-2}(f_1, \ldots, f_k)$ (or actually only d depends on D).
3. The assumption $\mathbb{E}[f_i] = 0$ has been removed.
4. $\rho(\mu)$ has been replaced by $\tilde{\rho}(\Omega_1, \ldots, \Omega_k, \mu)$.
5. Changed the dummy variable $1 \leq j \leq 3$ to $1 \leq a \leq 3$ because of a conflicting variable j in the proof.

Corollary 9.2.2. Assume the setting of Theorem 9.1.1, and further assume that $\tilde{\rho}(\Omega_1, \ldots, \Omega_k, \mu) < 1$. Then for every $\epsilon > 0$ there exist d and δ (depending only on ϵ, μ and D) such that the following holds. Let $f_i(x) \in [0, 1]$ for every i and x. Then if

$$\left| \langle f_1, \ldots, f_k \rangle_{\mathcal{N}} - \prod_{i=1}^{k} \mathbb{E}[f_i] \right| > \epsilon,$$

there exist three distinct indices $i_1, i_2, i_3 \in [k]$, and multi-indices $\sigma_1, \sigma_2, \sigma_3$ satisfying:

(a) $|S(\sigma_a)| \leq d$ for $1 \leq a \leq 3$.

(b) $\sigma_1, \sigma_2, \sigma_3$ intersect in the sense that $S(\sigma_1) \cap S(\sigma_2) \cap S(\sigma_3) \neq \emptyset$.

(c) $|\hat{f}_{i_a}(\sigma_a)| \geq \frac{\delta}{C^D}$ for $1 \leq a \leq 3$, where C is the constant from Theorem 9.1.1.

Proof. For $\rho \in [0, 1]$, let T_ρ be the operator on $L^2(\Omega^n, \mu^{\otimes n})$ mentioned in Section 9.3, i.e., for $f \in L^2(\Omega^n, \mu^{\otimes n})$, $T_\rho f$ is defined by $T_\rho f(x) = \mathbb{E}[f(y)]$, where $y \in \Omega^n$ is defined by letting $y_i = x_i$ with probability ρ, and letting y_i be a random sample from (Ω, μ) with probability $1 - \rho$. It is well-known and not hard to verify that $T_\rho f = \sum_\sigma \rho^{|\sigma|} \hat{f}(\sigma) \chi_\sigma$. It is also clear that the functions g_i only take values in $[0, 1]$.

Let $\gamma > 0$ be a parameter, and define $g_i = T_{1-\gamma} f_i$. By [2] Lemma 6.2 it holds that

$$|\langle f_1, \ldots, f_k \rangle_{\mathcal{N}} - \langle g_1, \ldots, g_k \rangle_{\mathcal{N}}| \leq \epsilon/2,$$

provided we take $\gamma = \Theta((1 - \tilde{\rho})\epsilon / \log(1/\epsilon))$.

We will now show that the functions $g_1, \dots, g_k$ have the property that there exist three indices i_1, i_2, i_3 and multi-indices $\sigma_1, \sigma_2, \sigma_3$ satisfying conditions (b) and (c) of the conclusion of the Corollary. Then, since the coefficient $\hat{g}_i(\sigma)$ of g_i have size at most $(1-\gamma)^{|\sigma|}$, the condition $|\hat{g}_{i_a}(\sigma_a)| \geq \delta/C^D$ implies that

$$|\sigma_a| \leq \frac{\log(C^D/\delta)}{\log(1/(1-\gamma))} := d,$$

so that also condition (a) of the conclusion is satisfied. Then since every coefficient of the f_i's has $|\hat{f}_i(\sigma)| \geq |\hat{g}_i(\sigma)|$, the fact that the functions $g_1, \dots, g_k$ satisfy the conclusion of the Corollary implies that the functions $f_1, \dots, f_k$ do as well.

Let us then see that the three of the functions $g_1, \dots, g_k$ have large intersecting Fourier coefficients. By the choice of γ and the fact that $\mathbb{E}[g_i] = \mathbb{E}[f_i]$, we have

$$|\langle g_1, \dots, g_k \rangle_{\mathcal{N}} - \prod_{i=1}^{k} \mathbb{E}[g_i]| > \epsilon/2.$$

Furthermore, since $\tilde{\rho}(\Omega_1, \dots, \Omega_k, \mu) < 1$, Theorem 2.5.1 applies. In the thesis it is stated with the stronger condition $\mu(a) > 0$ for every $a \in \Omega$, but as mentioned after the statement, it holds if this condition is replaced by $\tilde{\rho}(\Omega_1, \dots, \Omega_k, \mu) < 1$. See also [2], Theorem 6.6 and Lemma 6.9. Apply this theorem with error parameter $\epsilon/4$, giving some constants $\tau > 0$ and $d_* > 0$ (depending only on ϵ and μ), and three indices $i_1, i_2, i_3 \in [k]$ and $j \in [n]$ such that

$$\mathrm{Inf}_j^{\leq d_*}(g_{i_1}), \mathrm{Inf}_j^{\leq d_*}(g_{i_2}), \mathrm{Inf}_j^{\leq d_*}(f_{i_3}) \geq \tau.$$

Write $g_i = g_i^0 + g_i^1$, where g_i^1 is the part of g_i that depends on the j'th coordinate, i.e.,

$$g_i^1 = \sum_{j \in \sigma} \hat{g}_i(\sigma) \chi_\sigma.$$

Let $\delta := \frac{\tau\epsilon}{2k}$. If $g_{i_1}^1$, $g_{i_2}^1$, and $g_{i_3}^1$ each have some Fourier coefficient larger than δ/C^D, we are done, since every non-zero Fourier coefficient of g_i^1 contains j.

Otherwise, if the largest Fourier coefficient of, say, $g_{i_1}^1$ is smaller than δ/C^D, we can write

$$\langle g_1, \dots, g_k \rangle_{\mathcal{N}} = \left\langle g_1, \dots, g_{i_1}^0, \dots, g_k \right\rangle_{\mathcal{N}} + \left\langle g_1, \dots, g_{i_1}^1, \dots, g_k \right\rangle_{\mathcal{N}}.$$

By Theorem 9.1.1, the second term is bounded by δ, and the functions in the first term have the same expected values as the g_i's.

$$\left| \left\langle g_1, \dots, g_{i_1}^0, \dots, g_k \right\rangle_{\mathcal{N}} - \mathbb{E}[g_{i_1}^0] \cdot \prod_{i \neq i_1} \mathbb{E}[g_i] \right| \geq \epsilon/2 - \delta.$$

Furthermore, it is easy to see that $g_{i_1}^0(x)$ only takes values in $[0,1]$ (since $g_{i_1}^0$ gives the expected value of g_i when the values of all variables but x_1 have been fixed), so that this new set of functions satisfy the conditions of the statement of the corollary.

The rest of the proof is the same energy decrement argument as in the thesis. $\square$

References

[1] Svante Janson. *Gaussian Hilbert Spaces.* Cambridge University Press, 1997.

[2] Elchanan Mossel. Gaussian bounds for noise correlation of functions. arXiv Report math/0703683v3, 2007.

[3] Elchanan Mossel, Ryan O'Donnell, and Krzysztof Oleszkiewicz. Noise stability of functions with low influences: invariance and optimality. To appear in Annals of Mathematics, 2008.

[4] Krzysztof Oleszkiewicz. On a nonsymmetric version of the Khinchine-Kahane inequality. *Progress in Probability*, 56:157–168, 2003.