6.1

Suppose j is the number of seen symbols in the stream. Currently we are seeing a_{j+1}. We denote the sampling symbol as a_i. We maintain j and a_i. a_i is updated to a_{j+1} with probability $\frac{1}{j+1}$, and with probability $1-\frac{1}{j+1}$ remains the old value. If we keep a_i as our selection, then it will have been selected with probability $\left(1-\frac{1}{j+1}\right)\frac{1}{j}=\frac{1}{j+1}$, which is the correct probability for selecting a_i from the stream. Therefore, the space we have to maintain is $O(\log m+\log n)$.

6.3

see solution to 6.1.

each symbol is now a word.

6.8

$$H=\{h(x)=ax\ mod\ M\}$$

6.9

(a) No

Since the set $\{\mathrm{h}_{ab}\}$ can be determined by any two of equations $\mathrm{h}_{ab}(x)=u$, $\mathrm{h}_{ab}(y)=v$, $\mathrm{h}_{ab}(z)=w$, this set is not of hash functions 3-universal.

(b) $\mathrm{H}=\{\mathrm{h}_{abc}(x)=ax^2+bx+c\ mod\ p|0\le a,b,c<p\}$

With $\mathrm{h}_{abc}(x)=u$, $\mathrm{h}_{abc}(y)=v$, $\mathrm{h}_{abc}(z)=w$, we can get

$\begin{pmatrix} x^2 & x & 1 \\ y^2 & y & 1 \\ z^2 & z & 1 \end{pmatrix}\begin{pmatrix} a \\ b \\ c \end{pmatrix}=\begin{pmatrix} u \\ v \\ w \end{pmatrix}$ (mod p)

This equation has solution $\begin{pmatrix} a \\ b \\ c \end{pmatrix}=\begin{pmatrix} x^2 & x & 1 \\ y^2 & y & 1 \\ z^2 & z & 1 \end{pmatrix}^{-1}\begin{pmatrix} u \\ v \\ w \end{pmatrix}$, because $\mathrm{x}\neq\mathrm{y}\neq\mathrm{z}$.

So, there is a unique $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ that meet the criteria. Hence

$\mathrm{Prob}(\mathrm{h}_{abc}(x)=u,\mathrm{h}_{abc}(y)=v,\mathrm{h}_{abc}(z)=w)$

$=Prob(\text{ solution}\begin{pmatrix} a \\ b \\ c \end{pmatrix}=\begin{pmatrix} x^2 & x & 1 \\ y^2 & y & 1 \\ z^2 & z & 1 \end{pmatrix}^{-1}\begin{pmatrix} u \\ v \\ w \end{pmatrix})$

$=\dfrac{1}{p}*\dfrac{1}{p}*\dfrac{1}{p}$

6.10

Take k=3, Let H={(0,0,0),(0,1,1),(0,2,2),(1,0,1),(1,1,2),(1,2,0),(2,0,2),(2,1,0),(2,2,1)}