Bloomfilter Proof - Length equality

September 12, 2019

1 Main Theorem

The statement we wish to prove is of the form:

$$\forall ps, qs, P, \text{uniq ps}, \text{uniq qs},$$
$$\text{length ps} = \text{length qs},$$
$$\sum_{inds \in [0..n]^k | P\ inds} (ps \subseteq inds) = \sum_{inds \in [0..n]^k | P\ inds} (qs \subseteq inds)$$

We'll prove this by induction on ps The base case is trivial:

$$\sum_{inds \in [0..n]^k} (\emptyset \subseteq inds) = \sum_{inds \in [0..n]^k} (\emptyset \subseteq inds)$$
$$\sum_{inds \in [0..n]^k} 1 = \sum_{inds \in [0..n]^k} 1$$

The inductive step is:

$$\sum_{inds \in [0..n]^k | P\ inds} (p :: ps \subseteq inds) = \sum_{inds \in [0..n]^k | P\ inds} (q :: qs \subseteq inds)$$
$$\sum_{inds \in [0..n]^k | P\ inds \wedge p \in inds} (ps \subseteq inds) =$$
$$\sum_{inds \in [0..n]^k | P\ inds \wedge p \in inds} (qs \subseteq inds) =$$
$$\sum_{inds \in [0..n]^k | P\ inds} (p :: qs \subseteq inds) =$$

Now we must consider whether p is within qs

Case 1: $p \in qs$:

$$\sum_{inds \in [0..n]^k | P\ inds} (p :: [q | q \leftarrow qs, q \neq p] \subseteq inds) =$$

Using the IH on the ex

$$\sum_{inds \in [0..n]^k | P\ inds} (qs \subseteq inds) =$$

Case 2: $p \notin qs$:

Finally - using the fact that p can be interchanged with q (proven in Section 2)

$$\sum_{inds \in [0..n]^k | P\ inds \wedge q \in inds} (qs \subseteq inds) =$$
$$\sum_{inds \in [0..n]^k | P\ inds} (q :: qs \subseteq inds) =$$

2 Helper lemma

The statement we wish to prove is of the form:

$$\forall ps, p, \text{uniq ps},$$
$$\text{length ps} = \text{length qs},$$
$$\sum_{inds \in [0..n]^k | P \ inds} (ps \subseteq inds) = \sum_{inds \in [0..n]^k | P \ inds} (qs \subseteq inds)$$

We'll prove this by induction on ps The base case is trivial: