# *Lecture 12: Polynomial representing* OR *mod m*

*Sivakanth Gopi*

*November 4, 2019*

In the last lecture, we have seen that we can construct matching vector families from low degree representations of OR $\mod m$. In this lecture, we will construct construct low degree representations of OR

**Definition 1** (Polynomial representation of OR $\mod m$)**.** *A polynomial $p(x_1, \ldots, x_n)$ represents* $\mathrm{OR}_n \mod m$ *(over $\{0,1\}$ basis) if:*

1. $p(0,0,\ldots,0) = 0 \mod m$ *and*

2. $p(x) \neq 0 \mod m$ *for all non-zero $x \in \{0,1\}^n$.*

We will now prove that there are (surprisingly) low degree polynomials representing $\mathrm{OR}_n \mod m$ if $m$ has multiple prime factors. Recall that when $m$ is a prime power, we need degree at least $n/(m-1)$.

**Theorem 2** ([BBR94])**.** *Let $m = p_1 p_2 \cdots p_t$ be a product of $t$ distinct primes. Then there exists a polynomial representation of* $\mathrm{OR}_n \mod m$ *of degree $O_m(n^{1/t})$.*

The best known lower bound on the degree of polynomial representations of $\mathrm{OR}_n \mod m$ is much weaker.

**Theorem 3** ([TB98])**.** *Suppose $m$ has $t$ distinct prime factors. Then the degree of a polynomial representating* $\mathrm{OR}_n \mod m$ *is at least $\Omega_m((\log n)^{\frac{1}{t-1}})$.*

To prove Theorem 2, we will need some number theoretic preliminaries.

**Lemma 4** (Chinese Remainder Theorem (CRT))**.** *Let $m = ab$ where $a, b$ are coprime. Then the rings $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ are isomorphic and the map $x \mapsto (x \mod a, x \mod b)$ is an isomorphism. Because it is an isomorphism, given $x_1 \in \mathbb{Z}/a\mathbb{Z}$ and $x_2 \in \mathbb{Z}/b\mathbb{Z}$, there exists a unique $x \in \mathbb{Z}/m\mathbb{Z}$ s.t. $x \mod a = x_1$ and $x \mod b = x_2$.*

By the CRT, we can think of $\mathbb{Z}/6\mathbb{Z}$ as the product of two rings $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. For example $5 \mapsto (1,2)$ under the above isomorphism.

If $p$ is a prime, then every function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ can be represented exactly as a polynomial. But not every function $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ is a polynomial. Try to construct one such function. Hint: CRT.

**Lemma 5.** *Let $p$ be a prime and $n \geq 1$, then $(x+y)^{p^n} = x^{p^n} + y^{p^n}$* $\mod p$.

*Proof.* We will prove the base case $n = 1$. The general case follows from easy induction. By binomial theorem, $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$.

$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{i(i-1)\dots 1}$ is divisible by $p$ for $1 \le i \le p-1$ since the denominator doesn't contain any $p$ multiples. Therefore $(x+y)^p = x^p + y^p \mod p$. $\square$

The map $\sigma : \mathbb{F}_{p^r} \to \mathbb{F}_{p^r}$ given by $x \mapsto x^p$ is called the Frobenius endomorphism. An endomorphism is a map from an object to itself which preserves its structure. Here $\sigma(xy) = \sigma(x)\sigma(y)$ trivially. Also $\sigma(x+y) = \sigma(x) + \sigma(y)$ because of Lemma 5. Therefore $\sigma$ respects both addition and multiplication operations of the field. It is an important map in the study of finite fields.

**Lemma 6** (Lucas's theorem)**.** *Let $p$ be a prime and $a, b$ be some non-negative integers. Suppose $a = a_0 + a_1 p + a_2 p^2 + \dots$ and $b = b_0 + b_1 p + b_2 p^2 + \dots$ be the base $p$ representation of $a, b$ (Note that $0 \le a_i, b_i \le p-1$). Then,*

$$\binom{a}{b} \equiv \prod_{i \ge 0} \binom{a_i}{b_i} \mod p.$$

*Here $\binom{u}{v}$ is defined to be $0$ if $u < v$ and $\binom{0}{0} = 1$.*

*Proof.* Let $x$ be some variable. We will write $(x+1)^a \mod p$ in two different ways and compare coefficients to get the desired identity. By binomial theorem, $(x+1)^a \mod p = \sum_{b=0}^{a} (\binom{a}{b} \mod p) x^b$. We will now write $(x+1)^a \mod p$ in a different way.

$$\begin{aligned}
(x+1)^a \mod p &= (x+1)^{\sum_i a_i p^i} \mod p \\
&= \prod_{i \ge 0} (x+1)^{a_i p^i} \mod p \\
&= \prod_{i \ge 0} (x^{p^i} + 1)^{a_i} \mod p && \text{(By Lemma 5)} \\
&= \prod_{i \ge 0} \left( \sum_{b_i \in \{0,1,\dots,p-1\}} \binom{a_i}{b_i} x^{b_i p^i} \right) \mod p \\
& && \text{(By binomial theorem)} \\
&= \sum_{b_0, b_1, b_2 \dots \in \{0,1,\dots,p-1\}} \left( \prod_{i \ge 0} \binom{a_i}{b_i} \right) x^{\sum_{i \ge 0} b_i p^i} \\
& && \text{(Terms after applying binomial theorem to each term)} \\
&= \sum_{b \ge 0} \left( \prod_{i \ge 0} \binom{a_i}{b_i} \right) x^b
\end{aligned}$$

By comparing coefficients of $x^b$, we get the desired identity. $\square$

**Lemma 7.** *Let $p$ be a prime and $r \ge 1$ be some positive integer. There exists a polynomial $f(x_1, \dots, x_n)$ of degree $p^r - 1$ such that for $x \in \{0,1\}^n$, $f(x) = 0 \mod p$ iff $\sum_{i=1}^{n} x_i$ is divisible by $p^r$.*

*Proof.* Let $a = \sum_{i=1}^{n} x_i$. Let $a = a_0 + a_1 p + \dots a_{r-1} p^{r-1} + a_r p^r + \dots$ be the base $p$ expansion of $a$.

$$\begin{aligned} p^r \text{ divides } a &\iff a_0 = a_1 = \cdots = a_{r-1} = 0 \\ &\iff a_i = \binom{a}{p^i} \mod p \qquad \text{(By Lucas's theorem)} \\ &\iff \binom{a}{p^i} \mod p = 0 \text{ for all } 0 \le i \le r-1 \\ &\iff 1 - \prod_{i=0}^{r-1}\left(1 - \binom{a}{p^i}^{p-1}\right) = 0 \mod p \end{aligned}$$

Now observe that

$$\binom{a}{b} = \binom{\sum_{i=1}^n x_i}{b} = \sum_{S\subset[n],|S|=b} \prod_{i\in S} x_i$$

which is a degree $b$ polynomial in $x_1, \ldots, x_n$. Therefore

$$f(x) = 1 - \prod_{i=0}^{r-1}\left(1 - \binom{\sum_{j=1}^n x_j}{p^i}^{p-1}\right)$$

is the required polynomial of degree $(p-1)(p^{r-1} + \cdots + p + 1) = p^r - 1$.

$\square$

*Proof of Theorem 2.* We have $m = p_1 p_2 \ldots p_t$. Choose $r_1, \ldots, r_t$ as small as possible such that $p_i^{r_i} > n^{1/t}$ for all $i \in [t]$. By Lemma 7, there exists polynomials $f_1, \ldots, f_t$ in variables $x_1, \ldots, x_n$ of degrees $p_1^{r_1} - 1, \ldots, p_t^{r_t} - 1$ respectively, such that $f_i(x) = 0 \mod p_i$ iff $p_i^{r_i}$ divides $\sum_i x_i$.

Therefore $f_i(x) = 0 \mod p_i \; \forall i \in [t]$ iff $\sum_i x_i$ is divisible by $p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t} > (n^{1/t})^t = n$. Since $\sum_i x_i$ is at most $n$, $f_i(x) = 0 \mod p_i \; \forall i \in [t]$ iff $x = (0, 0, \ldots, 0)$.

We can combine these polynomials using Chinese Remainder theorem, into one polynomial $f(x)$ such that $f(x) = 0 \mod m$ iff $f_i(x) = 0 \mod p_i \; \forall i \in [t]$. The degree of $f$ is at most the maximum degree among $f_1, \ldots, f_t$. Therefore $\deg(f) = O(n^{1/t})$. $\square$

## *References*

[BBR94] David A Mix Barrington, Richard Beigel, and Steven Rudich. Representing boolean functions as polynomials modulo composite numbers. *Computational Complexity*, 4(4):367–382, 1994.

[Gro99] Vince Grolmusz. Superpolynomial size set-systems with restricted intersections mod 6 and explicit ramsey graphs. *Combinatorica*, 20:2000, 1999.

[TB98] Gabor Tardos and DA Mix Barrington. A lower bound on the mod 6 degree of the or function. *Computational Complexity*, 7(2):99–108, 1998.