# AN EXTREMAL PROBLEM IN THE HYPERCUBE AND OPTIMIZATION OF ASYNCHRONOUS CIRCUITS

Carlos Gustavo T. de A. Moreira and Pablo Emanuel

IMPA-Instituto de Matemática Pura e Aplicada

Estrada Dona Castorina, 110 - Jardim Botanico

22460-320, Rio de Janeiro-RJ

Brasil

gugu@ impa.br pablo@ impa.br

Abstract. We prove that if $m \geq 2$ then the minimum $k \in \mathbb{N}$ such that the $k$-cube $\{0,1\}^k$ can be decomposed as the disjoint union of connected adjacent subsets satisfies $2\log_2 m - \log_2 \log_2 m - 1 \leq k \leq 2\lceil \log_2 m \rceil - \lfloor \log_2 \log_2 m \rfloor + 5$.

## Introduction

One of the main uses of electronic digital circuits is implementing finite state machines. There are two main types of digital circuits: the synchronous circuits, in which all transitions occur in discrete time, determined by a clock pulse; and the asynchronous circuits, in which transitions may occur at any time.

In a digital circuit, the state is determined by the binary value (voltage or current) in some components, so it can be viewed as a fixed length binary word.

In a synchronous circuit, all such bits change state at the same time in a transition, namely the time determined by the clock pulse. In the asynchronous case, however, when there is a transition, some bits may change faster than others, and the circuit passes through intermediate states, that do not correspond to actual intermediate states in the state machine that is being implemented. Clearly, this problem would not occur if, in every state transition, only one bit changes.

In general, it isn't possible to assign a $k$-bit word to each state of the machine satisfying the condition that every transition is a 1-bit transition (e.g. complete graph with 3 states). In [1], Huffmann proposed, as a solution to this problem, to assign more than one word per state, and implement the transitions as a sequence of 1-bit transitions, such that the initial words in this sequence corresponds to the initial state of the transition and the other ones to the final state. He proved that this could be done, for a complete state machine ( complete graph ), with $2\lceil \log_2 m \rceil - 1$ bits, where $m$ is the number of states. We prove in this paper a better bound, and prove that it can't be significatively improved.

A more precise formulation of this problem is as follows:

• Each state is assigned to a subset of the set of the $k$-bit words (that can be viewed as the $k$-cube $\left(\mathbb{Z}/2\mathbb{Z}\right)^k$).

• Each 1-bit transition is an edge of the cube, so each transition can be viewed as a path in the cube graph. The way to avoid undesired transient states is to assure that every transition is a 1-bit transition.

We will consider the worst case, namely the complete machine state (each state has transitions to every other state).

So, the problem is to find the minimum $k$ such that the $k$-cube can be decomposed as the union of $m$ disjoint connected subsets $A_1, \ldots, A_m$ such that for each $i$, $j \leq m$ there is a pair of adjacent vertices, one of them in $A_i$ and the other one in $A_j$ .

**Statements and Proofs**

**Definition:** We say that two subsets $A, B$ of a hypercube $\{0,1\}^k$ are adjacent if there are two adjacent points $x \in A$, $y \in B$.

**Proposition 1.** *If $m \geq 2$ and the $k$-cube $\{0,1\}^k$ can be divided as the union of $m$ disjoint adjacent subsets then $k \geq 2\log_2 m - \log_2 \log_2 m - 1$.*

**Proof:** Suppose that the $k$-cube $\{0,1\}^k$ can be divided in $m$ disjoint subsets $A_1, A_2, \ldots, A_m$ such that for each $i, j \leq m$ there are $x, y$ adjacent vertices such that $x \in A_i$, $y \in A_j$. Then there is one of the sets $A_i$ such that $A_i$ has at most $\lfloor 2^k/m \rfloor$ elements and, since any vertex has exactly $k$ adjacent vertices and every $A_j$ is adjacent to $A_i$ for $j \neq i$, we have $k\lfloor 2^k/m \rfloor \geq m - 1 \Rightarrow k2^k \geq m(m-1)$, and so we have $k \geq 2\log_2 m - \log_2 \log_2 m - 1$ for $m \geq 2$. $\square$

**Proposition 2.** If $m \geq 2$ then the $k$-cube $\{0,1\}^k$ can be decomposed as the disjoint union of connected adjacent subsets for some $k \leq 2\lceil \log_2 m \rceil - \lfloor \log_2 \log_2 m \rfloor + 5$

**Proof:** We will present a construction of a decomposition that satisfies the conditions of the proposition. We will use many times the fact that a face of any dimension of a hypercube is always connected.

Let $n = \lceil \log_2 m \rceil$, $r = \lfloor \frac{n}{2} \rfloor$, $p = \lfloor \log_2 r \rfloor$. We will construct a decomposition of the $k$-cube, where $k = 4 + 2n - p \leq 2\lceil \log_2 m \rceil - \lfloor \log_2 \log_2 m \rfloor + 5$.

Let us write a typical element of the $k$-cube as $\underline{u} = a_1 a_2 b c \ \underline{x_0} \ \underline{x_1} \ \underline{y}$, where $a_1, a_2, b$ and $c$ are bits, $\underline{x_0}$, $\underline{x_1}$ belongs to the $(n-r)$-cube $\{0,1\}^r$ and $\underline{y}$ belongs to the $(n-p)$-cube $\{0,1\}^{n-p}$.

The $r$-cube $\{0,1\}^r$ can be regarded as an $r$-dimensional vector space over $\mathbb{Z}/2\mathbb{Z}$ with the canonical basis $\{e_1, e_2, \ldots, e_r\}$, where $e_j$ is the vector that has the $j$-th coordinate equal to 1 and all the other coordinates equal to 0. Since $p \leq \log_2 r$, we have $2^p \leq r$ so there is a surjective function $\tilde{f}\colon \{e_1, e_2, \ldots, e_r\} \to \left(\mathbb{Z}/2\mathbb{Z}\right)^p$ that extends in a unique way to a linear function $f\colon \left(\mathbb{Z}/2\mathbb{Z}\right)^r \to \left(\mathbb{Z}/2\mathbb{Z}\right)^p$. It follows that given $v \in \left(\mathbb{Z}/2\mathbb{Z}\right)^r$ and $w \in \left(\mathbb{Z}/2\mathbb{Z}\right)^p$ there is an element $e_j$ of the canonical basis of $\left(\mathbb{Z}/2\mathbb{Z}\right)^r$ such that $f(v + e_j) = w$ (note that $v + e_j$ is adjacent to $v$). Since $n-r \geq r$ we have a linear function $g\colon (\mathbb{Z}/2\mathbb{Z})^{n-r} \to (\mathbb{Z}/2\mathbb{Z})^p$ analogous to $f$.

We may define now a function $F\colon \left(\mathbb{Z}/2\mathbb{Z}\right)^k \to \left(\mathbb{Z}/2\mathbb{Z}\right)^{2r}$ in the following way: for $\underline{u} = a_1a_2bc\ \underline{x_0}\ \underline{x_1}\ \underline{y} \in \left(\mathbb{Z}/2\mathbb{Z}\right)^k$ we look at the 3 bits $a_1$, $a_2$ and $b^*$, where $b^*$ is the sum modulo 2 of all the bits of $u$. If at least 2 of these 3 bits are equal to 0 we say that $\underline{u}$ is of type I and define $F(\underline{u}) = \underline{x_0}\ \underline{x_1}$; otherwise we say that $u$ is of type II and define

$$F(\underline{u}) = \begin{cases} f(\underline{x_0})\underline{y}, & \text{if } c=0 \\ g(\underline{x_1})\underline{y}, & \text{if } c=1 \end{cases}$$

We claim that the $2^n$ sets $F^{-1}(\underline{x})$, $\underline{x} \in (\mathbb{Z}/2\mathbb{Z})^n$ are disjoint, connected and adjacent, so, given a bijection $h\colon \left(\mathbb{Z}/2\mathbb{Z}\right)^{2r} \to \{1,2,\ldots,2^{2r}\}$ (for instance $h(\sigma_1,\sigma_2,\ldots,\sigma_{2r}) = 1 + \sum\limits_{\ell=1}^{2r} \sigma_\ell 2^{\ell-1}$), the decomposition of $\left(\mathbb{Z}/2\mathbb{Z}\right)^k$ as $A_1 \cup A_2 \cup \cdots \cup A_m$ where $A_i = (h\circ F)^{-1}(i)$ for $1 \leq i < m$, $A_m = \bigcup\limits_{j\geq m} (h\circ F)^{-1}(j)$ satisfies the conditions of our problem.

To prove this let us first verify that for each $\underline{x}, \underline{y}$ in $(\mathbb{Z}/2\mathbb{Z})^n$ there are adjacent vertices $\underline{u_1} \in F^{-1}(\underline{x})$, $\underline{u_2} \in F^{-1}(\underline{y})$. If $\underline{x} = \underline{\widetilde{x_o}}\ \underline{\widetilde{x_1}} \in \left(\mathbb{Z}/2\mathbb{Z}\right)^n = (\mathbb{Z}/2\mathbb{Z})^r \times (\mathbb{Z}/2\mathbb{Z})^{n-r}$ we can take $a_1 = 0$, $a_2 = 1$ and $b$ such that $b^* = 0$, and $\underline{\tilde{y}} \in \left(\mathbb{Z}/2\mathbb{Z}\right)^{2r-p}$ equal to the projection of $\underline{y}$ in the last $2r-p$ coordinates. We will have $F(01b0\underline{\widetilde{x_0}}\ \underline{\widetilde{x_1}}\ \underline{\tilde{y}}) = \underline{\tilde{x}}$, and we can take $\underline{x_0}'$ adjacent to $\underline{\widetilde{x_0}}$ such that $f(\underline{x_0}')$ is the projection of $\underline{y}$ in the first $p$ coordinates, so $01b0\underline{x_0}'\ \underline{\widetilde{x_1}}\ \underline{\tilde{y}}$ is adjacent to $01b0\underline{\widetilde{x_0}}\ \underline{\widetilde{x_1}}\ \underline{\tilde{y}}$ and $F(01b0\underline{x_0'}\ \underline{\widetilde{x_1}}\ \underline{\tilde{y}}) = \underline{y}$.

Now we will prove that the sets $F^{-1}(\underline{x})$ are connected. We can decompose $F^{-1}(\underline{x})$ as $B_{\underline{x}} \cup C_{\underline{x}}$ where

$$B_{\underline{x}} = \{\underline{u} \in F^{-1}(\underline{x}) \mid \underline{u} \text{ if of type I}\} \quad \text{and}$$

$$C_{\underline{x}} = \{\underline{u} \in F^{-1}(\underline{x}) \mid \underline{u} \text{ is of type II}\}.$$

The previous argument can be used to show that $B_{\underline{x}}$ and $C_{\underline{x}}$ are adjacent since there are adjacent elements $\underline{u_1} \in B_{\underline{x}}$ and $\underline{u_2} \in C_{\underline{x}}$. It is enough to prove that $B_{\underline{x}}$ and $C_{\underline{x}}$ are connected.

If $\underline{u} = a_1 a_2 bc\ \underline{x_0}\ \underline{x_1}\ \underline{y} \in B_{\underline{x}}$, then $\underline{u}$ is equal or adjacent to $\underline{u}' = 00bc\ \underline{x_0}\ \underline{x_1}\ \underline{y} \in B_{\underline{x}}$, and the set $\widetilde{B}_{\underline{x}}$ of the $\underline{u}' \in B_{\underline{x}}$; such that $a_1 = a_2 = 0$ is clearly connected, since it is equal to $\{\underline{u}' = 00bc\ \underline{x_0}\ \underline{x_1}\ \underline{y} \mid \underline{x_0}\ \underline{x_1} = \underline{x}\}$, that is a face of the hypercube $\{0,1\}^k$.

If $\underline{u} = a_1 a_2 bc\ \underline{x_0}\ \underline{x_1}\ \underline{y} \in C_{\underline{x}}$ then $\underline{u}$ is equal or adjacent to $\underline{u}'' = 11bc\ \underline{x_0}\ \underline{x_1}\ \underline{y} \in C_{\underline{x}}$. The set $\widetilde{C}_{\underline{x}} = \{\underline{u}'' \in C_{\underline{x}} \mid a_1 = a_2 = 1\}$ can be decomposed as $D_{\underline{x}} \cup E_{\underline{x}}$ where $D_{\underline{x}} = \{\underline{u}'' \in C_{\underline{x}} \mid a_1 = a_2 = 1 \text{ and } c = 0\}$ and $E_{\underline{x}} = \{\underline{u}'' \in C_{\underline{x}} \mid a_1 = a_2 = 1 \text{ and } c = 1\}$. To prove that $\widetilde{C}_{\underline{x}}$ (and so $C_{\underline{x}}$) is connected, it is enough to show that any element $\underline{u}_1 \in D_{\underline{x}}$ can be joined by a path in $\widetilde{C}_{\underline{x}}$ to any element $\underline{u_2} \in E_{\underline{x}}$. This is a consequence of the following facts:

- $\underline{u_1} = 11\tilde{b}0\ \underline{\widetilde{x_0}}\ \underline{\widetilde{x_1}}\ \underline{\tilde{y}}$ belongs to the connected set $L(\underline{u_1})$ contained in $D_{\underline{x}}$ defined as

$$L(\underline{u_1}) = \{11b0\ \underline{x_0}\ \underline{x_1}\ \underline{y} \in D_{\underline{x}} \mid \underline{x_0} = \underline{\widetilde{x_0}}, \underline{y} = \underline{\tilde{y}}\}.$$

- $\underline{u_2} = 11b'1\ \underline{x_0}'\ \underline{x_1}'\ \underline{\tilde{y}}$ belongs to the connected set $M(\underline{u_2})$ contained in $E_{\underline{x}}$ defined as

$$M(\underline{u_2}) = \{11b1\ \underline{x_0}\ \underline{x_1}\ \underline{y} \mid \underline{x_1} = \underline{x_1}', \underline{y} = \underline{\tilde{y}}\}$$

- $(11\tilde{b}0\ \underline{\widetilde{x_0}}\ \underline{x_1}'\ \underline{\tilde{y}}) \in L(\underline{u_1})$ and $(11\tilde{b}1\ \underline{\widetilde{x_0}}\ \underline{x_1}'\ \underline{\tilde{y}}) \in M(\underline{u_2})$ are adjacent. $\square$

## REFERENCES


[1] D. A. Huffman, *A Study of the Memory Requirements of Sequential Switching Circuits*, M.I.T., Res. Lab. Electron. Tech. Rept. 293, April, 1955.

[2] Z. Kohavi, *Switching and Finite Automata Theory,* McGraw-Hill computer science series, 1978