数理解析研究所講究録
156巻 1972年 20-33

論理回路による計算時間

九大理・情報研　　棚次 奎介

§1. はじめに

一般に論理回路を構成する場合，Switching理論における素子の数の最小化問題にみられるように，使用される論理素子の個数が議論される。一方，素子の個数だけを問題にするのは集積回路の開発などによって非現実的になりつつあるとする立場から，S. Winograd および P.M. Spira は信号が素子を通過する時間を1とみなし，回路に入力を入れてから出力を得るまでの時間（計算時間）を回路，ないしはその回路が実現する関数の複雑さの基準とした。彼らは加算，乗算，有限群演算などについて計算時間の下限を求め，その下限にできるだけ近い時間で計算を実行する実際の論理回路を構成している。この方法は，いわば回路の"広がり"を犠牲にして"深さ"をできるだけ縮めようとしているという点において，parallel computation の理論への一つの重要な手がかりともなろう。

ここでは，一つの出力線からみてお互いに分離可能な入力の集合を定義し，それに基づいて P.M. Spira によって与えられた計算時間の一般的下限と上限を統一した立場で述べ、それの直接の応用例をいくつか示すことにする。

§2. 計算時間の一般的下限

実際にある関数を実現する論理回路を構成する場合、現実的な要請として、次のような回路が考えられる：$Z_d=\{0,1,\cdots,d-1\}$ とする。$g: Z_d^m \to Z_d$ なる関数 g を実行する論理素子を d-値素子といい（図1），入力線の数を r 以下に制限した素子によって構成される組合わせ回路を (d,r)-回路という。ただし，$d, r \geq 2$ とする。また素子の出力線は分枝可能である。

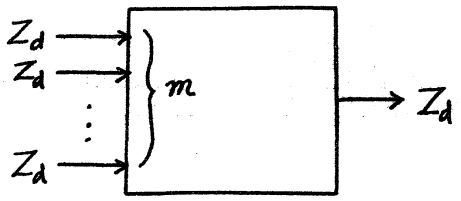

図 1.

ここでとりあつかう関数は全て次の形の f とする。すなわち，$f: X_1 \times X_2 \xrightarrow{\text{onto}} Y$ で X_1, X_2 は有限集合とする。以下ことわらない限り f で上の関数を表現する。

<u>定義2.1.</u>　回路 C が時間 t で f を計算するとは次のような場合をいう。整数 k_1, k_2, k_3 が存在し，時間0から $t-1$ までの入力が $[z_1(x_1), z_2(x_2)]$ であり続けるとき時間 t での出力が $h(f(x_1,x_2))$ であるような写像 $z_i: X_i \to Z_d^{k_i}$ $(i=1,2)$，

$h : Y \xrightarrow{1-1} Z_d^{k_3}$ が存在する。ここに $x_i \in X_i\ (i=1,2)$ とする。

定義 2.1 の回路 C の概略は図 2 に示される。

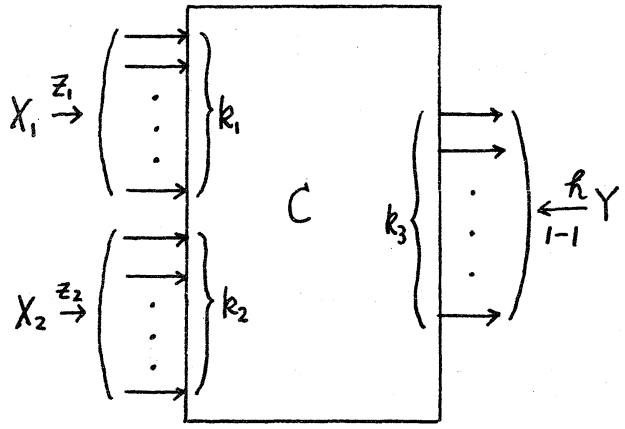

図 2

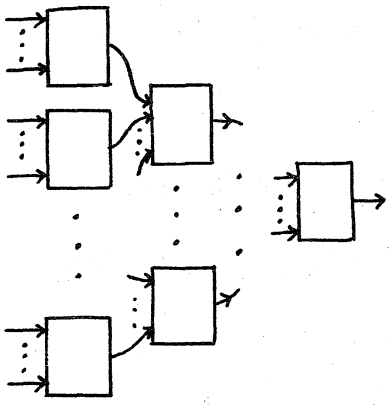

図 3

$h_j(y)$ を出力が $h(y)$ のときの j 番目の出力線上の値としよう。

<u>定義 2.2</u>　いま f を計算する (d,r)-回路を C とする。次のような集合 $S_1(j)$ を X_1 における C に対する h_j-可分集合という：$s_1 \neq s_2$ なる任意の $s_1, s_2 \in S_1(j)$ に対し、

$$h_j(f(s_1, x_2)) \neq h_j(f(s_2, x_2))$$

なる $x_2 \in X_2$ が存在する。

同様に $S_2(j)$ を定義できる。

(d,r)-回路において t 段目の論理素子はたかだか r^t 本の入力線（回路への）によって影響を受ける。なぜなら t 段目の論理素子が最も多くの入力によって影響を受けるのは図 3 のようにその素子までの回路構造が扇型の場合である。このこと

に注意して次の定理を得る．いま$\lceil x \rceil$をxより大きいかまたは等しいような最小の整数，$\lfloor x \rfloor$をxより小さいかまたは等しいような最大の整数とする．また$|S|$を集合Sの元の個数とする．

<u>定理 2.1</u>　Cを時間τでfを計算する(d, r)-回路とするとき

$$\tau \geq \max_{j} \left\{ \lceil \log_r (\lceil \log_d |S_1(j)| \rceil + \lceil \log_d |S_2(j)| \rceil) \rceil \right\}$$

証明．　j番目の出力線O_jが時間τでi番目の入力の組において$q < \lceil \log_d |S_i(j)| \rceil$本の入力線にのみ影響を受けるとすれば，$d^q < |S_i(j)|$より，$S_i(j)$の中に互いに$h_j$-可分でない要素が存在することになる．

Spira[3]は定理2.1をもとに、後に述べるような種々の関数に対する計算時間の下限を導いている．

この場合の下限とは"(d, r)-回路を用いてfを計算するには少なくともこれだけの時間が必要である"という意味であるが、実際には、その下限にどれほど近い段数の(d, r)-回路を作りうるかということが当然興味のあるところである．構成された(d, r)-回路の段数は"(d, r)-回路を用いてfを計算するにはたかだかこれだけの時間で十分である"という意味での下限となる．

§3. 計算時間の一般的上限

$f: X_1 \times X_2 \to Y$ において W は Y の任意の部分集合とする。$f_W: X_1 \times X_2 \to \{0,1\}$ を次のように定義する:

$$f_W(x_1, x_2) = \begin{cases} 1 & f(x_1, x_2) \in W \text{ のとき} \\ 0 & f(x_1, x_2) \notin W \text{ のとき} \end{cases}$$

<u>定義 3.1</u>　$x_{11} \in X_1$ と $x_{12} \in X_1$ が $E_W^{(1)}$-同値であるとは任意の $x_2 \in X_2$ に対して $f_W(x_{11}, x_2) = f_W(x_{12}, x_2)$ となることをいう。同様に X_2 の上の $E_W^{(2)}$-同値を定義する。

$E_W^{(i)}(x)$ を、x を含む $E_W^{(i)}$-同値類とする $(i=1,2)$.

<u>補題 3.1</u>　任意の $x_1 \in X_1$, $x_2 \in X_2$ に対して

$$f(E_W^{(1)}(x_1), E_W^{(2)}(x_2)) \subseteq W$$

または

$$f(E_W^{(1)}(x_1), E_W^{(2)}(x_2)) \cap W = \phi$$

のどちらかである。

証明.　$x_1' \in E_W^{(1)}(x_1)$, $x_2' \in E_W^{(2)}(x_2)$ に対して $f(x_1', x_2') \in W$ で、$x_1'' \in E_W^{(1)}(x_1)$, $x_2'' \in E_W^{(2)}(x_2)$ としよう。そのとき

$$f(x_1', x_2') \in W \Rightarrow f(x_1'', x_2') \in W \Rightarrow f(x_1'', x_2'') \in W.$$

したがって　$f(E_W^{(1)}(x_1), E_W^{(2)}(x_2)) \subseteq W$.

<u>定義 3.2</u>　$\mathcal{E}_W^{(i)} = \{E_{W1}^{(i)}, E_{W2}^{(i)}, \cdots, E_{Wn_i}^{(i)}\}$ は $\{E_W^{(i)}(x) \mid x \in X_i\}$ の異なる元の全体とする $(i=1,2)$.

一般に $x_1 \in X_1$ を与えて，$f(x_1, E^{(2)}_{wv}) \subseteq W$ なる $E^{(2)}_{wv} \in \mathcal{E}^{(2)}_w$ は一つ以上存在する．

<u>定義 3.3</u>　$M^{(1)}_w = \max_{x_2 \in X_2} |\{E^{(1)}_{wu} \in \mathcal{E}^{(1)}_w : f(E^{(1)}_w, x_2) \subseteq W\}|$

$M^{(2)}_w = \max_{x_1 \in X_1} |\{E^{(2)}_{wv} \in \mathcal{E}^{(2)}_w : f(x_1, E^{(2)}_{wv}) \subseteq W\}|$

f_W を計算する (d, r)-回路を構成する．構成法の概略は次のとうりである：　$x_1 \in X_1$ を与えたとき

$$f_W(x_1, x_2) = 1 \Leftrightarrow f_W(E^{(1)}_w(x_1), x_2) = 1$$

である．したがって $E^{(1)}_w(x_1)$ によって x_1 を code し，$f(E^{(1)}_{wu}, x_2) \subseteq W$ なる $E^{(1)}_{wu}$ の list として x_2 を code できる．$E^{(1)}_w(x_1)$ が x_2 に対する $E^{(1)}_{wu}$ の list に含まれるかどうかによって $f_W(x_1, x_2) = 1$ かどうかを決定できる．

<u>補題 3.2</u>　$f: X_1 \times X_2 \to Y$ で $W \subseteq Y$ とする．f_W, $\mathcal{E}^{(1)}_w$, $\mathcal{E}^{(2)}_w$, $M^{(1)}_w$, $M^{(2)}_w$ はいずれも今までに定義された通りとする．そのとき f_W を時間

$$\tau_W = 1 + \min_{i=1,2} \left\{ \left\lceil \log_r \left\lceil \frac{1}{\lfloor r/2 \rfloor} \left\lceil \log_d |\mathcal{E}^{(i)}_w| \right\rceil \right\rceil \right\rceil + \left\lceil \log_r M^{(i)}_w \right\rceil \right\}$$

で計算する (d, r)-回路が存在する．

証明　$L = \lceil \log_d |\mathcal{E}^{(1)}_w| \rceil$ とする．

まず $z: X_1 \to Z^L_d$ を次のような code 関数とする．

$$z(x_1) = \underbrace{(0, 0, \cdots, 0)}_{L} \qquad f(E_W^{(1)}(x_1), x_2) \cap W = \phi \text{ のとき}$$

$$z(x_1) = z(x_1') \qquad E_W^{(1)}(x_1) = E_W^{(1)}(x_1') \text{ のとき}$$

$z_1 : X_1 \to Z_d^{LM_W^{(1)}}$ は

$$z_1(x_1) = \underbrace{z(x_1)\, z(x_1) \cdots z(x_1)}_{M_W^{(1)}}$$

によって与えられる．ただし，$a = (a_1, a_2, \cdots, a_s)$，$b = (b_1, b_2, \cdots, b_t)$ のとき $ab = (a_1, a_2, \cdots, a_s, b_1, b_2, \cdots, b_t)$ とする．

$z_2 : X_2 \to Z_d^{LM_W^{(1)}}$ を定義しよう．$E_1, E_2, \cdots, E_{m(x_2)}$ は $f(E_j, x_2) \subseteq W$ $(1 \le j \le m(x_2) \le M_W^{(1)})$ を満たす $\mathcal{E}_W^{(1)}$ の元とする．E がそれ以外の $\mathcal{E}_W^{(1)}$ の元ならば補題 3.1 によって $f(E, x_2) \cap W = \phi$ である．そこで

$$z_2(x_2) = (z(x_{11})\, z(x_{12}) \cdots z(x_{1m(x_2)}), 1, 1, \cdots, 1)$$

とする．ここに $x_{1j} \in E_j$ $(1 \le j \le m(x_2))$ で，最後の 1 は $L(M_W^{(1)} - m(x_2))$ 個並んでいる．

$f_W(x_1, x_2)$ を計算するために $z_1(x_1) = (a_1, a_2, \cdots, a_{LM_W^{(1)}})$，$z_2(x_2) = (b_1, b_2, \cdots, b_{LM_W^{(1)}})$ とする．そのとき $0 \le s \le M_W^{(1)}$ なる整数 s が存在して，$sL+1 \le j \le (s+1)L$ なる全ての j に対して $a_j = b_j$ ならば $f_W(x_1, x_2) = 1$ である．

上の (d, r)-回路は次のように述べることができる：回路の第 1 段では $\lfloor r/2 \rfloor$ 個の a_i と $\lfloor r/2 \rfloor$ 個の b_i が pairwise に等しいかどうかを check するための d-値素子を $(1/\lfloor r/2 \rfloor)L$ 個用意．

する。ある素子に対してその入力が互いに全て等しければ出力は1であり，それ以外の場合は0である。第二段以降は，全ての入力が1のときのみ出力が1であるようなたかだかr本の入力線をもつd-値素子で扇型の回路を構成する（図4）。この扇型回路は「$\log_r \lceil (1/\lfloor r/2 \rfloor)L \rceil \rceil$段である。

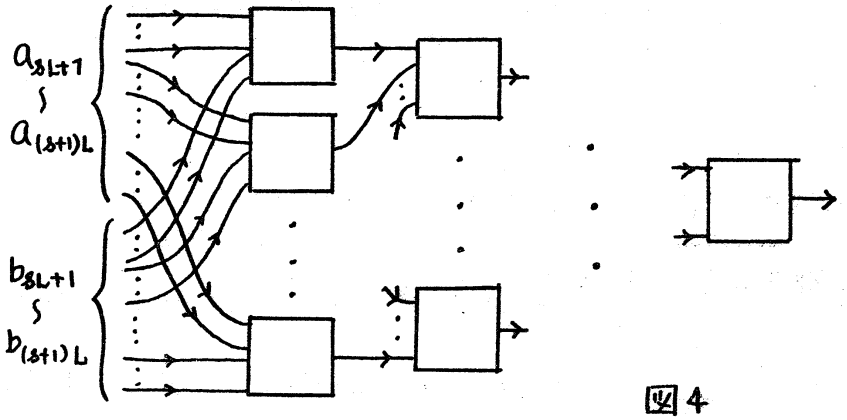

図4

上記の回路を$M_W^{(1)}$個並列に並べることによって$f(x_1, x_2) \in W$ならばそのうちの1つの出力が1であるような(d,r)-回路が得られる。したがってその回路の上に「$\log_r M_W^{(1)}$」段の扇型回路を構成することによってf_Wを計算する(d,r)-回路を得る。

<u>定義3.4</u>　$\mathcal{W} = \{W_1, W_2, \cdots, W_n\}$は$Y$の空でない部分集合の族とする。もし

$$\{W_i \mid y_1 \in W_i\} = \{W_i \mid y_2 \in W_i\} \Rightarrow y_1 = y_2$$

が成立するなら$\mathcal{W}$は完備であるという。但し，$Y = \bigcup_{i=1}^{n} W_i$とする。

<u>定理3.1</u>　$\mathcal{W}$はYの部分集合の完備族とする．そのとき時間

$$\tau = \max_{W_i \in \mathcal{W}} \{\tau_{W_i}\}$$

でfを計算する(d,r)-回路が存在する．ただし，τ_{W_i}は補題3.2で与えた計算時間とする．

証明　補題3.2で述べたようなf_{W_i}を計算する(d,r)-回路を並列に並べるとき$\mathcal{W}$の完備性からその出力のcode関数は1-1である。

通常の関数の殆んどは任意の$W \in \mathcal{W}$に対して$M_W^{(i)} = 1$となるようなYの部分集合の完備族をもつ．

<u>定義3.5</u>　次の様なYの部分集合の完備族$\mathcal{W}$が存在する場合fは正則であるという：任意の$W \in \mathcal{W}$を与える．任意の$x_2 \in X_2$に対して$f(E_W^{(1)}, x_2) \subseteq W$なる$E_W^{(1)} \in \mathcal{E}_W^{(1)}$はたかだか1つ存在する。または任意の$x_1 \in X_1$に対して$f(x_1, E_W^{(2)}) \subseteq W$なる$E_W^{(2)} \in \mathcal{E}_W^{(2)}$はたかだか1つ存在する．そしてそのような$\mathcal{W}$を正則な完備族という。

例えば有限体上での加算，乗算，有限群演算などは完備族$\mathcal{W} = \{\{y\} \mid y \in Y\}$をもつ正則な関数である．

fに対して$\mathcal{W}$が定義3.5を満たす完備族とすれば、明らかに任意の$W \in \mathcal{W}$に対して$\min_i \{M_W^{(i)}\} = 1$である．ここに，定理3.1の直接の系を得る。

<u>系3.1</u>　$f: X_1 \times X_2 \to Y$ は正則で，$\mathcal{W}$ は Y の部分集合の正則な充備族とする．そのとき時間

$$T = 1 + \lceil \log_r \lceil \frac{1}{\lfloor r/2 \rfloor} \lceil \log_d \left(\max_{W \in \mathcal{W}} \{ \min_{i=1,2} \{ |\mathcal{E}_W^{(i)}| \} \} \right) \rceil \rceil \rceil$$

で f を計算する (d, r)-回路が存在する。

次に f が正則な場合について定理2.1と定理3.1の結果を比較してみよう．

<u>補題3.3</u>　C は定理3.1において f の i 番目の変数に関して構成された (d, r)-回路であるとする．ただし，C の j 番目の出力線からは f_{W_j} の計算結果を得るものとする。$S_i(j)$ は f の i 番目の変数における C に対する h_j-可分集合とする。そのとき

$$|S_i(j)| = |\mathcal{E}_{W_j}^{(i)}|.$$

証明．　$h_j(f(x_1, x_2)) = f_{W_j}(x_1, x_2)$ なので $E_{W_j}^{(i)} \in \mathcal{E}_{W_j}^{(i)}$ の元は互いに h_j-可分でない。逆に

$$x_1, x_2 \in S_i(j) \Rightarrow E_{W_j}^{(i)}(x_1) \neq E_{W_j}^{(i)}(x_2).$$

したがって　$|S_i(j)| = |\mathcal{E}_{W_j}^{(i)}|$.

この補題に基いて系3.1を書き直せば

<u>系3.2</u>　f は正則関数とする．そのとき時間

$$T = 1 + \lceil \log_r \lceil \frac{1}{\lfloor r/2 \rfloor} \lceil \log_d \max_j \{ \min_i \{ |S_i(j)| \} \} \rceil \rceil \rceil$$

で f を計算する (d, r)-回路が存在する．

以上で得られた f の計算時間の f が正則な場合の上限(系3.2)と下限(定理2.1)を比べればその差はたかだか1であることが知れる。なぜなら

$$\max_j \{\lceil \log_r(\lceil \log_d |S_1(j)| \rceil + \lceil \log_d |S_2(j)| \rceil)\rceil\}$$
$$\geq \lceil \log_r(2\lceil \log_d(\max_j\{\min_i\{|S_i(j)|\}\})\rceil)\rceil$$

および

$$\lceil \log_r 2x \rceil \geq \lceil \log_r \lceil \frac{1}{\lfloor r/2 \rfloor} \cdot x \rceil \rceil$$

より

$$\max_j \{\lceil \log_r(\lceil \log_d |S_1(j)| \rceil + \lceil \log_d |S_2(j)| \rceil)\rceil\}$$
$$\geq \lceil \log_r \lceil \frac{1}{\lfloor r/2 \rfloor} \lceil \log_d(\max_j\{\min_i\{|S_i(j)|\}\})\rceil\rceil\rceil$$

となるから、したがって定理3.1の構成法はかなり良いことが理解できる。

§4 応用

まず、補題3.3の結論によってSpira[3,4]による導出よりも簡単に有限群演算の(d,r)-回路による計算時間の上限を求める。

<u>定義4.1</u> Gは有限群であるとする。$\{G\}=\{e\}$のとき$\delta(G)=1$とする。それ以外のときは$g \in G-\{e\}$に対して$\delta(g)$はgを含まないGの最大部分群の位数とし、$\delta(G)=\min_{g\in G-\{e\}}\{\delta(g)\}$とする。

<u>命題 4.1</u>　Gを任意の有限群とする。そのとき時間

$$t = 1 + \lceil \log_r \lceil \frac{1}{\lfloor r/2 \rfloor} \lceil \log_d \frac{|G|}{\delta(G)} \rceil \rceil \rceil$$

でGにおける演算を実行する (d,r)-回路が存在する。

証明.　まず $\max_j |S_1(j)| = |G|/\delta(G)$ なることを示す。

$\delta(G) > 1$ と仮定する。$g \neq e$ なる任意の $g \in G$ に対して g を含まない位数 $\delta(g)$ の部分群 K_g が存在する。$\mathcal{D}$ をGにおける K_g の左剰余類の全体だとすれば $\mathcal{D}$ は正則な完備集合となる。S は K_g の左剰余類からの各代表元（1つずつ）からなる集合とする。そのとき $j=1,2,\cdots,|\mathcal{D}|$ に対して $|S| = |S_1(j)|$ で $|S| = |G|/|K_g|$ となる。したがって $\max_j |S_1(j)| = |G|/\delta(G)$。

$\delta(G)=1$ ならば正則な完備族として $\mathcal{D} = \{\{g\} \mid g \in G\}$ を採用すれば明らかに $\max_j |S_1(j)| = |G|/\delta(G)$。

同様に $\max_j |S_2(j)| = |G|/\delta(G)$ を得る。

その他 Winograd らによって与えられた上限と下限のうちいくつかを以下に述べる。

<u>命題 4.2</u>　Gを有限群とする。CをGにおける演算を実行する (d,r)-回路とするとき その計算時間は

$$t \geq \lceil \log_r 2 \lceil \log_d \frac{|G|}{\delta(G)} \rceil \rceil$$

である。

<u>定義 4.1</u>　整数 m に対して $Q_m = \mathrm{l.c.m}\{1, 2, \cdots, m\}$, $\gamma(N) = \min\{m \mid Q_m \geqq N\}$ とする。

<u>命題 4.3</u>　$\varphi: Z_N \times Z_N \to Z_{2N-1}$ は $\varphi(a, b) = a + b$ とする。そのとき時間 τ_φ で φ を計算する (d, r)-回路が存在する。ここに

$$\tau_\varphi = 1 + \lceil \log_r \lceil \frac{1}{\lfloor r/2 \rfloor} \lceil \log_d \gamma(2N-1) \rceil \rceil \rceil .$$

<u>命題 4.4</u>　$\psi: \{1, 2, \cdots, N\} \times \{1, 2, \cdots, N\} \to \{1, 2, \cdots, N^2\}$ は $\psi(a, b) = a \cdot b$ とする。そのとき時間 τ_ψ で ψ を計算する (d, r)-回路が存在する。ここに

$$\tau_\psi = 1 + \lceil \log_r \lceil \frac{1}{\lfloor r/2 \rfloor} \lceil \log_d \gamma(2 \lfloor \log_2 N \rfloor - 1) \rceil \rceil \rceil .$$

<u>命題 4.5</u>　C_φ を時間 τ_φ で φ を計算する (d, r)-回路, C_ψ を時間 τ_ψ で ψ を計算する (d, r)-回路とする。そのとき

$$\tau_\varphi \geqq \lceil \log_r 2 \lceil \log_d \gamma(\lceil \frac{N}{2} \rceil) \rceil \rceil ,$$

$$\tau_\psi \geqq \lceil \log_r 2 \lceil \log_d \gamma(\lceil \frac{\lfloor \log_2 2N \rfloor}{2} \rceil) \rceil \rceil$$

である。

参考文献

1. S. Winograd, On the time required to perform addition, J. ACM, 12, No. 2 (1965), 277–285.

2. S. Winograd, On the time required to perform multiplication, J. ACM, 14, No. 4 (1967), 793–802.

3. P.M. Spira, The time required for group multi-plication, J.ACM, 16, No.2 (1969), 235-244.

4. P.M. Spira, On the computational complexity of finite functions and semigroup multiplication, Inform. Sci., 2 (1970), 35-49.

5. 棚次奎介, 論理回路による計算時間, 日本数学会応用数学分科会予稿集 (1971, 10月).

(於 京都 1972, 2, 24.)