代数幾何的符号の復号と多項式の素因数分解

データ科学研究系　計算機統計グループ
准教授　　丸山 直昌

代数幾何的符号の復号を多項式の素因数分解を用いて効率的に行う方法を模索している。その現状を報告する。

1　代数幾何的符号

q を素数巾、F_q を q 個の元から成る有限体、C を F_q 上の特異点が無い代数曲線、$\overline{C}$ をその非特異完備化とする。C 上の n 個の点集合 $\{p_1, p_2, \ldots, p_n\}$ を考え、$\overline{C} - C$ から点 p_0 を選ぶ。$\overline{C}$ 上の有理関数で p_0 で $k-1$ 位以下の極を持ち、他に極を持たないもの全体が成す線形空間を L とし、写像 $\psi : L \rightarrow {F_q}^n$ を、$f \in L$ に対して $\psi(f) = (f(p_1), f(p_2), \ldots, f(p_n))$ と定め、$\psi(L) \subset {F_q}^n$ を考える。$max(0, 2g-1) \leq k-1 \leq min(n-1, n+2g-2)$ の時 ψ は単射で、$dim\ \psi(L) = k-g$ であり、さらに $\psi(L)$ は最小距離が $n-k+1$ 以上の符号となる。ただしここに g は $\overline{C}$ の種数 (genus) である。

リードソロモン符号 $RS(n,k)$ は、C がアファイン直線で $n = q-1$ の場合である。この場合 $g=0$ で p_0 は無限遠点、L は次数 $k-1$ 以下の F_q 係数多項式の全体と見做せる。

2　誤り訂正復号

誤り訂正復号の数学的な定式化は、${F_q}^n$ の元 R を与えた時、R に「一番近い」$S \in \psi(L)$ を探す、という形で定式化される。

この定式化とリードソロモン符号の実用との関係を見てみよう。伝送路を通じて送りたい情報 $(m_1, m_2, \ldots, m_k)$ に対して、

$$f(x) = \sum_{i=1}^{i=k} m_i x^{i-1} \tag{2.1}$$

として、$S = (s_1, s_2, \ldots, s_n) = (f(p_1), f(p_2), \ldots, f(p_n))$ を送信する。通信路による錯乱を受けた受信情報 $R = (r_1, r_2, \ldots, r_n)$ から送信情報 $S = (s_1, s_2, \ldots, s_n) \in \psi(L)$ を推定することは、$f(x)$ 或は送った情報 $(m_1, m_2, \ldots, m_k)$ を求めることと等価である。

3 Gruswami-Sudan のアルゴリズム

Gruswami, V. and Sudan, M.(1999) が提案した復号アルゴリズムは、多項式の因数分解を使った次のようなものである。これはリードソロモン符号が $\psi(L)$ の形、つまり「多項式の値」で表されることを非常にうまく利用していると見ることができ、一般の代数幾何的符号にも応用できる側面を持っている。

Step1 n 個の点 (p_i, r_i) $(i = 1, 2, \ldots, n)$ で大きな次数の零点を持つ 2 変数多項式 $Q(x, y)$ を探す。

Step2 $Q(x, y)$ を因数分解して $y - f(x)$ の形の因子を見つける。

しかしこの方法では、 Step1 をどのようにしたら良いか、決定打にかけるようである。

(3.1) $B_{l,m}(r_1, \ldots, r_n) = \{Q(x, y) \in F_q[x, y] | (1, k-1) - 重み付き次数(Q) \leq l で、$

すべての$1 \leq i \leq n$について$Q(x, y)$は(p_i, r_i)で$m - 1$位以上の零点を持つ$\}$

とするとき、ある l, m に対して $B_{l,m}(r_1, \ldots, r_n)$ は 0 以外の元 $Q(x, y)$ を含むことはわかっており、その $Q(x, y)$ を因数分解すれば良いのだが、 $R = (r_1, r_2, \ldots, r_n)$ から $Q(x, y)$ を効率的に求める方法が欲しいところである。