整数リング上において置換多項式を使用するターボ符号のためのインタリーバ

Kwame Ackah Bohulu

11/17/2016

1 効果的な自由距離 (d_{ef}) を使用して、良いインタリーバを探索する。

決定論インタリーバでは大きな d_{ef} が良い性能を保証するわけではないが、小さい d_{ef} だと通常、悪い性能になる関係がある。このような悪い置換多項式を選ばないように、d_{ef} を基準とする。ランダムインタリーバと二次インタリーバの場合は、入力重み 2 エラーイベントが抑制できないが, いえるのは入力重み 2 エラーイベントが起きる確率は, フレーメサイズが無限にちかづくほど, ゼローになっていく。S-ランダムインタリーバの場合、それぞれの要素符号に起きる S より小さい距離を持つ入力重み 2 エラーイベントが防げる。$t \leq S$ の場合、S-ランダムインタリーバは $(x, x+t)$ を (y, z) にマッピングして、$|y-z| > S$。ところが、ある要素符号に起こる入力重み 2 エラーイベントは t が (cycle length) の倍数の値だけなので、S-ランダムインタリーバの能力がむだになる。置換多項式に基づいてインタリーバを使う場合、多項式の係数をうまく選べば、ある要素符号によく起きる重み 2 エラーイベントが避けられる。そうすると、それより大きい入力重み 2 エラーイベントも避けられる。1 番目の要素符号に起きる入力重み 2 エラーイベントの長さを $t+1$ とし、t は τ の倍数で、t のオーダーは o_t とする。 2 番目の要素符号に起きる入力重み 2 エラーイベントの長さ-1 は以下のようになる。

$$\Delta(x,t) = P(x+t) - P(x) = 2btx + bt^2 + at = c_1 x + bt^2 + at \tag{8}$$

性質 2.9 より、x の係数は $c_1 = 2bt$ のオーダーは $o_{c1} = o_2 + o_b + o_t$ である。$x \in \{0, 1, 2, ..., N-1\}$ のとき、式 (8) での第一項は $k \cdot p_N^{o_{c1}}, k = 0, 1, 2, ..., p_N^{o_N - o_{c1}} - 1$ それぞれの値は $p_N^{o_{c1}}$ 回をとる。x に従って $c_1 x$ の図を描くと $p_N^{(o_N - o_{c1})}$ の水平線が出る。$bt^2 + at$ は水平線のオフセットを与える。短い入力重み 2 エラーイベントを防止するために、t が τ の小さい倍数の場合、$\Delta(x,t)$ が τ の倍数の値を 0 から離れてほしい。このためには、ベクトル o_{c1} を大きくして、$\Delta(x,t)$ の図にある水平線の数が少なくなって、$\Delta(x,t)$ を 0 から離れる係数をうまく選ばれる。o_{c1} はもう大きいため、0 の上か下からの最初線を着目する。着目される線から 0 までの距離は以下のように書ける。

$$s = \pm\Delta(x,t) \ mod \ p_N^{o_{c1}} = (bt^2 + at) \ mod \ p_N^{o_{c1}} \tag{9}$$

a,b,τ が与えられたとき、$L_{(a,b,\tau)}$ は以下のように定義して、良いインタリーバを選ぶ基準とする。

$$L_{(a,b,\tau)}\ min\ (|s|+|t|)$$

要素符号が与えられたとき、$L_(a,b,\tau)$ から d_{ef} が計算できる。良い a と b を探索するとき、範囲を制限したらよい。以下の補題で a と b の範囲が制限できる。

補題 4.1
入力重み 2 エラーイベントの解析では、b を $b_1 \cdot b_0$=$b_1 \cdot p_N^{o_{b1}}$ のようにかけば b1 を 1 とすることができる。

Proof. $b_1 = 1$ と仮定すると、b_1 と N は互いに素である。ある置換多項式 $P_1(x) = p_N^{o_b}x^2 + at$ が与えたら、(9) は

$$s_1 = p_N^{o_b}t^2 + at\ mod\ p_N^{o_b+o_t+o_2}$$

もう一つの置換多項式 $P_2(x) = b_1 p_N^{o_b}x^2 + at$ が与えたら、(9) は

$$s_2 = b_1 p_N^{o_b}t^2 + at\ mod\ p_N^{o_b+o_t+o_2}$$

$s_2 - s_1$ を計算すると以下の式が出る。

$$s_2 - s_1 = (b_1 - 1)p_N^{o_b}t^2 + at\ mod\ p_N^{o_b+o_t+o_2} \tag{10}$$

2 は N の因数の場合 ：b_1 と N は互いに素であるので b_1 は奇数で、$b_1 - 1$ は偶数である。式 (10) の右辺のオーダーは少なくとも $o_2 + o_b + 2o_t$。

$$s_2 - s_1 = 0\ mod\ p_N^{o_b+o_t+o_2}$$

2 は N の因数でない場合 ：式 (10) の右辺のオーダーは少なくとも $o_b + 2o_t$ であり、 mod $o_b + o_t$ で計算する。

$$s_2 - s_1 = 0\ mod\ p_N^{o_b+o_t+o_2}$$

$P_1(x)$ と $P_2(x)$ の入力重み 2 エラーイベントの位置以外は同じ入力重み 2 エラーイベントを持っている。この観点から、$P_1(x)$ と $P_2(x)$ は均しいである。 □

補題 4.2
入力重み 2 エラーイベントの解析では、$b = b_1 \cdot p_N^{o_{b1}}$ があたえられたとき、a は $1 \le a \le p_N^{o_{b1}}$ となる a だけ考えば十分である。

Proof. 補題 4.1 の結果より $b = p_N^{o_b}$。

2 は N の因数でないとき ： $a_0 = a \ mod \ p_N^{o_b+o_2}$ とする。すると、$a = a_0 + lp_N^{o_b+o_2}$。

$$\begin{aligned} s &= \pm(bt^2 + (a_0 + lp_N^{o_b+o_2})t) \ mod \ p_N^{o_b+o_t+o_2} \\ &= \pm bt^2 + (a_0)t \ mod \ p_N^{o_b+o_t+o_2} \end{aligned} \tag{11}$$

これは $L_(a, b, \tau) = L_(a_0, b, \tau)$ を意味する。

2 は N の因数のとき ：一般性を失わずに、上の証明で $1 \leq a < p_N^{o_b+o_2}$ を仮定することができる。$a_0 = p_N^{o_b+o_2} - a$ とすると、

$$\begin{aligned} s &= \pm(bt^2 + (a_0 t) \ mod \ p_N^{o_b+o_2+o_t} \\ s &= \pm(bt^2 + (p_N^{o_b+o_t+o_2} - a)t) \ mod \ p_N^{o_b+o_2+o_t} \\ &= \pm(b(-t)^2 + (a(-t)) \ mod \ p_N^{o_b+o_2+o_t} \end{aligned} \tag{12}$$

また、$L_(a, b, \tau) = L_(a_0, b, \tau)$ □

7/5 と 5/7 要素符号の場合の結果をテーブル 1に書かれている。

a	1	3	5	7	9	11	13	15
L(5/7)	12	18	12	24	24	18	12	6
L(7/5)	4	8	12	16	16	8	12	32

Table 1: $\tau(7/5) = 2, \tau(5/7) = 3, N = 2^n, p_N = [2], o_N = [n], o_b = [4] \, b = 16$

2 結果

フレームサイズ N と要素符号にが与えられたら、良い置換多項式に基づいてインタリーバを探すことは、多項式の a と b を計算することになる。最初に、o_b の値を決める。前の分析で $p_N^{o_b}$ を大きくしなければならないですが、特別な入力重み 4 エラーイベントと入力重み 6 エラーイベントで成約を拘束しなければならない。o_b が決めたら、$b = p_N^{o_b}$ とし、定理 4.8 の範囲ですべての a を計算する。

6 種類の要素符号が選ばれて、テーブル 2 に書かれている。フレームサイズを $N = 2^n$ とし,N のベースを $p_N = 2$ になり、N のオーダーはスカラーになる。$N = 2^8$ の場合、要素符号に対して最良な置換多項式そして、入力重み 2 エラーイベントに対する最低距離と多重度がテーブル 2に書かれている。

シムレーションで置換多項式に基づいてインタリーバを S ーランダムインタリーバと二次インタリーバと比べた結果は、図 6-11 で示される。置換多項式に基づいたインタリーバは常に二次インタリーバと S ーランダムインタリーバより良い性能をもつ。

要素符号	Cycle length(τ)	最適多項式	d_{min}(多重度)	図
7/5	2	$15x + 16x^2$	18(512)	6
5/7	3	$15x + 32x^2$	28(512)	7
37/21	4	$7x + 8x^2$	24(56)	8
21/37	5	$15x + 32x^2$	28(512)	9
37/25	6	$15x + 16x^2$	24(512)	10
23/35	7	$15x + 32x^2$	36(512)	11

Table 2: 様々な要素符号に対して最適な置換多項式、フレーメサイズ 256

要素符号を RC 5/7 符号、フレームサイズ N を 1024 と 16384 とし、それぞれのインタリーバの最良の置換多項式は $P(x) = 31x+64x^2$ と $P(x) = 15x+32x^2$ に基づく。シムレーションでの結果は図 12 と 13 に示される。長いフレームサイズの場合、置換多項式に基づいたインタリーバの性能は、二次インタリーバより良いですが、S ーランダムインタリーバほどよくないということがわかる。

3 結論

この論文には、置換多項式に基づいてインタリーバがしょうかいされた。インタリーバの生成多項式のパラメータが与えたら、多項式を計算することで, 重要なエラーイベントの集合の d_{ef} が探索でき、本当の d_{ef} も近似できる。そして、近似値に対して、良いインタリーバの制限された探索ができる。紹介されましたインタリーバを S-ランダムインタリーバと二次インタリーバと比べられた。短いフレームサイズの場合,S-ランダムインタリーバより良い性能を持つインタリーバが見つけられた。長いフレームサイズの場合、紹介されたインタリーバは S-ランダムインタリーバと近い性能を持つ。二次インタリーバと比べた場合、どんなフレームサイズでも置換多項式に基づいてインタリーバの性能がたかいです。