Bounded independence vs. moduli
Ravi Boppana, Johan Håstad, Chin Ho Lee and Emanuele Viola

Pseudorandomness
- Given a string sampled from a distribution $D$
- Can you test if it comes from $D$ or it is random?

A distribution $D$ fools a test $T$ if
$$|\Pr[T(D) \text{ accepts}] - \Pr[T(U) \text{ accepts}]| \leq 1/3,$$
where $U$ is the uniform distribution.

What are mod $m$ tests?
- Count the number of 1s in the input string
- Check if it is divisible by $m$

A mod $m$ test on $n$ bits accepts if the number of 1’s in the input is divisible by $m$.

What are $k$-wise uniform distributions on $n$ bits?
- Look at any of the $k$ bits of the distribution
- These $k$ bits must be uniformly distributed

A distribution $D$ on $n$ bits is $k$-wise uniform if its marginal distribution on every $k$ bits is uniform.

Example: a 2-wise uniform distribution on 3 bits
Sample a string from $\{000,011,101,110\}$ at random

These strings have the same parity

What can $k$-wise uniform distributions fool?
- Any test on $k$ bits (by definition)
- Combinatorial rectangles, low-depth circuits, halfspaces, etc.

For what values of $k$, every $k$-wise uniform distribution fools mod $m$ test?

Fails completely when $m = 2, k = n - 1$
- Look at our example
- All the strings in the distribution are accepted by mod 2 test!

What about $m = 3$?
- What is the largest $k$ such that there exists a $k$-wise distribution in which all strings are accepted by mod 3 test?
- Somewhat surprisingly, $k$ can still be $\Omega(n)$!

Our results
- If $k = \Omega(n/m)$ then every $k$-wise uniform distribution fools mod $m$ test.
- If $k = O(n/m^2 \log m)$ then some $k$-wise uniform distribution fails to fool mod $m$ test.

Techniques
- Fourier analysis, approximation theory, etc.

Approximation theory

<table>
<thead>
<tr>
<th>1</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>m</td>
<td>2m</td>
<td>3m</td>
</tr>
</tbody>
</table>

Symmetrization

Continuous approximation

<table>
<thead>
<tr>
<th>1</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>m</td>
<td>2m</td>
<td>3m</td>
</tr>
</tbody>
</table>

Low-degree approximation