Remember that U_n is the decoder-function introduced in the lecture for the development of the (k,s)-Lupanov-representation. This function is "universal" in the following sence.

Lemma 7.4

For each function $h \in B_r$ there is an assignment $\alpha(h) \in \{0,1\}^u$ for the y-variables such that

$$U_n(z, \alpha(h)) = h(z).$$

Proof:

For each $a \in \{0,1\}^r$ define

$$\alpha(h)_{(a)} := h(a).$$

Let

$$L_{\Omega_0}(n) := \max \{ L_{\Omega_0}(f) \mid f \in B_n \}.$$

As shown in Section 1 of the lecture, the corresponding measure

$$C_{\Omega_0}(n) := \max \{ C_{\Omega_0}(f) \mid f \in B_n \}$$

is equal $\Theta(\frac{2^n}{n})$.

The bound $L_{\Omega_0}(n)$ is a little bit larger as shown in the following theorem.

Theorem 7.9

For every constant $\varepsilon > 0$ and sufficiently large n,

$$L_{\Omega_0}(n) \geq (1-\varepsilon)\frac{2^n}{\log n}.$$

Proof:

Exercise

(use that the number of full binary trees with t leaves is $\leq 4^t$)

∎

Theorem 7.9 $\Rightarrow$

$$L_{\Omega_0}(r) \geq \frac{2^{r-1}}{\log r} = \frac{n}{2\log\log n}.$$

Hence, the function $U_n(z,y)$ also requires so many z-leaves. Of course, this lower bound is trivial because U_n depends on all its y-variables such that at least n leaves are required.

Goal:

Enlarging the complexity of $U_n(z,y)$ by considering Boolean functions of $2n$ variables of the form

$$f(x,y) = U_n(g(x), y),$$

where $g: \{0,1\}^n \to \{0,1\}^r$ is some easily computable Boolean operator.

$\leadsto$

We arrange a set x of n variables into an $r \times m$ - matrix where $m = \frac{n}{r}$.

$$x = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ & & \vdots & \\ x_{r1} & x_{r2} & \cdots & x_{rm} \end{pmatrix}.$$

We assume that n is divisible by $r = \log n$.

Consider $\varphi \in B_m$ which is applied to the rows of x.

$\leadsto$

For $1 \leq i \leq r$ define

$$z_i := \varphi(x_{i1}, x_{i2}, \ldots, x_{im})$$

The universal function induced by φ is the following Boolean function of $2n$ variables:

$$U_n^{\varphi}(x,y) := U_n(z_1, z_2, \ldots, z_r, y)$$

$$\text{where } z_i := \varphi(x_{i1}, x_{i2}, \ldots, x_{im}).$$

We call φ the generating function of $U_n^{\varphi}(x,y)$.

Andreev has considered the universal function generated by the parity function

$$\oplus(u_1, u_2, \ldots, u_m) := u_1 \oplus u_2 \oplus \ldots \oplus u_m.$$

The resulting function $U_n^{\oplus}(x,y)$ depends on

$2n$ variables where $n = 2^r$ is a power of two.

The function first computes for $1 \leq i \leq r$ the parities

$$z_i := x_{i_1} \oplus x_{i_2} \oplus \dots \oplus x_{im}$$

Then

$$j := (z) \quad \text{where } z = z_1 z_2 \dots z_r .$$

Finally, the value $U_n^{\oplus}(x,y)$ is obtained by

$$U_n^{\oplus}(x,y) := y_j .$$

Theorem 7.10

$$L_{\Omega_0}(U_n^{\oplus}) \geq n^{5/2 - o(1)}$$

~~14.07.~~

Proof:

Fix a Boolean function $h \in B_r$ requiring the largest Ω_0-formula.

Theorem 7.8 $\Rightarrow$

Size of such a formula

$$\geq \frac{2^{r-1}}{\log r} = \frac{n}{2 \log\log n}$$

Lemma 7.4 $\Rightarrow$

There is an assignment $b \in \{0,1\}^n$ of the y-variables of $U_n(z,y)$ such that

$$U_n(z,b) = h(z).$$

Thus, the Boolean function

$$f(x) := U_n^{\oplus}(x,b) = h\left(\bigoplus_{j=1}^{m} x_{1j}, \bigoplus_{j=1}^{m} x_{2j}, \dots, \bigoplus_{j=1}^{m} x_{rj}\right)$$

of n variables is a subfunction of $U_n^{\oplus}(x,y)$.

Let

$$k := \lceil r \cdot \ln(4r) \rceil.$$

Let ρ be a random partial assignment from R_k.

Our first goal is to show that with a large probability at least one variable in each row of x remains unfixed by ρ.

Claim 1:

Prob(ρ assigns an $*$ to each row of x) $\geq 3/4$.

Proof of claim:

Note that the restriction ρ assigns an $*$ to each single variable with probability

$$\frac{\binom{n-1}{k-1}}{\binom{n}{k}} = \frac{k}{n}.$$

$\Rightarrow$

The probability that some of r rows get no $*$ is

$$\leq r\left(1 - \frac{k}{n}\right)^m \leq r \cdot e^{-\frac{km}{n}}$$

$$\leq r \cdot e^{-\ln(4r)} = \frac{1}{4}$$

This proves the claim. $\square$

Lemma 7.3 $\Rightarrow$

(*) $\mathrm{Prob}\left[L_{\Omega_0}(f_\rho) \leq 4\left(\frac{k}{n}\right)^{3/2} L_{\Omega_0}(f)\right] \geq 3/4.$

Moreover, some of the assignments satisfy both Claim 1 and inequality (*).

Let ρ be such an assignment.

Claim 1 $\Rightarrow$

h is a subfunction of f_ρ.

Furthermore by (*)

$$L_{\Omega_0}(f_\rho) \leq 4\left(\frac{k}{n}\right)^{3/2} \cdot L_{\Omega_0}(f).$$

By the choice of k

$$k = \lceil r \ln(4r) \rceil = O(\log n \cdot \log\log n).$$

Note that by the choice of h

$$L_{\Omega_0}(h) \geq \frac{n}{2\log\log n}$$

Altogether, we obtain

$$L_{\Omega_0}(U_n^{\oplus}) \geq L_{\Omega_0}(f) \geq \frac{1}{4}\left(\frac{n}{k}\right)^{3/2} L_{\Omega_0}(f_\rho)$$

$$\geq \frac{1}{4}\left(\frac{n}{k}\right)^{3/2} L_{\Omega_0}(h)$$

$$\geq \frac{1}{4}\left(\frac{n}{k}\right)^{3/2} \frac{n}{2\log\log n}$$

$$\geq n^{5/2 - o(1)}.$$

$\blacksquare$

The proof of Theorem 7.10 actually gives the lower bound

$$L_{\Omega_0}(U_n^{\oplus}) = \Omega\left(n^{\Gamma + 1 - o(1)}\right)$$

where Γ is the shrinking exponent of standard formulas. Using Håstad's result, we obtain

$$L_{\Omega_0}(U_n^{\oplus}) \geq n^{3 - o(1)}.$$