Hashing 2:

"Two-level hashing"
First level: table size \( O(N) \)
At each location: hash table (Collision-free)

Let

\[ i = \text{location index in the first level table}. \]

\[ c(i) = \text{num. of elements mapped to location } i \text{ in the first level table}. \]

Q: What should be the size of table at \( i \) for collision-free?

\[ c(i)^2 \]
Total table size:

\[ \sum_{i=1}^{M} C(i)^2 \]

Recall

\[ E[C] = \binom{N}{2} \cdot \frac{1}{M} \]

\[ E \left[ \sum_{i=1}^{M} \binom{C(i)}{2} \right] = \binom{N}{2} \frac{1}{M} \]

\[ E \left[ \sum_{i=1}^{M} (C(i)^2 - \sum_{i=1}^{M} C(i)) \right] = O(N) \quad \text{since} \quad M = O(N) \]

\[ E \left[ \sum_{i=1}^{M} C(i)^2 \right] = O(N) \]

\[ E \left[ \sum_{i=1}^{M} C(i) \right] = O(N) \]
Total table size = \( o(N) \)

Collision-free in \( O(N) \) space

"Perfect hashing"

\underline{\text{k-wise independent hash functions:}}

\textbf{Defn:} A family \( \mathcal{H} \) of hash functions \( U \rightarrow [M] \) is \( k \)-wise independent if for any \( k \) distinct keys \( x_1, \ldots, x_k \) and any \( k \) values \( d_1, \ldots, d_k \) we have

\[ P(h(x_1) = d_1 \land h(x_2) = d_2 \land \ldots \land h(x_k) = d_k) = \frac{1}{M^k} \]

For \( k = 2 \), "pairwise independent".
Suppose $H$ is $k$-wise indep. ($k > 2$)

1. $(k-1)$-wise indep.
2. For any $x \in \mathcal{U}$ and value $a \in [M]$
   
   \[ P \left[ h(x) = a \right] \leq \frac{1}{M} \]

3. Universal

Q: Which is stronger: pairwise indep. or universal?

E.g. Construction from last class $A$

\[ h(x) = Ax \]

$h(a) = 0$

\[ P \left[ h(a) = 0 \right] = 1 \]
Construction 1: 2-wise independent

\[ h(x) = Ax + b \quad \rightarrow \quad m \text{-length random binary vector.} \]

\[
\begin{pmatrix}
\text{(mxu)} \\
\text{(mx1)}
\end{pmatrix}
\]

(modulo 2)

Claim: ...is 2-wise independent

Q: num. of hash funs? \( 2^{um+m} \)

Q: bits to store? \( O(um) \)

Can we do this with fewer bits?
Construction 2 (using fewer bits)

- Fill first row and column with uniform random binary entries
- \( A_{i,j} = A_{i-1, j-1} \)
- \( h(x) = Ax + b \pmod{2} \)

Claim: \...
2-wise indep.