(601) 高校生セッション

加算結果を利用した3入力変数のあいまいな推測について
On Ambiguous Reasoning of Three Input Variables by Utilizing Additive Results

大杉 宗治 † 西本 陸人 † 上土井 陽子 †† 若林 真一 ††
Muneharu Ohsugi† Rikuto Nishimoto† Yoko Kamidoi†† Shin'ichi Wakabayashi††
† 広島県立広島国泰寺高等学校　†† 広島市立大学 大学院情報科学研究科

1 概要

2変数 x，y の加算結果 A のみから元の x, y の値を推測する場合には，x, y の値域に依存し，$x+y=A$ となるすべての組合せが推測結果となる．しかし，A に加えて，x, y にある操作を行った後の加算結果 B が与えられると，x, y の2進数表現のビット毎の組合せが判明する程度に推測できることが分かっている．このような推測をあいまいな推測と呼ぶ [1][2].

本研究では2変数に対するあいまいな推測方法が3変数 x, y, z を対象とした場合にも拡張可能であるか検討する．

2 2変数のあいまいな推測

入力変数 x と y を n ビット2進数とし，各桁 i $(1 \leq i \leq n)$ のビットをそれぞれ $x[i]$, $y[i]$ と表す．また，2変数 x,y を加算した結果の $(n+1)$ ビット2進数表現を A とし，各桁 i のビットを $A[i]$ と表す．さらに，x,y から A を計算したときの各桁 i での桁上げのビット表現を $C_A[i]$ と表す．入力変数 x,y の逆順表現 x^R, y^R を逆順ビット列と呼ぶ．逆順ビット列では各桁 i において $x[i]=x^R[n-i+1]$, $y[i]=y^R[n-i+1]$ が成り立つ．逆順ビット列に対し，x, y を正順ビット列，A を正順加算結果と呼ぶ．また，2変数 x^R,y^R を加算した結果の $(n+1)$ ビット2進数表現を B とし，逆順加算結果と呼び，各桁 i のビットを $B[i]$ と表す．さらに，x^R,y^R から B を計算したときの各桁 i での桁上げのビット表現を $C_B[i]$ と表す．桁上げビット表現の C_A,C_B に関しては，計算の都合により0桁目の値をもつこととし，$C_A[0]=0, C_B[0]=0$ とする．また，n 桁目の値としてそれぞれの加算結果の $n+1$ 桁目の値をもつこととし，$C_A[n]=A[n+1], C_B[n]=B[n+1]$ とする．

上記の場合，文献 [1], [2] により $A[i]$, $C_A[i]$ と $B[n-i+1]$, $C_B[n-i]$ から入力変数の i 桁目の値の組合せ $(x[i], y[i])$ を表1のように計算することができる．ここで，推測された $(x[i], y[i])$ の組合せが $(0,0), (1,1)$ の場合には $x[i], y[i]$ の値がそれぞれ，双方とも $0, 1$ であると決定できる．一方，推測された $(x[i], y[i])$ の組合せが $(0,1)$ の場合には $x[i], y[i]$ の値のどちらかが1であり，他方が0と決定できるが，どちらが1であるかは分からない．本研究ではこのような推測をあいまいな推測と呼ぶ．あいまいな推測結果の利用方法としては各ビット毎の論理積や論理和などの計算結果を各ビットの詳細を秘匿したまま得る秘匿計算方法への拡張が知られている [1].

3 3変数のあいまいな推測への拡張

本研究では **2** で説明した2変数に関するあいまいな推測方法を2進数表現された3変数に関するあいまいな推測方法に拡張できるか検討する．

まず，あいまいな推測の入力としては2変数の場合と同様に，n ビットの3変数 x, y, z の加算結果を表現する $(n+2)$ ビットの正順加算結果 A と x, y, z の逆順ビット列 x^R, y^R, z^R の加算結果を表現する $(n+2)$ ビットの逆順加算結果 B が与えられているとする．このとき，2変数のあいまいな推測とは異なり，正順加算結果において，各桁 i $(1 \leq i \leq n)$ の桁上げ $C_A[i]$ は，$x[i], y[i], z[i], C_A[i-1]$ が全て1の場合には10進数で2となること，$C_A[i-1]=2$ の場合でも $C_A[i]=2$ より，$0, 1, 2$ のいずれかとなる．同様に逆順加算結果においても，各桁 i $(1 \leq i \leq n)$ の桁上げ $C_B[i]$ は, $0, 1, 2$ のいずれかとなる．また，$C_A[n]=2^{A[n+2]}+A[n+1]$, $C_A[0]=0$, $C_B[n]=2^{B[n+2]}+B[n+1]$, $C_B[0]=0$ とする．

このとき，各桁 i $(1 \leq i \leq n)$ において，$A[i]$, $C_A[i]$ が与えられたときに，i 桁目の入力の組合せと次の桁上げの候補を表2に示す．例えば，$A[i]=0$ で $C_A[i]=1$ のときは表2より，$((x[i], y[i], z[i]), C_A[i-1])$ の組合せとしては $((0,0,0),2)$, $((0,0,1),1)$, $((0,1,1),0)$ の3つの候補のうちの1つを取り得ることを示している．

同様に，各桁 i $(1 \leq i \leq n)$ において，$B[n-i+1]$, $C_B[n-i]$ が与えられたときに，i 桁目の入力の組合せと次の桁上げの候補を表3に示す．例えば，$B[n-i+1]=0$ で $C_B[n-i]=1$ のときは表3より，$((x[i], y[i], z[i]), C_B[n-i+1])$ の組合せとしては $((0,0,1),1)$, $((1,1,1),2)$ の2つの候補のうちの1つを取り得ることを示している．

我々は表2と表3に基づいて，$x[i], y[i], z[i]$ の組合せと桁上げ $C_A[i-1]$ と $C_B[n-i+1]$ を推測する方法を以下に提案する．

文献 [1] の表1の作成方法を拡張して，各桁 i $(1 \leq i \leq n)$ での推測を表2による正順加算結果からの推測と表3による逆順加算結果からの推測で同じ $(x[i], y[i], z[i])$ をもつ候補のみを残す．例えば，先の例で $A[i]=0$, $C_A[i]=1$, $B[n-i+1]=0$, $C_B[n-i]=1$ のときには，$((x[i], y[i], z[i]), C_A[i-1])$ の組合せとし

表 1: 2 変数 x, y の正順加算結果と逆順加算結果からのあいまいな推測の対応表

正順加算ビット $A[i]$	桁上げ $C_A[i]$	逆順加算ビット $B[n-i+1]$	桁上げ $C_B[n-i]$	推測 組合せ $(x[i], y[i])$	推測 桁上げ $C_A[i-1]$	推測 桁上げ $C_B[n-i+1]$
0	0	0	0	0 0	0	0
0	0	0	1	適用なし		
0	0	1	0	適用なし		
0	0	1	1	0 0	0	0
0	1	0	0	0 0	1	0
0	1	0	1	0 1	1	1
0	1	1	1	1 1	0	1
1	0	0	0	0 0	1	0
1	0	0	1	0 1	0	0
1	0	1	0	0 1	0	0
1	0	1	1	0 1	1	0
1	1	0	0	1 1	1	1
1	1	0	1	適用なし		
1	1	1	0	適用なし		
1	1	1	1	1 1	1	1

て $((0,0,0),2)$, $((0,0,1),1)$, $((0,1,1),0)$ の 3 つの候補，$((x[i],y[i],z[i]),\ C_B[n-i+1])$ の組合せとして $((0,0,1),1)$, $((1,1,1),2)$ の 2 つの候補があった．よって，$(x[i],y[i],z[i])$ の組合せとしては双方に共通する $(0,0,1)$ が候補として残り，$C_A[i-1]=1$, $C_B[n-i+1]=1$ がそのときの桁上がりの組合せ候補となる．以降，$(x[i],y[i],z[i])$, $C_A[i-1]$, $C_B[n-i+1]$ の候補の組合せを $((x[i],y[i],z[i]),\ C_A[i-1],\ C_B[n-i+1])$ という形式で表現する．

このとき，表 1 での 2 変数に対するあいまいな推測方法とは異なり，$A[i]$, $C_A[i]$, $B[n-i+1]$, $C_B[n-i]$ が与えられたときに 2 つ以上の候補が残る場合がある．例えば，$A[i]=0$, $C_A[i]=1$, $B[n-i+1]=1$, $C_B[n-i]=1$ のときは $((0,0,0),2,0)$ と $((1,1,0),0,1)$ が候補として残ってしまう．このとき，$C_A[i-1]=2$, $C_B[n-i]=0$ として，$x[i-1], y[i-1], z[i-1]$ を推測する場合と，$C_A[i-1]=0$, $C_B[n-i]=1$ として，$x[i-1], y[i-1], z[i-1]$ を推測する場合の双方を考える必要がある．我々の方法ではこのような場合，候補ごとに分岐しながら推測を続け，どちらかの分岐で候補なしや桁上げの値に矛盾が生じた場合は分岐前に遡って候補を削除することで各桁の値を推測する．

4 提案方法の適用例

$n=6$, $x=100010$, $y=101010$, $z=111111$ とする．このとき，正順加算結果 A は $A=10001011$ であり，逆順加算結果 B は $B=1100101$ となる．

今，x, y, z は与えられず，$n=6$, $A=10001011$ と $B=1100101$ が入力として与えられたとする．このとき，A, B, $C_A[6]=2^{A[8]}+A[7]=2$, $C_B[6]=2^{B[8]}+B[7]=1$, $C_A[0]=C_B[0]=0$ を用いて，x, y, z の各桁のビットの組合せを提案方法に従い推測する．以下では，推測を 6 桁目 $(i=6)$ から始める上位桁からの推測例と 1 桁目 $(i=1)$ から始める下位桁からの推測例を示し，場合分けが継続するかについて考える．

表 2: 3 変数 x, y, z の正順加算結果からのあいまいな推測対応

正順加算ビット $A[i]$	桁上げ $C_A[i]$	推測 組合せ $(x[i], y[i], z[i])$	推測 桁上げ $C_A[i-1]$
0	0	0 0 0	0
0	1	0 0 0	2
		0 0 1	1
		0 1 1	0
0	2	0 1 1	2
		1 1 1	1
1	0	0 0 0	1
		0 0 1	0
1	1	0 0 1	2
		0 1 1	1
		1 1 1	0
1	2	1 1 1	2

4.1 上位桁からの推測例

1. $i=6$ とすると，$A[6]=0, C_A[6]=2, B[1]=1, C_B[0]=0$ より，$((x[6],y[6],z[6]), C_A[5], C_B[1])$ の組合せは $((1,1,1),1,1)$ であると推測できる．
2. $i=5$ とすると，$A[5]=0, C_A[5]=1, B[2]=0, C_B[1]=1$ より，$((x[5],y[5],z[5]), C_A[4], C_B[2])$ の組合せは $((0,0,1),1,1)$ であると推測できる．
3. $i=4$ とすると，$A[4]=1, C_A[4]=1, B[3]=1, C_B[2]=1$ より，$((x[4],y[4],z[4]), C_A[3], C_B[3])$ の組合せは $((0,1,1),1,1)$ であると推測できる．

表 3: 3 変数 x, y, z の逆順加算結果からのあいまいな推測対応

逆順加算ビット $B[n-i+1]$	桁上げ $C_B[n-i]$	推測組合せ $(x[i], y[i], z[i])$	推測桁上げ $C_B[n-i+1]$
0	0	0 0 0 0 1 1	0 1
0	1	0 0 1 1 1 1	1 2
0	2	0 0 0 0 1 1	1 2
1	0	0 0 1 1 1 1	0 1
1	1	0 0 0 0 1 1	0 1
1	2	0 0 1 1 1 1	1 2

4. $i = 3$ とすると，$A[3] = 0, C_A[3] = 1, B[4] = 0, C_B[3] = 1$ より，$((x[3], y[3], z[3]), C_A[2], C_B[4])$ の組合せは $((0,0,1), 1, 1)$ であると推測できる．

5. $i = 2$ とすると，$A[2] = 1, C_A[2] = 1, B[5] = 0, C_B[4] = 1$ より，$((x[2], y[2], z[2]), C_A[1], C_B[5])$ の組合せは $((0,0,1), 2, 1)$, $((1,1,1), 0, 2)$ のどちらかであると推測できる．

6. $i = 1$ とすると，

   - 場合 1: $((x[2], y[2], z[2]), C_A[1], C_B[5]) = ((0,0,1), 2, 1)$ の場合 $A[1] = 1$, $C_A[1] = 2$, $B[6] = 1$, $C_B[5] = 1$ より，$((x[1], y[1], z[1]), C_A[0], C_B[6])$ の組合せは存在しない．
   - 場合 2: $((x[2], y[2], z[2]), C_A[1], C_B[5]) = ((1,1,1), 0, 2)$ の場合 $A[1] = 1$, $C_A[1] = 0$, $B[6] = 1$, $C_B[5] = 2$ より，$((x[1], y[1], z[1]), C_A[0], C_B[6])$ の組合せは $((0,0,1), 0, 1)$ であると推測できる．

7. 場合 2 の推測が $C_A[0] = 0$, $C_B[6] = 1$ と整合し，推測が正しいことを確認できる．場合 1 は候補がないことから，$((x[2], y[2], z[2]), C_A[1], C_B[5]) = ((1,1,1), 0, 2)$ と推測できる．

4.2 下位桁からの推測例

逆順加算結果 B を正順加算結果 A', 正順加算結果 A を逆順加算結果 B'，逆順桁上げ C_B を正順桁上げ C'_A, 正順桁上げ C_A を正順桁上げ C'_B, $i' = n - i + 1$ と見なして, 表 2, 表 3 から $x[1], y[1], z[1]$ の組合せから推測する．なお，最終結果は上位桁からの推測例と同じ推測結果となるが場合分けが異なる．

1. $i' = 1$ とすると，$A'[6] = 1, C'_A[6] = 1, B'[1] = 1, C'_B[0] = 0$ より，$((x[1], y[1], z[1]), C'_A[5], C'_B[1])$ の組合せは $((0,0,1), 2, 0)$, $((1,1,1), 0, 1)$ のどちらかであると推測できる．

2. $i' = 2$ とすると，

   - 場合 1: $((x[1], y[1], z[1]), C'_A[5], C'_B[1]) = ((0,0,1), 2, 0)$ の場合 $A'[5] = 0$, $C'_A[5] = 2$, $B'[2] = 1$, $C'_B[1] = 0$ より，$((x[2], y[2], z[2]), C'_A[4], C'_B[2])$ の組合せは $((1,1,1), 1, 1)$ であると推測できる．
   - 場合 2: $((x[1], y[1], z[1]), C'_A[5], C'_B[1]) = ((1,1,1), 0, 1)$ の場合 $A'[5] = 0$, $C'_A[5] = 0$, $B'[2] = 1$, $C'_B[1] = 1$ より，$((x[2], y[2], z[2]), C'_A[4], C'_B[2])$ の組合せは $((0,0,0), 0, 0)$ であると推測できる．

3. $i' = 3$ とすると，

   - 場合 1: $((x[2], y[2], z[2]), C'_A[4], C'_B[2]) = ((1,1,1), 1, 1)$ の場合 $A'[4] = 0$, $C'_A[4] = 1$, $B'[3] = 0$, $C'_B[2] = 1$ より，$((x[3], y[3], z[3]), C'_A[3], C'_B[3])$ の組合せは $((0,0,1), 1, 1)$ であると推測できる．
   - 場合 2: $((x[2], y[2], z[2]), C'_A[4], C'_B[2]) = ((0,0,0), 0, 0)$ の場合 $A'[4] = 0$, $C'_A[4] = 0$, $B'[3] = 0$, $C'_B[2] = 0$ より，$((x[3], y[3], z[3]), C'_A[3], C'_B[3])$ の組合せは $((0,0,0), 0, 0)$ であると推測できる．

4. $i' = 4$ とすると，

   - 場合 1: $((x[3], y[3], z[3]), C'_A[3], C'_B[3]) = ((0,0,1), 1, 1)$ の場合 $A'[3] = 1$, $C'_A[3] = 1$, $B'[4] = 1$, $C'_B[3] = 1$ より，$((x[4], y[4], z[4]), C'_A[2], C'_B[4])$ の組合せは $((0,1,1), 1, 1)$ であると推測できる．
   - 場合 2: $((x[3], y[3], z[3]), C'_A[3], C'_B[3]) = ((0,0,0), 0, 0)$ の場合 $A'[3] = 1$, $C'_A[3] = 0$, $B'[4] = 1$, $C'_B[3] = 0$ より，$((x[4], y[4], z[4]), C'_A[2], C'_B[4])$ の組合せは $((0,0,1), 0, 0)$ であると推測できる．

5. $i' = 5$ とすると，

   - 場合 1: $((x[4], y[4], z[4]), C'_A[2], C'_B[4]) = ((0,1,1), 1, 1)$ の場合 $A'[2] = 0$, $C'_A[2] = 1$, $B'[5] = 0$, $C'_B[4] = 1$ より，$((x[5], y[5], z[5]), C'_A[1], C'_B[5])$ の組合せは $((0,0,1), 1, 1)$ であると推測できる．
   - 場合 2: $((x[4], y[4], z[4]), C'_A[2], C'_B[4]) = ((0,0,1), 0, 0)$ の場合 $A'[2] = 0$, $C'_A[2] = 0$, $B'[5] = 0$, $C'_B[4] = 0$ より，$((x[5], y[5], z[5]), C'_A[1], C'_B[5])$ の組合せは $((0,0,0), 0, 0)$ であると推測できる．

6. $i' = 6$ とすると，

- 場合 1: $((x[5], y[5], z[5]), C'_A[1], C'_B[5]) = ((0,0,1),1,1)$ の場合 $A'[1] = 1$, $C'_A[1] = 1$, $B'[6] = 0$, $C'_B[5] = 1$ より，$((x[6], y[6], z[6]), C'_A[0], C'_B[6])$ の組合せは $((0,0,1),2,1)$ か $((1,1,1),0,2)$ のどちらかであると推測できる．
- 場合 2: $((x[5], y[5], z[5]), C'_A[1], C'_B[5]) = ((0,0,0),0,0)$ の場合 $A'[1] = 1$, $C'_A[1] = 0$, $B'[6] = 0$, $C'_B[5] = 0$ より，$((x[6], y[6], z[6]), C'_A[0], C'_B[6])$ の組合せは $((0,0,0),1,0)$ であると推測できる．

7. 場合 1 の $((x[6], y[6], z[6]), C'_A[0], C'_B[6])$ の組合せ $((1,1,1),0,2)$ の推測が $C'_A[0] = 0$, $C'_B[6] = C_A[6] = 2$ と整合し，正しいことを確認できる．$i' = 2,3,4,5,6$ において，全て場合 1 の推測だけが正しいことが分かる．

4.3 適用例のまとめ

上記の適用例では上位桁からの推測では少ない場合分けであいまいな推測を終えることができたが，下桁からの推測では始めの桁から最後の桁まで場合分けが続き，最後の桁の推測が終わらないと最初の桁の推測を確定することができなかった．また，$i' = 7$ と続いたとすると場合分けが 3 つ以上になる可能性もあった．一方，上位桁からの推測結果と下位桁からの推測結果は矛盾を生じることはないので，双方を組み合わせることで場合分けを削減できる可能性があることもわかった．

5 まとめ

本研究では従来知られていた 2 変数に対するあいまいな推測方法が 3 変数 x, y, z を対象とした場合にも拡張可能であるかどうかについて検討した．検討の結果，場合分けが続く可能性があるが，3 変数 x, y, z の値をあいまいに推測できると考えられる推測方法を提案し，適用例を示した．今後，全ての入力について，提案方法で常に正しくあいまいに推測できるかどうか，さらに，提案方法が変数のビット数 n に比例する計算時間で実行可能かどうかを検討する予定である．

参考文献

[1] 櫻田潤一, 上土井陽子, 若林真一, “分散データベースにおける匿名化可能判定のための安全で効率的なプロトコル”, 第 4 回データ工学と情報マネジメントに関するフォーラム (DEIM2012) 論文集, c5-5 (2012).
(http://db-event.jpn.org/deim2012/proceedings/detail.html)

[2] 櫻田潤一, 上土井陽子, 若林真一, “分散データベースにおける匿名化可能判定プロトコルの効率化”, コンピュータセキュリティシンポジウム 2012 (CSS2012) 論文集, 1D2-3 (2012).