CS 498 algorithm Spring 2019 Ray Ying (xinruiy2@illinois.edu)
Homework 1 Problem 3 Aditya Pillai (apillai4@illinois.edu)

Solution:

(a) In order to have $A\omega = \gamma$ mod 2, we need each have every element in the output vector of size m mod 2 to be the same as every corresponding element in γ:

$P[A\omega[i] = \gamma[i] \bmod 2]$ for all $0 \le i \le m-1$

Since A and b is picked uniform at random, each element in A has probability exactly half of being 0 and exactly half of being 1. When you multiply matrix A with vector b, the index i of the result vector will be the vector multiplication of ith row in A and b. Since each element of the result vector has to mod 2, the index i of the result will based on the number of matching 1s in ith row in A and vector b(matching means in the same index of the vector b and the vector of ith row of A are both 1).
Therefore, let k be the number of 1s in the vector b, $n-k$ will be the number of 0s in the vector. The probability of the result from vector b and the vector of ith row of A mod 2 being 0 (binomial theorem applies here):

$$\frac{2^{(n-k)} \bullet \sum_{j=0}^{\lfloor (k/2) \rfloor} \binom{k}{2j}}{2^n} = \frac{\sum_{j=0}^{\lfloor (k/2) \rfloor} \binom{k}{2j}}{2^k} = \frac{2^{(k-1)}}{2^k} = \frac{1}{2}$$

Then, the probability of the result from vector b and the vector of ith row of A mod 2 being 1:

$$\frac{2^{(n-k)} \bullet \sum_{j=0}^{\lfloor (k-1/2) \rfloor} \binom{k}{2j+1}}{2^n} = \frac{\sum_{j=0}^{\lfloor (k-1/2) \rfloor} \binom{k}{2j+1}}{2^k} = \frac{1}{2}$$

Therefore, if $\gamma[i] = 1$ for $0 \le i \le n-1$, $P[A\omega[i] \bmod 2 = 1] = \frac{1}{2}$. If $\gamma[i] = 0$, $P[A\omega[i] \bmod 2 = 0] = \frac{1}{2}$. Since $P[A\omega[i] = \gamma[i] \bmod 2]$ is independent from $P[A\omega[j] = \gamma[j] \bmod 2]$ if $i \neq j$, therefore, the $P[A\omega = \gamma \bmod 2] = \prod_{i=1}^{m} P[A\omega[i] = \gamma[i]] = \frac{1}{2^m}$.

In order to prove that for every X_u and X_v for $v \neq u$, they are independent. We need to show pairwise independent, which implies we have to show that $Pr[Au + b = \alpha \wedge Av + b = \beta] = Pr[Au + b = \alpha] \bullet Pr[Av + b = \beta]$ for any $v \neq u$.

What we proved above, we can say that $Pr[Au + b = \alpha] = Pr[Av + b = \beta] = \frac{1}{2^m}$. Since $Pr[Au + b = \alpha \wedge Av + b = \beta] = Pr[A(u-v) = (\alpha - \beta) \wedge b = \beta - Av]$, if we can show that $Pr[A(u-v) = (\alpha - \beta) \wedge b = \beta - Av] = Pr[A(u-v) = (\alpha - \beta)] \cdot Pr[b = \beta - Av]$, then we can calculate $Pr[Au + b = \alpha \wedge Av + b = \beta]$.

Because $Pr[Au = \alpha \wedge Av = \beta) = Pr[A(u-v) = (\alpha - \beta)] = \frac{1}{2^m}$(we can substitute the γ with $\alpha - \beta$ and $u - v$ with w), for any $b = \beta - Av$, the probability of $Pr[A(u-v) = (\alpha - \beta)] = \frac{1}{2^m}$. By the principle of conditional probability, if $P(A|B) = P(A)$ then A and B are independent.

Therefore, $Pr[A(u-v)=(\alpha-\beta)\wedge b=\beta-Av]=Pr[A(u-v)=(\alpha-\beta)]\cdot Pr[b=\beta-Av]$ is true thus the probability of $Pr[A(u-v)=(\alpha-\beta)\wedge b=\beta-Av]=Pr[A(u-v)=(\alpha-\beta)]\cdot Pr[b=\beta-Av]=\frac{1}{2^m}\cdot Pr[b=\beta-Av]$. Once again, $Pr[b=\beta-Av]=Pr[Av=(\beta-b)]=\frac{1}{2^m}$.

Hence, $Pr[Au+b=\alpha\wedge Av+b=\beta]=Pr[A(u-v)=(\alpha-\beta)]\cdot Pr[b=\beta-Av]=Pr[A(u-v)=(\alpha-\beta)]\cdot Pr[b=\beta-Av]=\frac{1}{2^m}\cdot\frac{1}{2^m}=Pr[Au+b=\alpha]\bullet Pr[Av+b=\beta]$. We proved pairwise independent, then it is guaranteed that X_u and X_v are independent for $u\neq v$.

(b) We proved that randomized vectors multiplication from size n to size n mod 2 has $\frac{1}{2}$ chance of being 1 and $\frac{1}{2}$ chance of being 0. Having 2 randomized vector of size n', where $n'\leq n$, it will still satisfies as long as vectors are random based on the calculation in part a (we never have specific restriction on the size).

If a vector v of size n can divided into 2 parts and each part is a sub-vector of a randomized vector of size n, we can proved that $Pr[vb \bmod 2=1]=Pr[vb \bmod 2=0]=\frac{1}{2}$. Since we can divided b into same size of 2 sub-vector, the first sub-vector multiplies the first sub-vector of v and the second sub-vector multiplies the second sub-vector of v. The chance of first sub-vector multiplication has even 1s or odd 1s are both $\frac{1}{2}$, same for second sub-vector multiplication. Then, the probability of even number of 1s for vb is both sub-vector multiplication have odd 1s or both have even 1s, $\frac{1}{2}\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{2}$. Therefore, the probability of having odd number of 1s is also $\frac{1}{2}$.

We will divided the situation into 3 cases:

(1) $m<n$: If we look at the last row of A, we can divided the row into two parts: first part of a randomized list of size s and one sub-vector of size $n-s$ come from row 1. Since the first row is selected at random, its sub-vector is also random. Then we know the last bit of Ab mod 2 will have $\frac{1}{2}$ be 1 and $\frac{1}{2}$ be 0. Similar for all the row between row 1 and the last row as they can be divided into one sub-vector of the first row and one sub-vector of the first part of the randomized list the last row, they are both random. Therefore, each index of $A\omega$ has probability of $\frac{1}{2}$ to be 1 after mod 2.

(2) $m>n$: If m is slightly bigger than n, then the only change between $m<n$ is that the last row of A itself will be a random vector. Every row in between is the same, combination of one sub-vector from first row and one sub-vector from last row. Therefore, each index of $A\omega$ has probability of $\frac{1}{2}$ to be 1 after mod 2.

(3) $m>>n$ Then the difference with m slightly larger than n is there will be multiple first rows and last rows. Every $n\times n$ size of matrix in A can be treat as $m>n$, therefore, every row is the combination of one sub-vector from its corresponding "first row" and one sub-vector from its corresponding "last row". Therefore, each index of $A\omega$ has probability of $\frac{1}{2}$ to be 1 after mod 2.

Then we proved that every index of $A\omega$ has $\frac{1}{2}$ to be the same as γ.

We also need to prove for every two row i and row j in A, where $i\neq j$, if we can prove that $Pr[A[i]b \bmod 2]=Pr[A[i]b \bmod 2 \mid A[j]b \bmod 2]$ for any $i\neq j$, then every two rows are independent. For simplicity, let's make row i in A R_i and row j in A R_j. As we are looking for matching 1s, we only pay attention to the index in b that is 1, these indexes will be same for R_i and R_j. Let k be the sum of indexes of 1 in b, we are choosing number 1s in these indexes in R_j and R_i: $Pr[R_jb \bmod 2==0]=\frac{\sum_{j=0}^{\lfloor(k/2)\rfloor}\binom{k}{2j}}{2^k}=\frac{2^{(k-1)}}{2^k}=\frac{1}{2}$. Since we are looking over the same indexes for R_i and R_j, suppose for all x_j in these indexes in R_j has no intersection for all x_i in these indexes in R_i, then simply, the probability of $Pr[R_i b \bmod 2 == 0] = \frac{1}{2}$. If there are x_i that both in the indexes in R_i and R_j, seems we are shifting every row, x_i won't be in the same index for R_i and R_j, therefore, there will be some x_i are not in x_j. Suppose we have z number of duplicated in both indexes in R_i and R_j, we want to proved that what every number of 1s in these z duplicated x_i, the probability of $Pr[R_i b \bmod 2 == 0] = \frac{1}{2}$. If the duplicated number of z has odd 1s, $Pr[R_i b \bmod 2 == 0]$ under this condition, there should be odd 1s in the remaining of R_i to make the result mod 2 equal to 0. $Pr[R_i b \bmod 2 == 0] = \frac{\sum_{j=0}^{\lfloor (k-z)/2 \rfloor} \binom{(k-z)}{2j+1}}{2^{(k-z)}} = \frac{2^{(k-1-z)}}{2^{k-z}} = \frac{1}{2}$. When the duplicated number of z has even 1s, $Pr[R_i b \bmod 2 == 0]$ under this condition, there should be even 1s in the remaining of R_i to make the result mod 2 equal to 0. $Pr[R_i b \bmod 2 == 0] = \frac{\sum_{j=0}^{\lfloor (k-z)/2 \rfloor} \binom{(k-z)}{2j}}{2^{(k-z)}} = \frac{2^{(k-1-z)}}{2^{k-z}} = \frac{1}{2}$. Therefore, we proved that no matter how many the duplicated x_i are, the probability of R_i to be 0 and 1 are both 1/2 and it's not depended on whether R_j is 0 and 1. Therefore, by the principle of conditional probability, we can say that $Pr[A[i]b \bmod 2] = Pr[A[i]b \bmod 2 \mid A[j]b \bmod 2]$ for any $i \neq j$, thus every two rows are pairwise independent.

We will make an assumption for any $m \times n$ $Toeplitz$ matrix A, the every outcome of $A\omega$ will be equally likely.

Base case: When $m = 1$, there is only one row, the outcome mod 2 is one single number. It has $\frac{1}{2}$ chance of being 1 and $\frac{1}{2}$ chance of being 0, therefore, among all outcome, each outcome has same probability.

Induction step: Suppose it's true for $k \times n$, we want to prove that it holds for $(k+1) \times n$ still holds. Since we proved before $k \times n$, each outcome will have single probability in $k \times n$, when adding one row, the row itself will have $\frac{1}{2}$ probability of being 1 and $\frac{1}{2}$ of being 0. Since the row is pairwise independent to every row above, any outcome's of any row above will not be affect, and the outcome of $k+1$ row will still be uniformly distributed($\frac{1}{2}$ being 0 and $\frac{1}{2}$ being 1).

Therefore, the $(k+1) \times n$ $toeplitz$ will have every outcome uniformly distributed. Hence, we proved that for any $toeplitz$ A matrix of $m \times n$, each outcome is uniformly distributed. Therefore, with total number of outcomes are 2^m, the probability of $P[A\omega = \gamma \bmod 2] = \frac{1}{2^m}$.

(c) The number of bits we need to generated the $Toeplitz$ matrix $A \in \{0,1\}^{m \times n}$ is $logM + logN - 1$. The storage is also $logM + logN - 1$.

■