Matematiska Institutionen,
KTH

**Problem till övning nr 8 den 28 april, Diskret matematik CINTE, SF1610, vt 14.**

**OBS.** Efter kontrollskriving nr 3 mellan kl 13.00 och 14.00 gör vi en kort paus, varefter följande problem diskuteras.

1. (E) Bestäm antalet RSA-krypton med parametrarna $n, e, d$ som man kan skapa med ett $n$ i intervallet $50 \leq n \leq 60$.

2. (E) En 1-felsrättande kod $C$ med längden $n = 11$ defineras av parity-check matrisen

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

   (a) Bestäm antalet ord $|C|$ i koden $C$.

   (b) Rätta orden 11000000000, 11111110111, och 01100000000.

   (c) Bestäm antalet ord som varken finns i den felkorrigerande koden $C$ och inte heller går att rätta.

3. (E) Undersök, t ex genom att skriva funktionerna nedan på en disjunktiv normalform, om nedanstående Booleska polynom representerar samma Booleska funktion:

$$(x\bar{y} + \bar{x})\bar{z}\bar{w} + \bar{y}(\bar{x} + z) \qquad \text{resp.} \qquad \bar{y}(\bar{w} + z) + \bar{x}\bar{z}(\bar{y} + y\bar{w})$$

4. (D) Bestäm antalet Booleska funktioner $f(x, y, z, u, w)$ från $\mathrm{B}^5$ till B sådana att

$$f(x, y, z, u, w) = f(x, y, z, \bar{u}, w), \quad \text{och} \quad f(0, 1, 0, 1, 0) = f(1, 0, 1, 0, 1).$$

5. (C) Karaktärisera samtliga Booleska funktioner $g$ och $h$ från $\mathrm{B}^n$ till B sådana att det finns minst en Boolesk funktion $f$ som löser "andragrads-ekvationen" $ff + fg = h$.

**SVAR.**

1. 44.
2. (a) 128
   (b) 11010000000, 11111110111, resp går ej att rätta.
   (c) 512.
3. Ja, de beskriver samma funktion.
4. 32768
5. Varje par av Booleska funktioner $g$ och $h$ från $\mathrm{B}^n$ till B ger en lösbar ekvation.