# Pairwise Random

Operations are mod 2.
Definition: Pairwise independence.
Suppose we take $h \in \mathcal{H}$ randomly, where $h : \{0,1\}^n$ to $\{0,1\}^m$. Then, for $x \neq y$, for $h$ chosen randomly from $\mathcal{H}$, $Prob(h(x) = a, h(y) = b) = 2^{-2m}$.
Theorem: Consider a function from $\{0,1\}^n$ to $\{0,1\}^m$.
If we use $C \in m \times n$ matrix and $d \in \{0,1\}^m$, then $\lambda C, d.[Cx + d]$ is pairwise random family.
Proof:
$Prob(Cx + d = a$ and $Cy + d = b)$
$= Prob(Cx - a = d$ and $C(y - x) = b - a)$
$= 2^{-m} * 2^{-m}$.

Theorem: Suppose $T \subseteq \{0,1\}^n$ and $2^k \leq |T| < 2^{k+1}$.
Then, for pairwise independent hash function family, $\{0,1\}^n$ to $\{0,1\}^{k+2}$

$Prob_{|h \in \mathcal{H}|}(|\{x : x \in T, h(x) = 0\}| = 1) \geq 1/8$

Proof: For any fixed $x \in T$,

$Prob(h(x) = 0$ and $h(y) \neq 0$, for all $y \in T - \{x\})$

$= Prob(h(x) = 0) * Prob(h(y) \neq 0$, for all $y \in T - \{x\} \mid h(x) = 0)$.

$= 2^{-k-2} * (1 - Prob(h(y) = 0$, for some $y \in T - \{x\} \mid h(x) = 0))$.

$\geq 2^{-k-2} * (1 - (|T| - 1) * 2^{-k-2}) \geq 2^{-k-2} * 1/2 = 2^{-k-3}$.

Considering all possible $x \in T$, we get that the probability of success as required is at least
$2^k * 2^{-k-3} = 1/8$.

# Reduction from SAT to U-SAT

- Formula $\varphi$, with variables $x_1, \ldots, x_n$.
- $\psi_k$: the formula for $Cx + d = 0$, assuming number of satisfying assigments is between $\geq 2^k$ and $< 2^{k+1}$.
- Thus, $\varphi \wedge \psi_k$ will have exactly one satisfying assignment with probability at least 1/8 if $\varphi$ is satisfyable with number of satisfying assignments in $[2^k, 2^{k+1})$ and $0$ satisfying assignments otherwise.
- Making formula for $\psi_k$: make formulas for $C_i \cdot x + d_i = 0$.
  $y_{i,1} = c_{i,1} \cdot x_1 + d_1$
  $y_{i,j+1} = y_{i,j} + c_{i,j+1} \cdot x_{j+1} + d_{j+1}$.
  $y_{i,n} = 0$