

## Section 9

### 1. (Pairwise Independence) (MU Exercise 15.2)

- (a) Let  $X, Y$  be numbers chosen independently and uniformly at random from  $\{0, \dots, n\}$ . Let  $Z$  be their sum modulo  $n + 1$ . Show that  $X, Y, Z$  are pairwise independent but not independent.
- (b) Extend this example to give a collection of random variables that are  $k$ -wise independent but not  $(k + 1)$ -wise independent.

### 2. (Hashing) (MU Exercise 15.3)

For any family of hash functions from a finite set  $U$  to a finite set  $V$ , show that, when  $h$  is chosen at random from that family of hash functions, there exists a pair of elements  $x$  and  $y$  such that:

$$\Pr(h(x) = h(y)) \geq \frac{1}{|V|} - \frac{1}{|U|} \quad (1)$$

This result should not depend on how the function  $h$  is chosen from the family.

### 3. (Pairwise Independence) (MU Exercise 15.6)

Our analysis of Bucket sort in Section 5.2.2 assumed that  $n$  elements were chosen independently and uniformly at random from the range  $[0, 2^k)$ . Suppose instead that  $n$  elements are chosen uniformly from the range  $[0, 2^k)$  in such a way that they are only pairwise independent. Show that, under these conditions, Bucket sort still requires linear expected time.