Quantum Information and Computation, Vol. 5, No. 2 (2005) 176–177

ERRATUM

QUANTUM LOWER BOUND FOR RECURSIVE FOURIER SAMPLING

SCOTT AARONSON
School of Mathematics, Institute for Advanced Study
Princeton, New Jersey, USA

Received December 20, 2004

I correct a technical error in [1]. The conclusions about Recursive Fourier Sampling are unaffected.

Keywords:
Communicated by: R Jozsa & J Watrous

In my paper "Quantum Lower Bound for Recursive Fourier Sampling" [1], the argument depended crucially on a measure of Boolean functions $g : \{0,1\}^n \to \{0,1\}$ that I called the "nonparity coefficient" $\mu(g)$. The intuition was that $\mu(g)$ should measure the distance of g from a parity function, with $\mu(g) = 0$ if and only if g itself was the parity (or the negation of the parity) of some subset of input bits. I defined $\mu(g)$ formally as follows:

Definition 1 *The nonparity coefficient $\mu(g)$ of g is the maximum μ^* for which the following holds. There exist distributions D_0, D_1 over $g^{-1}(0)$ and $g^{-1}(1)$ respectively such that for all $z \in \{0,1\}^n \setminus \{0^n\}$, $\widehat{s}_0 \in g^{-1}(0)$ and $\widehat{s}_1 \in g^{-1}(1)$,*

$$\Pr_{s_0 \in D_0}[s_0 \cdot z \equiv \widehat{s}_1 \cdot z \,(\mathrm{mod}\, 2)] \geq \mu^* \text{ and}$$
$$\Pr_{s_1 \in D_1}[s_1 \cdot z \equiv \widehat{s}_0 \cdot z \,(\mathrm{mod}\, 2)] \geq \mu^*.$$

This definition is mistaken. The problem is that $\mu(g) = 0$ does not imply that g is a parity function. To see this, let g be the logical AND of the n input bits. Then $g^{-1}(1) = \{1^n\}$, so there is only one distribution D_1 over $g^{-1}(1)$, which places all weight on 1^n. Furthermore, clearly there exist $z \in \{0,1\}^n \setminus \{0^n\}$ and $\widehat{s}_0 \in g^{-1}(0)$ such that $1^n \cdot z \not\equiv \widehat{s}_0 \cdot z$, and therefore

$$\Pr_{s_1 \in D_1}[s_1 \cdot z \equiv \widehat{s}_0 \cdot z \,(\mathrm{mod}\, 2)] = 0.$$

It follows that $\mu(g) = 0$.

To fix this problem, we simply need to use what I called the "two-sided nonparity coefficient," $\mu_2(g)$, in Section 4 of [1].

Definition 2 *$\mu_2(g)$ is the maximum μ^* for which there exist distributions D_0, D_1 over $g^{-1}(0)$ and $g^{-1}(1)$ respectively such that for all $z \in \{0,1\}^n \setminus \{0^n\}$, $\widehat{s}_0 \in g^{-1}(0)$ and $\widehat{s}_1 \in g^{-1}(1)$,*

$$\Pr_{s_0 \in D_0, s_1 \in D_1} [s_0 \cdot z \equiv \widehat{s}_1 \cdot z \pmod 2 \quad \vee \quad s_1 \cdot z \equiv \widehat{s}_0 \cdot z \pmod 2] \geq \mu^*.$$

My original motivation for introducing $\mu_2(g)$ was to generalize the results from total to partial functions. But the new definition has the additional advantage of being correct:

Proposition 1 *For all g (partial or total), $\mu_2(g) = 0$ if and only if g can be written as the parity (or the NOT of the parity) of a subset $B \subseteq \{1, \ldots, n\}$ of input bits.*

Proof For the 'if' direction, form an input $z \in \{0,1\}^n$ by taking $z[i] = 1$ if and only if $i \in B$, and choose $\widehat{s}_0$ and $\widehat{s}_1$ arbitrarily. This ensures that $\mu^* = 0$. For the 'only if' direction, if $\mu_2(g) = 0$, we can choose D_0 to have support on all 0-inputs, and D_1 to have support on all 1-inputs. Then there must be a z such that $s_0 \cdot z$ is constant as we range over $g^{-1}(0)$, and $s_1 \cdot z$ is constant as we range over $g^{-1}(1)$. Take $i \in B$ if and only if $z[i] = 1$. ■

Furthermore, the two key theorems about $\mu(g)$ still hold for $\mu_2(g)$: first, for all partial or total g, the quantum query complexity of the RFS_h^g problem is $\Omega\left((1-\mu_2(g))^{-h/2}\right)$. Second, if $\mu_2(g)$ is less than a positive constant (namely $\left(2-\sqrt{2}\right)/4 \approx 0.146$), then $\mu_2(g) = 0$, or equivalently g is a parity function. These theorems were claimed without proof in Section 4 of [1]. They are proven explicitly in my PhD thesis [2].

References

1. S. Aaronson (2003), *Quantum lower bound for recursive Fourier sampling*, Quantum Inf. Comput., Vol.3, pp. 165-174. quant-ph/0209060.
2. S. Aaronson (2004), *Limits on Efficient Computation in the Physical World*, UC Berkeley PhD thesis. quant-ph/0412143.