Reportes Científicos
de la FACEN

Vol. 8, Nº 1 (2017): 89-90

Comunicación Corta

http://dx.doi.org/10.18004/rcfacen2017080189-90

A BLOCK-SENSITIVITY LOWER BOUND FOR QUANTUM TESTING HAMMING DISTANCE

UN LÍMITE INFERIOR DE SENSIBILIDAD DE BLOQUE PARA PRUEBAS CUÁNTICAS DE LA DISTANCIA DE HAMMING

Marcos Villagra*

*Núcleo de Investigación y Desarrollo Tecnológico, Facultad Politécnica, Universidad Nacional de Asunción. Email: mvillagra@pol.una.py.

The Gap-Hamming distance problem is the promise problem of de- ciding if the Hamming distance h between two strings of length n is greater than a or less than b, where the gap $g = |a - b| \geq 1$ and a and b could depend on n. In this short note, we give a lower bound of $\Omega(\sqrt{n/g})$ on the quantum query complexity of computing the Gap- Hamming distance between two given strings of lenght n. The proof is a combinatorial argument based on block sensitivity and a reduction from a threshold function.

A generalized definition of the Hamming distance is the following: given two strings x and y, decide if the Hamming distance $h(x, y)$ is greater than a or less than b, with the condition that $b < a$. Note that this definition gives a partial boolean function for the Hamming distance with a gap. There is a entire body of work on the computation of a particular case of this notion of Hamming distance in the decision tree and communication models known as the *Gap-Hamming distance* (GHD) problem, which asks to differentiate the cases $h(x, y) \leq n/2 - n$ and $h(x, y) \geq n/2 + n$ (Woodruff, 2007). A lower bound on GHD implies a lower bound on the memory requirements of computing the number of distinct elements in a data stream (Indyk *et al.*, 2003). Chakrabarti *et al.* (2011) give a tight lower bound of $\Omega(n)$; their proof was later improved by Vidick (2011) and then by Sherstov (2011). For the Hamming distance with a gap of the form $n/2 \pm g$ for some given g, Chakrabarti and Regev (2011) also prove a tight lower bound of $\Omega(n^2/g^2)$. In the quantum setting, there is a communication protocol with cost $O\left(\sqrt{n}\log n\right)$ (Buhrman *et al.*, 1998).

Suppose we are given oracle access to input strings x and y. In this note, we prove a lower bound on the number of queries to a quantum oracle to compute the Gap-Hamming distance with an arbitrary gap, that is, for any given $g = a - b$.

Theorem 1.1.
Let $x, y \in \{0, 1\}^n$ and $g = a - b$ with $0 \leq b < a \leq n$. Any quantum query algorithm for deciding if $h(x, y) \geq a$ or $h(x, y) \leq b$ with bounded-error, with the promise that one of the cases hold, makes at least $\Omega(\sqrt{n/g})$ quantum oracle queries.

The proof is a combinatorial argument based on block sensitivity. The key ingredient is a reduction from a a threshold function. A previous result of Nayak *et al.* (1999) implies a tight lower bound of $\Omega\left(\sqrt{n/g} + \sqrt{h(n-h)}/g\right)$; their proof, however, is based on the polynomial method of Beals *et al.* (2001) and it is highly involved. The proof presented here, even though it is not tight, is simpler and requires no heavy machinery from the theory of polynomials.

Proof of Theorem 1.1

Let a, b be such that $0 \leq b < a \leq n$. Define the partial boolean function $GapThr_{a,b}$ on $\{0, 1\}^n$ as

$$GapThr_{a,b}(x) = \begin{cases} 1 & \text{if } |x| \geq a \\ 0 & \text{if } |x| \leq b. \end{cases} \quad (1)$$

To compute $GapThr_{a,b}$ for some input x, it suffices to compute the Hamming distance between x and the all 0 string. Thus, a lower bound for Gap-Hamming distance follows from a lower bound for $GapThr_{a,b}$.

Recibido: 26/5/2017

Aceptado: 20/6/2017

Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a function, $x \in \{0, 1\}^n$ and $B \subseteq \{1, \ldots, n\}$ a set of indices called a block. Let x^B denote the string obtained from x by flipping the variables in B. We say that f is *sensitive* to B on x if $f(x) \neq f(x^B)$. The block sensitivity $bs_x(f)$ of f on x is the maximum number t for which there exist t disjoint sets of blocks $B_1, \ldots, B_t$ such that f is sensitive to each B_i on x. The *block sensitivity* $bs(f)$ of f is the maximum of $bs_x(f)$ over all $x \in \{0, 1\}^n$.

From (Beals *et al.*, 2001) we know that the square root of block sen- sitivity is a lower bound on the bounded-error quantum query complexity. Thus, Theorem 1.1 follows inmediately from the lemma below.

Lemma 2.1. $bs(GapThr_{a,b}) = \Theta(n/g)$.

Proof. Let $x \in \{0, 1\}^n$ be such that $GapThr_{a,b}(x) = 0$ and suppose that $|x| = b$. To obtain a 1-output from x we need to flip at least $g = a - b$ bits of x. Hence, we divide the $n - b$ least significant bits of x in non-intersecting blocks, where each block flips exactly g bits. The number of blocks is $\left\lfloor \frac{n-b}{a-b} \right\rfloor$, which is at most $bs_x(GapThr_{a,b})$. To see that $\left\lfloor \frac{n-b}{a-b} \right\rfloor$ is the maximum number of such non-intersecting blocks, consider what happens when the size of a block is different from g. If the size of a block is less that g, then we cannot obtain a 1-output from x; if the size of a block is greater than g, then the number of blocks decreases. Thus, we have that $bs_x(GapThr_{a,b}) = \left\lfloor \frac{n-b}{g} \right\rfloor$.

For any x' with $|x'| < b$, we need to flip $a - b$ bits plus $b - |x'|$ bits. Using our argument of the previous paragraph, the size of each block is thus $g + b - |x'|$, and hence, $bs_{x'}(GapThr_{a,b}) = \left\lfloor \frac{n-|x'|}{g+b-|x'|} \right\rfloor$. Note that $bs_{x'}(GapThr_{a,b}) \leq bs_x(GapThr_{a,b})$.

For the case when $GapThr_{a,b}(x) = 1$ and $|x| = a$, to obtain a 0-output from x we need to flip at least g bits of x. Hence the same argument applies, and thus, $bs_x(GapThr_{a,b}) = \left\lfloor \frac{n-a}{g} \right\rfloor$.

Taking the maximum between the cases when $|x| = b$ and $|x| = a$, we have that $bs(GapThr_{a,b}) = \max\{(n-b)/g, (n-a)/g\} = \Theta(n/g)$.

REFERENCES

Beals, R., Buhrman, H., Cleve, R., Mosca, M. & De Wolf, R. (2001). Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4): 778-797.

Buhrman, H., Cleve, R. & Wigderson, A. (1998). Quantum vs. classical communication and computation. *Proceedings of the 30th annual ACM Symposium on Theory of Computing (STOC)*: 63–68.

Chakrabarti, A. & Regev, O. (2011). An optimal lower bound on the communication complexity of gap-hamming-distance. *Proceedings of the 43rd ACM Symposium on Theory of Computing (STOC)*: 51-60.

Indyk, P. & Woodruff, D. (2003). Tight lower bounds for the distinct elements problem. *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*: 283–288.

Nayak, A. & Wu, F. (1999). The quantum query complexity of approximating the median and related statistics. *Proceedings of the 31st annual ACM symposium on Theory of computing (STOC)*: 384–393.

Sherstov, A. (2011). The Communication Complexity of Gap Hamming Distance. *Electronic Colloquium on Computational Complexity*, Report TR11-063. 9 pp.

Vidick, T. (2011). A concentration inequality for the overlap of a vector on a large set, with application to the communication complexity of the gap- hamming-distance problem. *Electronic Colloquium on Computational Complexity*, Report TR11-051 9 pp.

Woodruff, D. (2007). *Efficient and Private Distance Approximation in the Communication and Streaming Models*. Ph.D. thesis, MIT, USA. 114 pp.