

Proof of Lower Bound Theorem

Additional assumption on the decentralized algorithm:

The current message holder has knowledge of the locations and long-range contacts of all nodes that have come in contact with the message.

We show that any decentralized algorithm even with this additional knowledge will have the polynomial lower bound if $r \neq 2$.

Case 1: $0 \leq r < 2$

Assume $n \geq n_0$, where n_0 is a sufficiently large fixed constant.

We lower bound the expected number of steps required for the message to travel from s to t , both generated uniformly at random from the grid.

$$\sum_{u \neq v} d(u, v)^{-r} \geq \sum_{j=1}^{n/2} (j) j^{-r}$$

$$= \int_1^{n/2} x^{1-r} dx \geq \frac{1}{(2-r)} ((n/2)^{2-r} - 1)$$

$$\geq \frac{1}{(2-r)2^{3-r}} n^{2-r}$$

if we assume $n \geq 2^{3-r}$.

Let U denote the set of nodes within lattice distance pn^δ of t .

Note that

$$|U| \leq 1 + \sum_{j=1}^{pn^\delta} 4j \leq 4p^2 n^{2\delta}$$

where we assume n is large enough that $pn^\delta \geq 2$.

Define $\lambda = ((2 - r)2^{7-r}qp^2)^{-1}$.

Let E' be the event that within λn^δ steps, the message reaches a node other than t with a long-range contact in U .

$$\Pr[E'] \leq \sum_{i \leq \lambda n^\delta} \Pr(E'_i)$$

where E'_i is the event that this happens in step i .

$$\begin{aligned}
\Pr[E'_i] &\leq \frac{q|U|}{\frac{1}{(2-r)2^{3-r}}n^{2-r}} \\
&\leq \frac{(2-r)2^{3-r}q4p^2n^{2\delta}}{n^{2-r}} \\
&= \frac{(2-r)2^{5-r}qp^2n^{2\delta}}{n^{2-r}}
\end{aligned}$$

$$\text{Thus } \Pr[E'] \leq \frac{(2-r)2^{5-r}\lambda qp^2n^{3\delta}}{n^{2-r}} \leq 1/4$$

Let F denote the event that the chosen source s and target t are separated by a lattice distance of at least $n/4$. We can show $\Pr[F] \geq 1/2$. Hence, $\Pr(F \cap E'^c) \geq 1/4$.

Let X denote the random variable equal to the number of steps taken for the message to reach t . Let E denote the event that the message reaches t within λn^δ steps.

$$\Pr[E|F \cap E'^c] = 0, \text{ hence } E[X|F \cap E'^c] \geq \lambda n^\delta.$$

$$E[X] \geq E[X|F \cap E'^c] \Pr[F \cap E'^c] \geq \frac{1}{4} \lambda n^\delta$$

Case 2: $r > 2$

Let $\epsilon = r - 2$. Consider a node u , and let v be a randomly generated long-range contact of u .

$$\begin{aligned}\Pr[d(u, v) > m] &\leq \sum_{j=m+1}^{2n-2} (4j)(j^{-r}) \\ &= 4 \sum_{j=m+1}^{2n-2} j^{1-r} \\ &\leq \int_m^{\infty} x^{1-r} dx \\ &\leq (r - 2)^{-1} m^{2-r} = \epsilon^{-1} m^{-\epsilon}\end{aligned}$$

$\beta = \frac{\epsilon}{1+\epsilon}$, $\gamma = \frac{1}{1+\epsilon}$ and $\lambda' = \frac{\min(\epsilon, 1)}{8q}$. Assume that $n^\gamma \geq p$.

Let E' be the event that in step i , the message reaches a node $u \neq t$ that has a long-range contact v satisfying $d(u, v) > n^\gamma$. Let $E' = \cup_{i \leq \lambda' n^\beta} E'_i$ that this happens in the first $\lambda' n^\beta$ steps.

We have

$$\begin{aligned} \Pr(E') &\leq \sum_{i \leq \lambda' n^\beta} \Pr(E'_i) \\ &\leq \lambda' n^\beta q \epsilon^{-1} n^{-\epsilon \gamma} \\ &= \lambda' q \epsilon^{-1} \leq \frac{1}{4} \end{aligned}$$

Rest of proof similar to the previous case.