Stemmer, Uri
Locally private \(k\)-means clustering. (English) Zbl 07415119

Summary: We design a new algorithm for the Euclidean \(k\)-means problem that operates in the local model of differential privacy. Unlike in the non-private literature, differentially private algorithms for the \(k\)-means objective incur both additive and multiplicative errors. Our algorithm significantly reduces the additive error while keeping the multiplicative error the same as in previous state-of-the-art results. Specifically, on a database of size \(n\), our algorithm guarantees \(O(1)\) multiplicative error and \(\approx n^{1/2+a}\) additive error for an arbitrarily small constant \(a > 0\). All previous algorithms in the local model had additive error \(\approx n^{2/3+a}\). Our techniques extend to \(k\)-median clustering.

We show that the additive error we obtain is almost optimal in terms of its dependency on the database size \(n\). Specifically, we give a simple lower bound showing that every locally-private algorithm for the \(k\)-means objective must have additive error at least \(\approx \sqrt{n}\).

MSC:
68T05 Learning and adaptive systems in artificial intelligence

Keywords:
differential privacy; local model; clustering; \(k\)-means; \(k\)-median

Software:
SuLQ

Full Text: Link

References:

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.