2. A collection $\mathcal{A}$ of events are *d-wise independent* if for any subset $\mathcal{B} \subseteq \mathcal{A}$ of size d or less, the probability that all events in $\mathcal{B}$ occur is the product of their probabilities. Consider the following generalization of Luby's scheme. For each $u \in \mathcal{Z}_p$, let A_u be any subset of $\mathcal{Z}_p$. Randomly select $x_0, \ldots, x_{d-1} \in \mathcal{Z}_p$. Show that the p events

$$x_0 + x_1 u + x_2 u^2 + \cdots + x_{d-1} u^{d-1} \quad \in \quad A_u$$

for $u \in \mathcal{Z}_p$ are d-wise independent. (*Hint.* Consider $d \times d$ Vandermonde matrices over $\mathcal{Z}_p$ with rows

$$(1,\ u,\ u^2,\ \ldots,\ u^{d-1})$$

shown in class to be nonsingular.)

3. Consider the following random NC algorithm for finding a maximal (not maximum) matching in an undirected graph $G = (V, E)$. The algorithm proceeds in stages. At each stage, a matching M is produced, and the matched vertices and all adjacent edges are deleted. Each stage proceeds as follows:

   (a) In parallel, each vertex u chooses a neighbor $t(u)$ at random. Set

   $$H := \{(u, t(u)) \mid u \in V\}\ .$$

   (b) If there are two or more edges $(u, t(u))$ in H with $t(u) = v$, then v chooses one of them arbitrarily and deletes the rest from H.

   (c) Let U be the set of vertices with at least one incident edge in H. Each vertex in the graph (U, H) has degree 1 or 2. If 2, it randomly selects one of its two incident edges as its favorite. If 1, it selects its one incident edge as its favorite.

   (d) For each edge $e \in H$, e is included in M if it is the favorite of both its endpoints.

   Show that M is a matching, and the expected number of edges deleted is at least a constant fraction of the remaining edges. Conclude that the expected number of stages before achieving a maximal matching is $O(\log m)$.

~~solutions to $Ax = z$ also has dimension $d - k$. In $\mathcal{Z}_p$, any such subspace has p^{d-k} elements. Thus~~

$$\begin{aligned} &\frac{1}{p^d} \sum_{z_u \in A_u,\ u \in \mathcal{B}} \left|\{(x_0, \ldots, x_{d-1}) \mid \bigwedge_{u \in \mathcal{B}} \sum_{i=0}^{d-1} x_i u^i = z_u\}\right| \\ &= \frac{1}{p^d} \sum_{z_u \in A_u,\ u \in \mathcal{B}} p^{d-k} \\ &= \frac{p^{d-k}}{p^d} \sum_{z_u \in A_u,\ u \in \mathcal{B}} 1 \\ &= \frac{1}{p^k} \prod_{u \in \mathcal{B}} a_u . \end{aligned}$$

3. The solution to this problem is very similar to the analysis of Luby's algorithm given in class. Recall from there that a vertex is *good* if

$$\sum_{u \in N(v)} \frac{1}{d(u)} \geq \frac{1}{3} .$$

Lemma A *For all good v,* $\Pr(v \in U) \geq \frac{1}{9}$.

Proof. If v has a neighbor u of degree 2 or less, then

$$\begin{aligned} \Pr(v \in U) &\geq \Pr(v = t(u)) \\ &\geq \frac{1}{2} . \end{aligned}$$

Otherwise $d(u) \geq 3$ for all $u \in N(v)$, and as in the analysis of Luby's algorithm, there must exist a subset $M(v) \subseteq N(v)$ such that

$$\frac{1}{3} \leq \sum_{u \in M(v)} \frac{1}{d(u)} \leq \frac{2}{3} .$$

Then

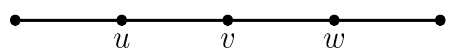
$$\begin{aligned} &\Pr(v \in U) \\ &\geq \Pr(\exists u \in M(v)\ v = t(u)) \\ &\geq \sum_{u \in M(v)} \Pr(v = t(u)) - \sum_{\substack{u, w \in M(v) \\ u \neq w}} \Pr(v = t(u) \wedge v = t(w)) \\ &\quad \text{(by inclusion-exclusion)} \\ &\geq \sum_{u \in M(v)} \Pr(v = t(u)) - \sum_{\substack{u, w \in M(v) \\ u \neq w}} \Pr(v = t(u)) \cdot \Pr(v = t(w)) \end{aligned}$$

$$
\begin{aligned}
& \text{(by pairwise independence)} \\
\geq\ & \sum_{u \in M(v)} \frac{1}{d(u)} - \sum_{u,w \in M(v)} \frac{1}{d(u)} \cdot \frac{1}{d(w)} \\
=\ & \Big(\sum_{u \in M(v)} \frac{1}{d(u)}\Big) \cdot \Big(1 - \sum_{w \in M(v)} \frac{1}{d(w)}\Big) \\
\geq\ & \frac{1}{3} \cdot \frac{1}{3} \quad = \quad \frac{1}{9}\ .
\end{aligned}
$$

□

Lemma B *For all v,* $\Pr(v \textit{ is matched} \mid v \in U) \geq \frac{1}{2}$.

Proof. There are several cases, depending on the number of H-neighbors of v and the number of H-neighbors of each H-neighbor of v. The situation minimizing the likelihood of v being matched is



There are eight possibilities for the choices of favorites of u, v, w, all equally likely. Of these, four give matchings for v. Thus

$$\Pr(v \text{ is matched} \mid v \in U) \quad \geq \quad \frac{1}{2}\ .$$

□

Combining Lemmas A and B, the probability that any particular good vertex is matched is at least $\frac{1}{18}$. The remainder of the argument is exactly like the analysis of Luby's algorithm given in class.

Note that the proof of Lemma A required only pairwise independence and the proof of Lemma B required only 3-wise independence, thus using Exercise 2 the algorithm can be made deterministic.