一点符号(One-point Code)の復号

丸山 直昌　　データ科学研究系　准教授

1　はじめに

近年研究されている代数幾何的符号の中でも、一点符号(One-point Code)と呼ばれるものは、未知の実用的な符号が見つかる可能性という意味で興味深いものです。

2　定義

一点符号は代数幾何的符号の一種として定義されますので、まず代数幾何的符号の定義を述べます。$\boldsymbol{X}$を有限体$\mathbb{F}_q$上の特異点が無い完備代数曲線、$\boldsymbol{G}$を$\boldsymbol{X}$上の因子($\boldsymbol{X}$上の点の形式的な和)とし、$\{\boldsymbol{p_1}, \boldsymbol{p_2}, \ldots, \boldsymbol{p_n}\}$は$\boldsymbol{X}$上の相異なる$\boldsymbol{n}$個の点で$\boldsymbol{G}$を構成するどの点とも異なるものものとします。$\boldsymbol{X}$上の有理関数$\boldsymbol{f}$で、その因子$(\boldsymbol{f})$と$\boldsymbol{G}$を加えたものが正の因子となるもの全体と$\boldsymbol{0}$がなす線型空間を$\boldsymbol{L}$とします(この$\boldsymbol{f}$の条件は、「$\boldsymbol{f}$の極が$\boldsymbol{G}$を構成する点だけにあり、その位数が対応する$\boldsymbol{G}$の点の係数を越えない」、と言い換えることができます)。写像$\boldsymbol{\psi : L \to {\mathbb{F}_q}^n}$を、$\boldsymbol{f \in L}$に対して$\boldsymbol{\psi(f) = (f(p_1), f(p_2), \ldots, f(p_n))}$と決めると、$\boldsymbol{\psi(L) \subset {\mathbb{F}_q}^n}$が符号の役割を果たします。このことは次のGoppaによる命題によって理解できます。

Proposition(Goppa). $\boldsymbol{max(0, 2g-1) \leq degG \leq min(n-1, n+2g-2)}$ の時$\boldsymbol{\psi}$は単射で、

$$\boldsymbol{dim\ \psi(L) = degG + 1 - g.}$$

さらに、$\boldsymbol{\psi(L)}$の最小距離は$\boldsymbol{n - degG}$以上である。ただしここに$\boldsymbol{g}$は$\boldsymbol{\overline{X}}$の種数(genus)である。

このGoppaの命題は良く知られたリーマン・ロッホの定理から簡単に導き出せます。このようにして構成される符号は一般に代数幾何的符号と呼ばれます。$\boldsymbol{G}$が一点$\boldsymbol{p_0}$の定数倍の場合を一点符号と呼びます。

3　リードソロモン符号

リードソロモン符号は元々巡回符号の一種として定義されますが、一点符号として表現できることも知られています。$\boldsymbol{X}$が射影直線で$\boldsymbol{p_0}$が無限遠点とした場合の一点符号は、リードソロモン符号と等価です。具体的に書きますと、有限体$\mathbb{F}_q$の$\boldsymbol{q}$個の元を$\boldsymbol{x_0, x_1, \ldots, x_n}$とし、

$$\boldsymbol{RS(n,k) = \{(f(x_1), f(x_2), \ldots, f(x_n)) | f(x)}\text{は}$$
$$\text{次数}\boldsymbol{k-1}\text{以下の}\mathbb{F}_q\text{係数多項式}\}$$

とすると、$\boldsymbol{RS(n,k)}$は$\boldsymbol{n(=q-1)}$次元ベクトル空間の中の$\boldsymbol{k}$次元部分空間で、これがリードソロモン符号のもう一つの表示を与えます。

4　リードソロモン符号の復号

符号の復号とは、数学的には${\mathbb{F}_q}^n$の元を一つ与えたとき、それに一番近い$\boldsymbol{\psi(L)}$の元を探すこと、と言うことができます。これは写像$\boldsymbol{\psi}$で移すもとの元を探すこととと等価です。リードソロモン符号$\boldsymbol{RS(n,k)}$について述べると、与えられた$\boldsymbol{(r_1, r_2, \ldots, r_n)}$に対して、$\boldsymbol{(f(x_1), f(x_2), \ldots, f(x_n))}$が一番近くなるなるような$\boldsymbol{f}$を求めることです。実際の通信の状況では、$\mathbb{F}_q$の$\boldsymbol{k}$個分の情報$\boldsymbol{(m_1, m_2, \ldots, m_k)}$を送信したい場合、

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

として、$\boldsymbol{(s_1, s_2, \ldots, s_n) = (f(x_1), f(x_2), \ldots, f(x_n))}$を送信します。受信情報$\boldsymbol{(r_1, r_2, \ldots, r_n)}$から送信情報$\boldsymbol{(s_1, s_2, \ldots, s_n)}$を推定することは、$\boldsymbol{f(x)}$或は$\boldsymbol{(m_1, m_2, \ldots, m_k)}$を求めることと等価で、これによって送信したかった情報$\boldsymbol{(m_1, m_2, \ldots, m_k)}$が求まります。

5　Gruswami-Sudanのアルゴリズム

Gruswami, V. and Sudan, M.(1999)はリードソロモン符号$\boldsymbol{RS(n,k)}$の復号を多項式の因数分解を使って行う次のようなアルゴリズムを提案しました。

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

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

もし伝送誤差が全くなければ、$\boldsymbol{s_i = r_i}$であり、Step1で作る$\boldsymbol{Q(x,y)}$が、目的とする$\boldsymbol{y - f(x)}$の倍元となっていることは想像し易いでしょう。

6　一点符号の復号とBMS復号法

リードソロモン符号以外の符号で、同様のアルゴリズムを考えることができれば、多項式の素因数分解の手法が使えるので、有力と思われます。一点符号の中でも$\boldsymbol{X}$が非特異な平面代数曲線の完備化である場合には、$\boldsymbol{p_0}$を無限遠点に取り、上記$\boldsymbol{f(x)}$を2変数の$\boldsymbol{f(x,y)}$に、$\boldsymbol{Q(x,y)}$を3変数の$\boldsymbol{Q(x,y,z)}$に置き換えて同じような事ができれば好都合です。

S. Sakata(2009)はBMS(Berlekamp-Massey-Salkata)復号法という有力な手法を使い、Gruswami-Sudanのアルゴリズムに証明を与えています。それればかりか、上記のような一点符号の場合にもその議論を使って、Gruswami-Sudanのアルゴリズムの一般化に証明を与えています。

以下では$\boldsymbol{RS(n,k)}$の双対符号$\boldsymbol{RS(n,k)^{\perp}}$の復号がBMS復号法の枠組でどのように扱われるか説明します。

$\boldsymbol{\alpha}$を有限体$\mathbb{F}_q$内での1の原始$\boldsymbol{n = q-1}$乗根、$\boldsymbol{x_i = \alpha^{i-1}, i = 1, \ldots, n}$とし、送信情報を$\boldsymbol{(s_1, s_2, \ldots, s_n)}$、受信情報を$\boldsymbol{(r_1, r_2, \ldots, r_n)}$、エラー発生場所を$\boldsymbol{E = \{i | s_i \neq r_i\}}$とします。受信情報から、まず$\boldsymbol{E}$を推定し、次に誤差$\boldsymbol{e_i = r_i - s_i}$を推定して、それにより送信情報$\boldsymbol{(s_1, s_2, \ldots, s_n)}$を決めるという方針で進みます。

$\boldsymbol{E}$を決めるために無限系列$\boldsymbol{u = (u_j)}$を$\boldsymbol{u_j = \sum_{i=0}^{i=n-1} e_{i+1} \alpha^{ji}}$と定め、$\boldsymbol{u}$の特性イデアル$\mathbf{I}(\boldsymbol{u})$を$\boldsymbol{\{f \in \mathbb{F}_q[x] | f \circ u = 0\}}$と定義します。ここに$\boldsymbol{f \circ u}$は、$\boldsymbol{f = f(x) = \sum_{l=0}^{m} f_l x^l}$に対して、$\boldsymbol{v_j = \sum_{l=0}^{m} f_l u_{l+j}}$によって定まる無限系列$\boldsymbol{v = (v_j)}$です。

この復号法の要は次のLemmaです。

Lemma. $\boldsymbol{E}$は特性イデアル$\mathbf{I}(\boldsymbol{u})$の零点集合に一致する。

ただし、系列$\boldsymbol{u_j}$のうち受信情報$\boldsymbol{(r_1, r_2, \ldots, r_n)}$から直接計算できるものは$\boldsymbol{j = 0}$から$\boldsymbol{d-1}$の分だけで、他はわかりません。それでも$\boldsymbol{E}$の元の個数が少ない場合にはうまくゆきます。

この手法は一点符号の場合にも拡張でき、Gruswami-Sudanのアルゴリズムの一般化の証明でも活躍します。

7　今後の方向性

一点符号にはこのようにかなり有力な復号法があるようであり、また符号を具体的に表示することについても、見易い表示を作れることが期待できます。平面曲線$\boldsymbol{X}$を表示する方程式を決めると、そのような表示と復号アルゴリズムを書き下すことができると期待され、そのような符号の中に効率が高いものがあれば、実用性が高いと考えられます。そのようなものを具体的に探すことは、一つのテーマとして興味深いでしょう。

また、上記の復号法では近年注目されているグレーブナー基底の理論を応用して研究する道が開けて来ました。理論的にも興味あるテーマであると考えています。