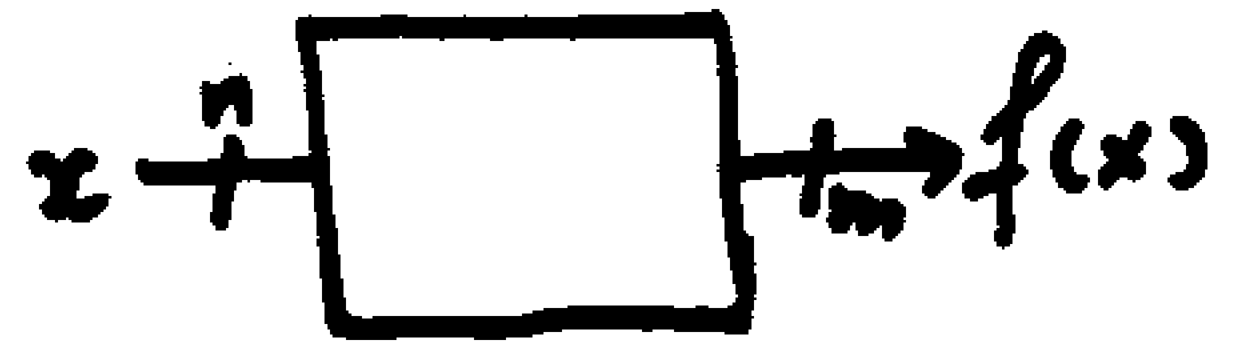
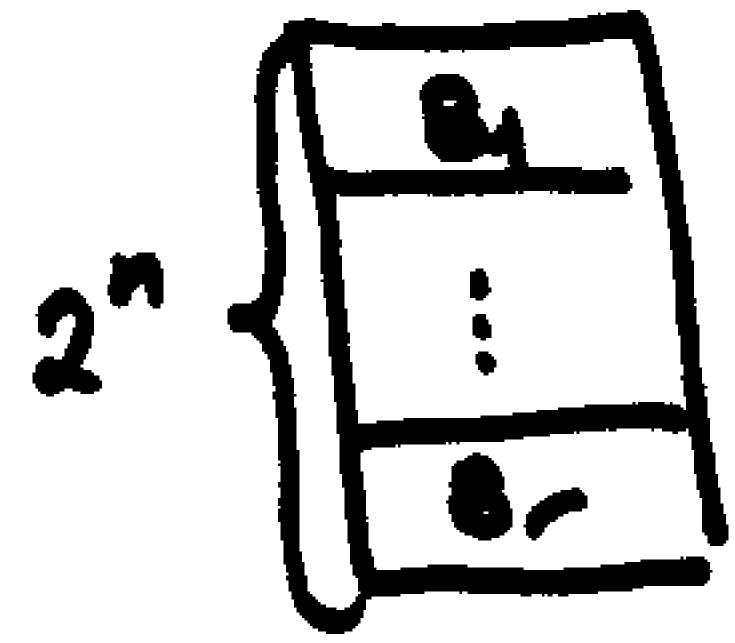
Linear Checks SC753

154

General Case





$\sum_{x \in B_i} f(x) = K$ for any B_i

Testing time $T = |B_i|$ - number of elements in B_i

T depends on $f \Rightarrow T(f)$

Problem: For a given f find an optimal partition $\{B_1, \dots, B_r\}$ minimizing $T(f) = |B_i|$

Solution:
M.G. Karpovsky, "Error Detection for Polynomial Computations"
IEE J. on Computer & Digital Techniques
Feb 1979, 2 pp 48-56

Estimations on $T(f)$

1. Let σ - binary $n \times n$ matrix and $\varphi(x) = f(\sigma x \oplus y)$ for some fixed y
(All additions are modulo 2)

Then $T(\varphi) = T(f)$

2. Nontrivial checks $(T(f) < 2^n)$

Necessary condition

$$\sum_x f(x) = d \cdot 2^i \quad ; d, i \text{ - integers}$$

3. Lower Bound

$$T(f) \geq 2^n \min_{\{x \mid f(x) \neq 0\}} f(x) \left(\sum_x f(x) \right)^{-1}$$

$$\sum_x f(x) \neq 0$$

Linear checks for Polynomials

$$f(x) = x^s + a_1 x^{s-1} + a_2 x^{s-2} + \dots + a_{s-1} x + a_s$$

Solution: Construct a maximal linear code V with the distance $s+1$

1) Code is a set of binary n-vectors
2) Code is linear if a componentwise XOR of a two vectors from the code is a vector from the code
3) A distance between two vectors is a number of components where these vectors do not coinside
4) A distance of a code is a min distance between two vectors from the code

<u>Example 1</u> $n=3$

$$f(x) = x^2 - 1$$

$$V = \begin{pmatrix} 000 \\ 111 \end{pmatrix} \quad V^{\perp} = \begin{matrix} 000 \\ 011 \\ 110 \\ 101 \end{matrix} = B_1$$

$$B_2 = \begin{matrix} 001 \\ 010 \\ 111 \\ 100 \end{matrix} \qquad \sum_{x \in B_1} f(x) = \sum_{x \in B_2} f(x) = K_f$$

$$K_f = 0^2 - 1 + 3^2 - 1 + 6^2 - 1 + 5^2 - 1 = 67$$

∴ All polynomials of the same degree have the same linear checks (but with different K)

∴ All blocks have the same size

∴ Size of a block depends on S and n.

For any two vectors

$x = (x_1, x_2, \dots, x_n)$

$y = (y_1, y_2, \dots, y_n)$

scalar product:

$$(x, y) = x_1 y_1 \oplus x_2 y_2 \oplus \dots \oplus x_n y_n$$

x is orthogonal to y iff $(x, y) = 0$

A code $V^\perp$ is orthogonal to V iff for any $x \in V$, $y \in V^\perp$ $(x, y) = 0$

Solution of the linear checks problem for polynomials:

$$\sum_{x \in V^\perp} f(x \oplus \tau) = c$$

where $V^\perp$ is a code which is orthogonal to a maximal code with distance $s+1$ (s is the degree of f)

Example 2. $n=5$

$f(x) = x^2 + 3x - 4$ $\qquad (s=2)$

$$V = \begin{pmatrix} 0&0&0&0&0 \\ 1&0&0&1&1 \\ 0&1&1&0&1 \\ 1&1&1&1&0 \end{pmatrix}$$ rows of V are vectors from the code

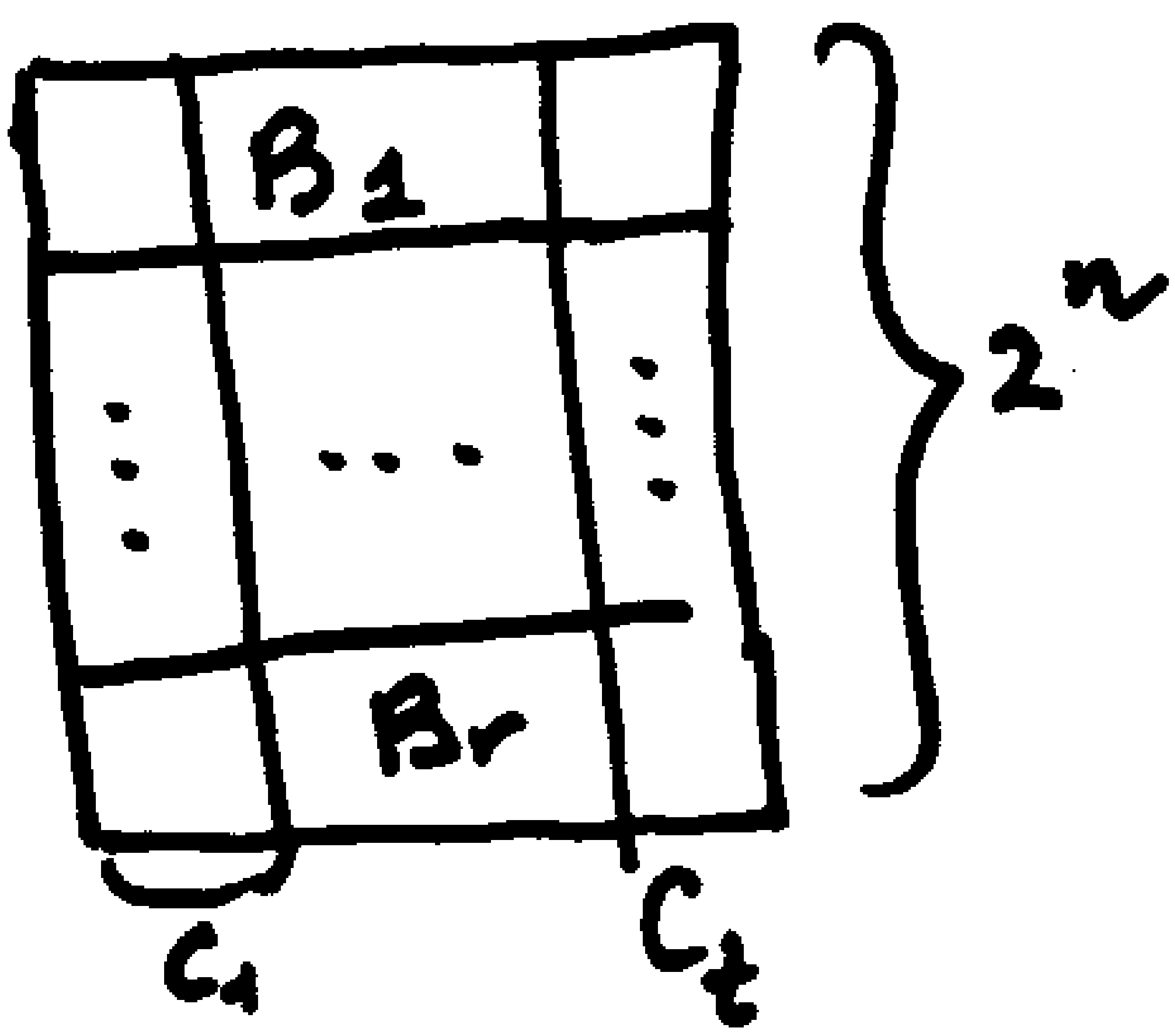
$$V^{\perp} = \begin{pmatrix} 0&0&0&0&0 \\ 0&1&1&0&0 \\ 1&0&0&1&0 \\ 1&1&1&1&0 \\ 1&1&0&0&1 \\ 1&0&1&0&1 \\ 0&1&0&1&1 \\ 0&0&1&1&1 \end{pmatrix}$$ rows of $V^{\perp}$ are vectors from the code $V^{\perp}$

$t(f) = 8$

$$\sum_{\tau \in V^{\perp}} f(x \oplus \tau) = K$$ for any x

Error Detection / Correction in Memories by Linear checks

2 orthogonal checks based on
2 orthogonal partitions of input space



n - number of bits in the address

$$\sum_{x \in B_i} f(x) = K_1 \quad \text{for any } i, \; i = 1, \ldots, r$$

$$\sum_{x \in C_i} f(x) = K_2 \quad \text{for any } i, \; i = 1, \ldots, t$$

For 2 orthogonal checks:

1) Correct all single errors

2) Detect all double and triple errors

3) Probability of correction for double errors

$P^c(2) \geq 1 - 2^{n-m+3}$ $\quad m > n$

m - is a # of bits in data
n - is a # of bits in an address

4) Probability of detecting of errors with multiplicity $\ell > 3$

$P \geq 1 - (2^m - 1)^{-2}$

For bitwise errors:

$P \geq 1 - (2m - 1)^{-2}$

the number of READ, WRITE instructions: 2^{n+2} – the same as for MSCAN

Experimental results (simulation)

Table 1: Error-correcting capability of two checks

Function $f(Z) = f(Z_1, Z_2)$ / l	$P^c(l)$ $Z_1 + Z_2$	$Z_1 - Z_2$	$Z_1 Z_2$	$Z - 1$	$Z^2 - Z - 1$
2	100	100	100	100	100
3	99.90	99.90	97.00	99.93	58.06
4	99.90	99.90	88.86	99.90	23.46
5	99.33	99.26	76.43	99.56	6.36

Results of computer experiments on error-correcting capability of two orthogonal equality checks ($n = m = 8$, for every l and every $f(Z)$ 3000 experiments have been made to estimate $Pc(l)$).

Table 2: Bitwise errors

Function $f(Z) = f(Z_1, Z_2)$ / l	$P^c(l)$ $Z_1 + Z_2$	$Z_1 - Z_2$	$Z_1 Z_2$	$Z - 1$	$Z^2 - Z - 1$
2	99.93	99.83	99.13	99.83	98.50
3	99.70	99.53	94.93	99.46	54.63
4	99.43	99.13	84.96	99.08	20.96
5	98.70	98.60	71.43	98.43	6.26

Results of computer experiments on error-correcting capability of two orthogonal equality checks ($n = m = 8$; for every l and every $f(Z)$ 3000 experiments have been made to estimate $Pc(l)$)

IEE PROCEEDINGS, Vol. 131, Pt. E, No. 5, SEPTEMBER 1984

Algorithms for error detection/correction in ROMs, RAMs by linear checks are given in: M. G. Karpovsky, "Memory testing by Linear Checks", IEE Proc. vol 131 N5 Sept. 1984

Linear Check for Functions of Several Variables

Let $f(x_1, x_2, \ldots, x_t)$, $x_i \in \{0,1\}^{n_i}$, $n = \sum_{i=1}^{t} n_i$

Let $V_i^\perp$ is a first block of a linear check for f when all the variables except x_i are fixed (f considered as a function of x_i only) $(i = 1, \ldots, t)$

Then $V^\perp = V_1^\perp \times V_2^\perp \times \ldots \times V_t^\perp$ will be the first block for $f(x_1, x_2, \ldots, x_t)$ $\left(V^\perp = \{(\tau_1, \tau_2, \ldots, \tau_t) \mid \tau_i \in V_i^\perp\}\right)$

<u>Example 1</u> $f(x_1, x_2) = x_1 * x_2$; $x_1, x_2 \in \{0,1\}^3$, $n_1 = n_2 = 3$

$V_1^\perp = \{000, 111\}$ $V_2^\perp = \{000, 111\}$

$V^\perp = V_1^\perp \times V_2^\perp = \{(000\ 000), (000\ 111), (111\ 000), (111\ 111)\}$

$K_f = 0 \cdot 0 + 0 \cdot 7 + 7 \cdot 0 + 7 \cdot 7 = 49$. $\square$

Let $T_f = |V^\perp|$ $T_{f_i} = |V_i^\perp|$. Then

$$T_f = \prod_{i=1}^{t} T_{f_i}$$

<u>Example 2</u> $f(x_1, x_2) = x_1^2 x_2 + 3x_2$, $x_1 \in \{0,1\}^5$, $x_2 \in \{0,1\}^3$

$V_1^\perp$ is a linear span of rows of $H = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$, $T_{f_1} = 8$

$V_2^\perp$ is $\{000, 111\}$, $T_{f_2} = 2$ $T_f = 16$

LINEAR INEQUALITY CHECKS

for a given $f(x)$ and $\varepsilon > 0$

$$\Big| \sum_{\tau \in V^{\perp}} f(x \oplus \tau) - K \Big| \overset{?}{\leq} \varepsilon$$

(For $\varepsilon = 0$ equality checks as before)

Denote $|V^{\perp}| = T(f, \varepsilon)$ $\quad$ ($T(f,0) = T(f)$)

Small increase in ε may result in a drastic decrease of $T(f, \varepsilon)$

Example

$$f(y) = y^{-0.5} \sin \tfrac{\pi}{2} y^{0.5}$$

where $y = 2^{-23} x \qquad x \in \{0, 1, \dots, 2^{23} - 1\}$

$n = 23 \qquad 0 \leq y < 1$

$T(f,0) = 2^{23}$

Select $\varepsilon = 5 \cdot 10^{-3}$

note

$$y^{-0.5} \sin \frac{\pi}{2} y^{0.5} = P_2(y) + \Delta_2(y)$$

where

$$P_2(y) = 0.07287 y^2 - 0.64338 y + 1.57064$$

Chebusheff Polynomial

and $\Delta_2(y) \le 14 \cdot 10^{-5}$ for every y

Select a linear check for $P_2(y)$

Chose $(23,18)$ Hamming code with distance 3. Then $|V^{\perp}| = 2^5$

and $\varepsilon \le 14 \cdot 10^{-5} \cdot 2^5 \le 5 \cdot 10^{-3}$

Thus we have for this example

$T(f,0) = 2^{23}$ $T(f, 5 \cdot 10^{-3}) = 2^5$