Lecture 6: Grolmusz' construction of a Matching Vector family

Lecturer: Zeev Dvir *Scribe: Kalina Petrova*

Degree of the OR function

Definition 6.1. A polynomial $g \in \mathbb{Z}_m[\mathbf{x}_1, \ldots, \mathbf{x}_n]$ *represents* a Boolean function $f : \{0,1\}^n \to \{0,1\} \mod m$ if

$$\forall \mathbf{x} \in \{0,1\}^n, g(\mathbf{x}) \begin{cases} = 0 \mod m & \text{if } f(\mathbf{x}) = 0 \\ \neq 0 \mod m & \text{if } f(\mathbf{x}) = 1 \end{cases}$$

Note that without loss of generality we can take g to be multilinear, that is, $\forall i \in [n], \deg(\mathbf{x}_i) \leq 1$ in g. This is because if $a \in \{0,1\}$, then $\forall h \geq 1, a^h = a$.

Definition 6.2. Let $\deg_p(f) = \min\{\deg(g) | g \text{ represents } f \mod p\}$

Lemma 6.1. Suppose $f \in \mathbb{F}_p[\mathbf{x}_1, \ldots, \mathbf{x}_n]$, where p is prime, is a multilinear non-zero polynomial of degree at most d, where $d > 0$. Then:

$$|\{\mathbf{a} \in \{0,1\}^n | f(\mathbf{a}) = 0\}| \leq 2^n - 2^{n-d},$$

where equality is achieved for $f = \prod_{i=1}^{d} \mathbf{x}_i$.

Proof. We can prove the lemma by induction on n. In the base case, $n = 1$, we have $d = 1$, so f is an expression linear in $\mathbf{x}_1$, and thus can have at most one zero, so the inequality holds. Suppose we have shown the inequality holds for polynomials of $n-1$ variables. We show that it also holds for any polynomial f with of n variables. We can express f in the following way: $f(\mathbf{x}_1, \ldots, \mathbf{x}_n) = \mathbf{x}_1 g(\mathbf{x}_2, \ldots, \mathbf{x}_n) + h(\mathbf{x}_2, \ldots, \mathbf{x}_n)$. Notice that the polynomial g is of degree at most $d-1$. Then, if we let $K = |\{\mathbf{a} \in \{0,1\}^{n-1} | g(\mathbf{a}) = 0\}|$, we have:

$$\begin{aligned} |\{\mathbf{a} \in \{0,1\}^n | f(\mathbf{a}) = 0\}| &\leq 2|\{\mathbf{a} \in \{0,1\}^{n-1} | g(\mathbf{a}) = 0\}| + |\{\mathbf{a} \in \{0,1\}^{n-1} | g(\mathbf{a}) \neq 0\}| \\ &= 2K + (2^{n-1} - K) \\ &= K + 2^{n-1} \\ &\leq 2^{n-1} - 2^{n-1-d+1} + 2^{n-1} \\ &= 2^n - 2^{n-d}, \end{aligned}$$

where the first inequality holds because if $g(\mathbf{x}_2, \ldots \mathbf{x}_n) \neq 0$, there is exactly one value of $\mathbf{x}_1$, for which $f(\mathbf{x}) = 0$, but if $g(\mathbf{x}_2, \ldots \mathbf{x}_n) = 0$, there might be up to two values of $\mathbf{x}_1$ such that $f(\mathbf{x}) = 0$. The second inequality holds by the inductive step.

$\square$

Example 6.1. Let $f(\mathbf{x}) = OR(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n) = \begin{cases} 0 & \text{if } \forall i \in [n], \mathbf{x}_i = 0 \\ 1 & \text{otherwise} \end{cases}$

Claim 6.1. If p is prime, then $deg_p(f) \geq \frac{n}{p-1}$.

Proof. Suppose that $g \in \mathbb{F}_p[\mathbf{x}_1, \ldots, \mathbf{x}_n]$ represents f. Take $h = 1 - g^{p-1}(\mathbf{x})$. Then

$$h(\mathbf{x}) = \begin{cases} 1 & \text{if } \forall i \in [n], \mathbf{x}_i = 0 \\ 0 & \text{otherwise} \end{cases}.$$

Let $\tilde{h}(\mathbf{x})$ be the multilinear polynomial such that $\forall \mathbf{a} \in \{0,1\}^n, \tilde{h}(\mathbf{a}) = h(\mathbf{a})$. We can get $\tilde{h}$ from h by replacing all occurrences of $\mathbf{x}_i^k$ with $\mathbf{x}_i$ for any $i \in [n]$ and $k \geq 1$. Notice that $\deg(\tilde{h}) \leq \deg(h) \leq (p-1)\deg(g)$. Now by Lemma 6.1, $|\mathbf{a} \in \{0,1\}^n | \tilde{h}(\mathbf{a}) = 0| \leq 2^n - 2^{n - \deg(\tilde{h})}$. On the other hand, we know that $\tilde{h}$ has exactly $2^n - 1$ zeros, so we get that $2^n - 1 \leq 2^n - 2^{n-\deg(\tilde{h})}$, therefore $\deg(\tilde{h}) \geq n$. From here and from $(p-1)\deg(g) \geq \deg(\tilde{h})$ we get that $\deg(g) \geq \frac{n}{p-1}$.

$\square$

Note that Claim 6.1 also holds if p is a power of some prime number [TB98].

Surprisingly, replacing $\mathbb{F}_p$ with $\mathbb{Z}_m$, where m is composite, allows a representation of OR to have much smaller degree.

Theorem 6.1 ([BBR92])**.** There exists a polynomial $g \in \mathbb{Z}_6[\mathbf{x}_1, \ldots, \mathbf{x}_n]$ that represents the OR function $\mod 6$ with $\deg(g) \leq O(\sqrt{n})$.

Proof. We are going to use the following theorem:

Theorem 6.2 (Chinese Remainder Theorem [Ste08])**.** Let $m = pq$, where p and q are different primes. Then $\mathbb{Z}_m \cong \mathbb{Z}_p \times \mathbb{Z}_q$, where the isomorphism $\varphi : \mathbb{Z}_m \to \mathbb{Z}_p \times \mathbb{Z}_q$ is given by $\varphi(k) = (k \mod p, k \mod q)$.

Corollary 6.1. Let $m = pq$ for p and q distinct primes. If $k = 0 \mod p$ and $k = 0 \mod q$, then $k = 0 \mod m$.

Example 6.2. Let $m = 6, p = 2, q = 3$. Then $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. The table below gives the isomorphism from $\mathbb{Z}_6$ to $\mathbb{Z}_2 \times \mathbb{Z}_3$.

k	$\varphi(k)$
0	$(0,0)$
1	$(1,1)$
2	$(0,2)$
3	$(1,0)$
4	$(0,1)$
5	$(1,2)$

Notice that addition and multiplication is preserved under φ, that is $\varphi(k_1+k_2) = \varphi(k_1) + \varphi(k_2)$. For instance, $2+4 = 0 \mod 6$ in $\mathbb{Z}_6$, and $(0,2)+(0,1) = (0,3) = (0,0)$ in $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Definition 6.3. $k \in \mathbb{Z}_6 \setminus \{0\}$ is a *zero divisor* if $\exists \ell \in \mathbb{Z}_6 \setminus \{0\}$ such that $k \cdot \ell = 0$.

Notice that k is a zero divisor if and only if at least one of the two elements of the pair $\varphi(k)$ is zero.

The Chinese Remainder Theorem extends to polynomials, that is, if p and q are prime numbers with $m = pq$, then $\mathbb{Z}_m[\mathbf{x}_1,\ldots,\mathbf{x}_n] \cong \mathbb{Z}_p[\mathbf{x}_1,\ldots,\mathbf{x}_n] \times \mathbb{Z}_q[\mathbf{x}_1,\ldots,\mathbf{x}_n]$, where the isomorphism $\varphi : \mathbb{Z}_m[\mathbf{x}_1,\ldots,\mathbf{x}_n] \to \mathbb{Z}_p[\mathbf{x}_1,\ldots,\mathbf{x}_n] \times \mathbb{Z}_q[\mathbf{x}_1,\ldots,\mathbf{x}_n]$ is given by $\varphi(f(x)) = (f(x) \mod p, f(x) \mod q)$. The reason why this extension of the φ we defined above works is because a polynomial on n variables modulo some number t is an expression that uses sums and products and so we can simply apply φ on all the coefficients.

Example 6.3. If $m = 6, p = 2, q = 3$, take $f(x) = 4\mathbf{x}_1^2 + 3\mathbf{x}_1\mathbf{x}_2 + 5\mathbf{x}_1 + 1 \in \mathbb{Z}_6[\mathbf{x}_1,\mathbf{x}_2]$. Then we have $\varphi(f(x)) = (\mathbf{x}_1\mathbf{x}_2 + \mathbf{x}_1 + 1, 2\mathbf{x}_1^2 + 2\mathbf{x}_1 + 1)$.

Moreover, the extension works in the other direction as well: given two polynomials $f_p \in \mathbb{Z}_p[\mathbf{x}_1,\ldots,\mathbf{x}_n]$ and $f_q \in \mathbb{Z}_q[\mathbf{x}_1,\ldots,\mathbf{x}_n]$, there exists a unique polynomial $f \in \mathbb{Z}_m[\mathbf{x}_1,\ldots,\mathbf{x}_n]$ such that $f \mod p = f_p$ and $f \mod q = f_q$ and $\deg(f) = \max\{\deg(f_p), \deg(f_q)\}$.

We give an outline of the proof of Theorem 6.1 here. For any $\mathbf{a} \in \{0,1\}^n$, let $\|\mathbf{a}\| = |\{i \in [n] | \mathbf{a}_i = 1\}|$, also referred to as the Hamming weight of $\mathbf{a}$. We construct two polynomials $f_2 \in \mathbb{Z}_2[\mathbf{x}_1,\ldots,\mathbf{x}_n]$ and $f_3 \in \mathbb{Z}_3[\mathbf{x}_1,\ldots,\mathbf{x}_n]$ such that, if $2^d \approx \sqrt{n}$ and $3^e \approx \sqrt{n}$, we have that $\forall \mathbf{a} \in \{0,1\}^n$:

$$\begin{aligned} f_2(\mathbf{a}) =& 0 \Leftrightarrow \|\mathbf{a}\| = 0 \mod 2^d \\ f_3(\mathbf{a}) =& 0 \Leftrightarrow \|\mathbf{a}\| = 0 \mod 3^e \end{aligned}$$

We make sure that f_2 and f_3 have degree approximately $\sqrt{n}$. Intuitively, the reason we can do this is because by the Schwartz-Zippel lemma, the number of zeros of f_2 and f_3, if they have degree approximately $\sqrt{n}$, is at most $\sqrt{n}2^{n-1}$, and the number of values of $\mathbf{a}$ such that the above condition requires that $f_2(\mathbf{a}) = 0$ or $f_3(\mathbf{a}) = 0$ is far smaller than $\sqrt{n}2^{n-1}$ – it's approximately $\sum_{i=1}^{\sqrt{n}} \binom{n}{i\sqrt{n}} \leq \sum_{i=1}^{\sqrt{n}} 2^{n-1} = \sqrt{n}2^{n-1}$. Then, using the Chinese Remainder Theorem, we combine f_2 and f_3 to get $f = (f_2, f_3) \in \mathbb{Z}_6[\mathbf{x}_1,\ldots,\mathbf{x}_n]$. This gives us

$$\begin{aligned} f(\mathbf{a}) = 0 &\Leftrightarrow f_2(\mathbf{a}) = 0 \text{ and } f_3(\mathbf{a}) = 0 \\ &\Leftrightarrow \|\mathbf{a}\| = 0 \mod 2^d \text{ and } \|\mathbf{a}\| = 0 \mod 3^e, \end{aligned}$$

and using the Chinese Remainder Theorem on $\mathbb{Z}_{2^d} \times \mathbb{Z}_{3^e} \cong \mathbb{Z}_{2^d 3^e}$, we have that

$$\|\mathbf{a}\| = 0 \mod 2^d \text{ and } \|\mathbf{a}\| = 0 \mod 3^e \Leftrightarrow \|\mathbf{a}\| = 0 \mod 2^d 3^e.$$

If we make sure that $2^d 3^e > n$, then we get

$$\begin{aligned} \|\mathbf{a}\| = 0 \mod 2^d 3^e &\Leftrightarrow \|\mathbf{a}\| = 0 \\ &\Leftrightarrow \mathbf{a} = \mathbf{0}, \end{aligned}$$

where we use $\mathbf{a} = \mathbf{0}$ to denote $\forall i \in [n], \mathbf{a}_i = 0$. Putting it all together, we get $f(\mathbf{a}) = 0 \Leftrightarrow \mathbf{a} = \mathbf{0}$, which is what we wanted to show.

Now we give the details of this intuition. We use the following lemma.

Lemma 6.2. If p is a fixed prime number, then $\forall d \in \mathbb{N}$, there exists a polynomial $f_p \in \mathbb{Z}_p[\mathbf{x}_1, \ldots, \mathbf{x}_n]$ such that $\deg(f) \leq p^d - 1$ and $\forall \mathbf{a} \in \{0,1\}^n$, $f_p(\mathbf{a}) = 0 \Leftrightarrow \|\mathbf{a}\| = 0 \mod p^d$.

Proof. Let $w = \|\mathbf{a}\| \in \{0, 1, \ldots, n\}$. Write w in its base p expansion: $w = \sum_{j=0}^{\infty} \mathbf{w}_j p^j$, with each $\mathbf{w}_j \in \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. Then we define f_p as a symmetric function in $\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_{d-1}$ of degree at most $d(p-1)$. More specifically, let $f_p(\mathbf{a}) = \prod_{j=0}^{d-1}(1-\mathbf{w}_j^{p-1}) - 1 \mod p$. Now we show that $f_p(\mathbf{a}) = 0 \Leftrightarrow \|\mathbf{a}\| = 0 \mod p^d$.

- First, suppose that $\|\mathbf{a}\| = w = 0 \mod p^d$. This means that $\forall j \in \{0, 1, \ldots, d-1\}, \mathbf{w}_j = 0$. Then $f_p(\mathbf{a}) = \prod_{j=0}^{d-1}(1 - \mathbf{w}_j^{p-1}) - 1 \mod p = \prod_{j=0}^{d-1} 1 - 1 \mod p = 1 - 1 \mod p = 0$.
- Now suppose that $f_p(\mathbf{a}) = 0$. Suppose that for some $j \in \{0, 1, \ldots, d-1\}$, $\mathbf{w}_j \neq 0$. Then by Fermat's Little Theorem $\mathbf{w}_j^{p-1} = 1 \mod p$, so $f_p(\mathbf{a}) = \prod_{j=0}^{d-1}(1 - \mathbf{w}_j^{p-1}) - 1 \mod p = 0 - 1 \mod p = p - 1 \neq 0$. We have reached a contradiction assuming that for some $j \in \{0, 1, \ldots, d-1\}, \mathbf{w}_j \neq 0$. Therefore, $\forall j \in \{0, 1, \ldots, d-1\}, \mathbf{w}_j = 0$, which implies that $w = 0 \mod p^d$.

Now we need to show that $\forall i \in \{0, 1, \ldots, d-1\}$, we can write $\mathbf{w}_j(\mathbf{a})$ as a low degree polynomial in $\mathbb{Z}_p[\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n]$, so that $f_p(\mathbf{a})$ has degree at most $p^d - 1$. We make use of Lucas' Theorem.

Theorem 6.3 (Lucas' Theorem [AL12])**.** Let p be a prime number and let $r, s \in \mathbb{N}$. If the base p expansions of r and s are $r = \sum_{j=0}^{\infty} \mathbf{r}_j p^j$ and $s = \sum_{j=0}^{\infty} \mathbf{s}_j p^j$, then $\binom{r}{s} = \prod_{j=0}^{\infty} \binom{\mathbf{r}_j}{\mathbf{s}_j} \mod p$, where we define $\binom{m}{n} = 0$ in case $m < n$.

We use Lucas' Theorem to show the following claim, which in turn will help us finish the proof of Lemma 6.2.

Claim 6.2. For any $j \in \{0, 1, \ldots, d-1\}$, $\mathbf{w}_j(\mathbf{x}) = Sym_{p^j}(\mathbf{x}) \mod p$, where $Sym_s(\mathbf{x}), s \in [n]$, is the s-th elementary symmetric polynomial, defined in the following way:

$$Sym_s(\mathbf{x}) = \sum_{S \subseteq [n], |S|=s} \prod_{j \in S} \mathbf{x}_j.$$

Proof. Notice that $Sym_{p^j}(\mathbf{a}) = \binom{w}{p^j}$, and by Theorem 6.3, $\binom{w}{p^j} = \binom{\mathbf{w}_j}{1} \prod_{j' \neq j} \binom{\mathbf{w}_{j'}}{0} = \binom{\mathbf{w}_j}{1} = \mathbf{w}_j$.

□

Using Claim 6.2, we get that $f_p(\mathbf{x}) = \prod_{j=0}^{d-1}(1 - Sym_{p^j}^{p-1}(\mathbf{x})) - 1$. This gives us $\deg(f_p) \leq \sum_{j=0}^{d-1} \deg(Sym_{p^j}(\mathbf{x}))(p-1) = \sum_{j=0}^{d-1} p^j(p-1) = p^d - 1$. Thus, we have a polynomial f_p of degree at most $p^d - 1$ such that $f_p(\mathbf{a}) = 0 \mod p$ if and only if $\|\mathbf{a}\| = 0 \mod p^d$, which completes the proof of Lemma 6.2.

□

Now we finish the proof of Theorem 6.1. Take d and e such that $\sqrt{n} < 2^d \leq 2\sqrt{n}$ and $\sqrt{n} < 3^e \leq 3\sqrt{n}$. By Lemma 6.2, there are two polynomials $f_2 \in \mathbb{Z}_2[\mathbf{x}_1, \ldots, \mathbf{x}_n]$ and $f_3 \in \mathbb{Z}_3[\mathbf{x}_1, \ldots, \mathbf{x}_n]$ such that $\deg(f_2) \leq 2^d - 1$, $deg(f_3) \leq 3^e - 1$, and $f_2(\mathbf{a}) = 0$ iff $\|\mathbf{a}\| = 0 \mod 2^d$, $f_3(\mathbf{a}) = 0$ iff $\|\mathbf{a}\| = 0 \mod 3^e$. Now by the Chinese Remainder Theorem for polynomials, $f = (f_2, f_3) \in \mathbb{Z}_6[\mathbf{x}_1, \ldots, \mathbf{x}_n]$ has degree at most $\max(\deg(f_2), \deg(f_3))$, which is at most $3\sqrt{n}$, and $f(\mathbf{a}) = 0$ iff $\|\mathbf{a}\| = 0 \mod 2^d 3^e$. Since $2^d 3^e > n$, $\|\mathbf{a}\| = 0 \mod 2^d 3^e$ iff $\|\mathbf{a}\| = 0$ iff $\forall i \in [n], \mathbf{a}_i = 0$. So $f(\mathbf{a}) = 0$ iff $\forall i \in [n], \mathbf{a}_i = 0$. Thus, f represents the OR function.

□

Obtaining a Matching Vector family

Using Theorem 6.1, we can get a Matching Vector family.

Theorem 6.4 ([Gro00]). There exists a Matching Vector family over $\mathbb{Z}_6^\ell$ of size $\ell^{\frac{C \log \ell}{\log^2 \log \ell}}$, where $C = \frac{1}{81}$.

Proof. We will use Theorem 6.1. If h is the number of variables in the OR function we are looking at, then the polynomial $f \in \mathbb{Z}_6[\mathbf{x}_1, \ldots, \mathbf{x}_h]$, which represents OR has $\deg(f) = O(\sqrt{h})$. Define the following 2^h polynomials: $\forall \mathbf{b} \in \{0,1\}^h$, let $g_{\mathbf{b}}(\mathbf{x}) = f((\mathbf{b} - \mathbf{x})^{\cdot 2})$, where $(\mathbf{a}_1, \ldots, \mathbf{a}_h)^{\cdot 2} = (\mathbf{a}_1^2, \ldots, \mathbf{a}_h^2)$. We will use the following claim:

Claim 6.3.

$$\forall \mathbf{a} \in \{0,1\}^h, g_{\mathbf{b}}(\mathbf{a}) \begin{cases} = 0 \mod 6 & \text{if } \mathbf{a} = \mathbf{b} \\ \neq 0 \mod 6 & \text{if } \mathbf{a} \neq \mathbf{b} \end{cases}$$

Proof. If $\mathbf{a} = \mathbf{b}$, then $g_{\mathbf{b}}(\mathbf{a}) = f(\mathbf{0}) = 0$. Otherwise, $(\mathbf{a} - \mathbf{b})^{\cdot 2} \neq \mathbf{0}$, so $f((\mathbf{a} - \mathbf{b})^{\cdot 2}) \neq 0 \mod 6$. $\square$

We now have two sets of vectors of size 2^h, $\mathbf{a} \in \{0,1\}^h$ and $\mathbf{b} \in \{0,1\}^h$, with the property outlined in Claim 6.3. This has a similar structure to Matching Vector families, but is not quite what we want – we want the dot product of $\mathbf{a}$ and $\mathbf{b}$ to have the property that $g_{\mathbf{b}}(\mathbf{a})$ has. To achieve this, we will "linearize" the two sets of vectors. We will need the following definitions.

Definition 6.4. For any polynomial $g \in \mathbb{Z}_6[\mathbf{x}_1, \ldots, \mathbf{x}_h]$ with $\deg(g) \leq d$, let $Coef(g) \in \mathbb{Z}_6^{\binom{h+d}{d}}$ be the coefficient vector of g under some fixed order of monomials.

Definition 6.5. Let $V_{\leq d} : \mathbb{Z}_6^h \to \mathbb{Z}_6^{\binom{h+d}{d}}$, the degree $\leq d$ Veronese embedding, be such that $\forall g \in \mathbb{Z}_6[\mathbf{x}_1, \ldots, \mathbf{x}_h]$ with $\deg(g) \leq d$, and $\forall \mathbf{a} \in \mathbb{Z}_6^h$, we have $g(\mathbf{a}) = \langle Coef(g), V_{\leq d}(\mathbf{a}) \rangle$

Example 6.4. Let $h = 2$, $d = 2$. If $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2)$, then $V_{\leq 2}(\mathbf{a}) = (1, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_1\mathbf{a}_2, \mathbf{a}_1^2, \mathbf{a}_2^2)$ and $Coef(g) = (g_0, g_1, g_2, g_3, g_4, g_5)$, where $g(\mathbf{x}) = g_0 + g_1\mathbf{x}_1 + g_2\mathbf{x}_2 + g_3\mathbf{x}_1\mathbf{x}_2 + g_4\mathbf{x}_1^2 + g_5\mathbf{x}_2^2$.

Now we can set $\Big(\mathbf{v}_{\mathbf{b}} = Coef(g_{\mathbf{b}})\Big)_{\mathbf{b} \in \{0,1\}^h}$ and $\Big(\mathbf{u}_{\mathbf{a}} = V_{\leq d}(\mathbf{a})\Big)_{\mathbf{a} \in \{0,1\}^h}$. Then $\Big(\big(\mathbf{v}_{\mathbf{b}}\big)_{\mathbf{b} \in \{0,1\}^h}, \big(\mathbf{u}_{\mathbf{a}}\big)_{\mathbf{a} \in \{0,1\}^h}\Big)$ is a Matching Vector family of size 2^h. This is because $\forall \mathbf{a}, \mathbf{b} \in \{0,1\}^h$, $\langle \mathbf{u}_{\mathbf{a}}, \mathbf{v}_{\mathbf{b}} \rangle = g_{\mathbf{b}}(\mathbf{a})$, which is 0 modulo 6 if and only if $\mathbf{a} = \mathbf{b}$. We have that $\forall \mathbf{a}, \mathbf{b} \in \{0,1\}^h$, $\mathbf{v}_{\mathbf{b}}, \mathbf{u}_{\mathbf{a}} \in \mathbb{Z}_6^{\binom{h+d}{d}}$. Note that $d \leq 3\sqrt{h}$. Set $l = \binom{h+d}{d}$. Then we have that $l = \frac{(h+d)!}{h!d!} = \frac{(h+1)\cdot(h+1)\cdot\dots\cdot(h+d)}{1\cdot 2\cdot\dots\cdot d} \leq (2h)^d \leq 2h^{3\sqrt{h}}$. Now the size of our Matching Vector family is 2^h, and we'll show that $2^h \geq l^{\frac{C \log l}{\log^2 \log l}}$, where $C = \frac{1}{81}$. Since $l^{\frac{C \log l}{\log^2 \log l}} = 2^{\frac{C \log^2 l}{\log^2 \log l}}$, it is enough to show that $h \geq \frac{C \log^2 l}{\log^2 \log l}$.

$$\frac{C\log^2 l}{\log^2\log l} \leq$$
$$\frac{\left(3\sqrt{h}\log(2h)\right)^2}{81\log^2\left(3\sqrt{h}\log(2h)\right)} \leq$$
$$\frac{9h\log^2(2h)}{81\log^2(\sqrt{h})} =$$
$$\frac{h\left(2\log(\sqrt{h})+1\right)^2}{9\log^2(\sqrt{h})} \leq$$
$$\frac{9h\log^2(\sqrt{h})}{9\log^2(\sqrt{h})} = h$$

Thus, we have a Matching Vector family of size $l^{\frac{\log l}{81\log^2\log l}}$.

□

Exercise 6.1. Extend the construction given in the proof of Theorem 6.4 to $\mathbb{Z}_m$, where $m = p_1 \dots p_t$, where $p_1, \dots, p_t$ are distinct primes, $t > 2$. What is the size of the Matching Vector family we can get in the case of t primes?

Exercise 6.2. Show that if p is prime, then any function $f : \mathbb{Z}_p^n \to \{0,1\}$ can be computed exactly by a polynomial $g \in \mathbb{Z}_p[\mathbf{x}_1, \dots, \mathbf{x}_n]$. Show that this is not true if we replace $\mathbb{Z}_p$ with $\mathbb{Z}_{pq}$ for p and q prime.

Exercise 6.3. Let $f : \{0,1\}^{2n} \to \{0,1\}$ be defined in the following way:

$$\forall \mathbf{a}, \mathbf{b} \in \{0,1\}^n, f(\mathbf{a}, \mathbf{b}) = \begin{cases} 0 & \text{if } \mathbf{a} = \mathbf{b} \\ 1 & \text{if } \mathbf{a} \neq \mathbf{b} \end{cases}$$

Find a polynomial $g \in \mathbb{Z}_6[\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{y}_1, \dots, \mathbf{y}_n]$ that represents f with $\deg(g) = O(\sqrt{n})$. Is there a polynomial $g' \in \mathbb{Z}_p[\mathbf{x}_1, \dots, \mathbf{x}_n, \mathbf{y}_1, \dots, \mathbf{y}_n]$ for p prime with $\deg(g') = O(\sqrt{n})$ that represents f?

References

[AL12] Manjil P. Saikia Alexandre Laugier. A new proof of lucas' theorem. *Notes on Number Theory and Discrete Mathematics*, 18(4):1–6, 2012.

[BBR92] David A. Mix Barrington, Richard Beigel, and Steven Rudich. Representing boolean functions as polynomials modulo composite numbers. In *STOC '92 Proceedings of the twenty-fourth annual ACM symposium on Theory of computing*, pages 455–461, 1992.

[Gro00] Vince Grolmusz. Superpolynomial size set-systems with restricted intersections mod 6 and explicit ramsey graphs. *Combinatorica*, 20:71–86, 2000.

[Ste08] William A. Stein. *Elementary Number Theory*. Springer-Verlag, 11 2008.

[TB98] Gabor Tardos and David A. Mix Barrington. A lower bound on the mod 6 degree of the OR function. *Computational Complexity*, 7:99–108, 11 1998.