Solubilidade de Sistemas de Equações Aditivas.

Daiane Soares Veras (dai1188@hotmail.com)

Orientador:Paulo Henrique de Azevedo Rodrigues (paulo@mat.ufg.br)

Introdução

No corpo dos números reais, todo polinômio homogêneo diagonal de grau par com coeficientes positivos possui somente a solução trivial (solução nula). Entretanto, sob determinadas hipóteses, pode-se garantir a existência de solução não trivial para formas aditivas em n variáveis e grau k no corpo dos números p-ádicos, denotado por $\mathbb{Q}_p$. Um problema clássico, relacionado a sistemas de formas aditivas sobre o corpo dos números p-ádicos, é garantir a solubilidade não trivial p-ádica de tais sistemas. Um bom resultado é dado pelo *Teorema de Dörner* [2]:

Teorema 1. *Sejam r, k, n inteiros positivos com $k > 1$ e $n > 2rk$. Existe um $p_0 = p_0(r,k)$ tal que todo sistema de equações*

$$F_i(x) = a_{i1}x_1^k + \cdots + a_{in}x_n^k = 0, i = 1, ..., r \tag{1}$$

com coeficientes $a_{ij} \in \mathbb{Z}$, tem uma solução p-ádica não trivial para todo $p > p_0(r,k)$.

A respeito do teorema acima sabe-se que a estimativa para o número de variáveis $n > 2rk$ é a melhor possível. Assim a questão que permanece é a obtenção de uma estimativa para $p_0(r,k)$.

Baseados na conjectura de Wooley [4], Atkinson, Brüden e Cook mostraram em [1] que podemos tomar $p_0(r,k) = k^{2r+2}$. Este resultado é garantido via *Lema de Hensel* demonstrando-se o seguinte teorema:

Teorema 2. *Sejam $m = 2r+1$, $b_{ij}, d_i \in \mathbb{Z}$ tais que $B = (b_{ij})$ é altamente não singular no corpo $K = \mathbb{F}_p$. Então o sistema de congruências*

$$b_{i1}x_1^k + \cdots + b_{im}x_m^k \equiv d_i(modp), i = 1, ..., r \tag{2}$$

tem solução não singular módulo p para todo primo $p > k^{2r+2}$.

Para o nosso objetivo, utilizaremos o teorema (2) apenas no caso em que $K = \mathbb{F}_p$, entretanto o resultado também é verdadeiro para o caso mais geral em que $K = \mathbb{F}_q$, $q = p^f$. Esta generalização pode ser encontrada em [1].

Algumas Definições

Definição 1. *Seja $B = (b_{ij})$ uma matriz $r \times m$ num corpo K. Para cada $0 \le d \le r$, denotamos por $\mu(d, B)$ o número máximo de colunas de B que estão em um mesmo subespaço d-dimensional de K^r. Em particular, se $m = 2r+1$ e $\mu(d,B) \le 2d$ para todo $d \le r-1$ dizemos que B é* ***altamente não singular****.*

Definição 2. *Para $b_{ij}, d_i \in \mathbb{Z}$, uma solução x de (2)é dita de posto ρ se a matriz $(b_{ij}x_j)$ tem posto ρ em $\mathbb{F}_p$, e é dita* ***não singular*** *se a matriz tem posto máximo.*

Definição 3. *Para $1 \le \nu \le r$ definimos $q_\nu(B)$ como sendo o número mínimo de componentes com entradas não nulas em pelo menos uma das ν combinações lineares linearmente independentes das linhas de uma matriz B.*

Demonstração do Teorema (2)

Lema 1. *Seja A uma matriz $r \times m$ sobre um corpo K e t um inteiro positivo. Então A possui t submatrizes $r \times r$ não singulares sobre K disjuntas, se e somente se,*

$$m - \mu(d, A) \ge t(r-d) \tag{3}$$

vale para todo $d \le r-1$.

Segue imediatamente que se B é uma matriz $r \times (2r+1)$ altamente não singular, então B contém duas matrizes $r \times r$ não singulares.

Reenumerando as variáveis e usando operações sobre as linhas, a matriz B dos coeficientes da congruência (2) pode ser reescrita na forma $[I, B_0]$ onde I é a matriz identidade $r \times r$ e B_0 é uma matriz $r \times (r+1)$. Com esta matriz dos coeficientes e $u = (u_1, ..., u_r)$ nós associamos as formas lineares

$$\Lambda_j = u_1 b_{1j} + \cdots + u_r b_{rj} \quad j = 1, ..., m \tag{4}$$

onde $m = 2r+1$. Então

$$\Lambda_j = u_j, \quad \text{para} \quad j = 1, ...r. \tag{5}$$

Então, para cada matriz B $r \times m$ temos

$$\mu(d, B) + q_{r-d}(B) = m. \tag{6}$$

Note que uma matriz B $r \times (2r+1)$ é altamente não singular se, e somente se, $q_i(B) > 2i$ para $i = 0, ..., r-1$.
Nós classificamos os pontos $u \not\equiv 0$ nos subconjuntos $\mathcal{S}_\tau$, onde $u_{\tau+1}$ é a primeira variável não nula entre $u_1, ..., u_r$.

Em outras palavras, podemos escrever $\mathcal{S}_\tau$ da seguinte maneira:

$$\mathcal{S}_\tau = \left\{u \in \mathbb{F}_p^r : u_1 = \cdots = u_\tau = 0, u_{\tau+1} \neq 0\right\} \quad 0 \le \tau \le r-1. \tag{7}$$

Para um τ fixo, com $0 \le \tau \le r-1$, sejam Λ_j^* as restrições de Λ_j ao espaço vetorial $\mathcal{S}_\tau^{'} = \mathcal{S}_\tau \cup \{\mathbf{0}\}$. Neste subespaço as formas $\Lambda_1^*, ..., \Lambda_m^*$ têm uma matriz $(r-\tau) \times m$

$$B' = [0_\tau, I_{r-\tau}, B_1],$$

onde B_1 consiste nas $r-\tau$ últimas linhas de B_0. Se tomarmos quaisquer ν combinações lineares, linearmente idependentes, das linhas de B' estaremos simplesmente tomando as mesmas combinações lineares das linhas de B, e portanto $q_\nu(B') \ge q_\nu(B)$ para $\nu = 1, ..., r-\tau$.

Então, $q_\nu(B') > 2\nu$ para $\nu = 1, ..., r-\tau-1$. A primeira coluna não nula corresponde a $u_{\tau+1}$ e as $2r-\tau$ colunas restantes dão uma matriz B'' $(r-\tau)\times(2r-\tau)$ satisfazendo $q_\nu(B'') \ge 2\nu$. Portanto, pelo Lema (1) estas $2r-\tau$ colunas contêm duas matrizes $(r-\tau)\times(r-\tau)$ não singulares e disjuntas. Podemos então reenumerar as colunas $\tau+2, ..., 2r+1$ para obter dois conjuntos disjuntos de $r-\tau$ elementos

$$V_1 = \{\tau+2, ..., r+1\}, \quad V_2 = \{r+2, ..., 2r-\tau+1\}, \tag{8}$$

tais que para $i = 1, 2$ as restrições Λ_ν^* das formas lineares Λ_ν a $\mathcal{S}_\tau$, são conjuntos de formas linearmente independentes.

Para demonstrar o teorema (2) vamos usar somas exponenciais e estimar um limite superior para o número de soluções singulares.
Seja ξ uma raíz primitiva p-ésima da unidade. Definimos

$$T(u) = \sum_{xmodp} \xi^{ux^k} \tag{9}$$

Para $u \not\equiv 0(modp)$, temos que

$$|T(u)| \le (k-1)\sqrt{p}. \tag{10}$$

Defina

$$S = \sum_{umodp} |T(u)|^2, \tag{11}$$

então o número de soluções da congruência $x^k \equiv y^k(modp)$ é igual a $p^{-1}S$. Para cada $x \not\equiv 0$(mod p) temos no máximo k soluções para y, e portanto

$$\mathcal{S} \le p(1 + k(p-1)) < kp^2. \tag{12}$$

Assim o número N de soluções do sistema de congruências (2) é dado por

$$p^r N = \sum_{umodp} T(\Lambda_1(u)) \ldots T(\Lambda_m(u)) \xi^{-\mathbf{u.d}} \tag{13}$$

Classificando os pontos $u \not\equiv 0$ nos subconjuntos $\mathcal{S}_\tau$ e denotando por Σ_τ o lado direito de (13) aplicado nos pontos $u \in \mathcal{S}_\tau$ obtemos

$$|p^r N - p^m| \le \Sigma_0 + \Sigma_1 + \cdots + \Sigma_{r-1} \tag{14}$$

e usando a estimativa trivial para $|T(u)|$,

$$\Sigma_\tau \le p_\tau \sum_{u \in \mathcal{S}_\tau} |T(\Lambda_{\tau+1}(u)) \ldots T(\Lambda_m(u))|. \tag{15}$$

Para $i = 1, 2$ as funções $(u_{\tau+1}, ..., u_r) \mapsto (\Lambda_\nu^* : \nu \in V_i)$ são não singulares e então

$$\Sigma_\tau \le (k-1)\sqrt{p}p^{2\tau}(\theta_1\theta_2)^{1/2} < (k-1)k^{r-\tau}p^{2r+(1/2)}, \tag{16}$$

onde

$$\theta_i = \sum_{\mathcal{S}_\tau} \prod_{\nu \in V_i} |T(\Lambda_\nu^*)|^2 = \sum_{\mathcal{S}_\tau} \prod_{j=\tau+1}^{r} \left|T(u_j)\right|^2 = \mathcal{S}^{r-\tau}. \tag{17}$$

Usando (14) e lembrando que estamos tomando $m = 2r+1$ temos:

$$\left|N - p^{r+1}\right| < k^{r+1}p^{r+(1/2)} - kp^{r+(1/2)} \tag{18}$$

Note que, para $p > k^{2r+2}$, o lado direito de (18) é menor ou igual a p^{r+1}, donde obtemos $kp^{r+(1/2)} < N$. Desse modo, para provarmos a afirmação do teorema (2) é suficiente mostrarmos que o número de soluções singulares Σ^* satisfaz

$$\Sigma^* < kp^{r+(1/2)}. \tag{19}$$

Sendo assim, para provar (19), suponha que exista uma solução de posto $\nu > 0$ com t variáveis não nulas. Como B é altamente não singular temos que $\nu \le t \le 2\nu$. Usando operações sobre as linhas e reenumerando as t colunas obtemos $[I_\nu, C]$, onde C é uma matriz $\nu \times (t-\nu)$. As variáveis não nulas correspondentes às colunas de C podem ser escolhidas livremente, de $(p-1)^{t-\nu}$ maneiras. Para cada escolha temos uma equação de grau k sobre as variáveis correspondentes a I_ν, o que nos dá k^ν escolhas para estas variáveis.

Segue imediatamente que

$$\Sigma^* \le 1 + \sum_{\nu=1}^{r-1}\sum_{t=\nu}^{2\nu} \binom{2r+1}{t} k^\nu (p-1)^{t-\nu}.$$

Através de cálculos simples podemos notar que

$$\binom{2r+1}{t} < 2^{2r}$$

$$1 + (p-1) + \cdots + (p-1)^\nu \le p^\nu$$

$$\Sigma^* < 2^{2r}\sum_{\nu=1}^{r-1}(kp)^\nu.$$

Para $k \ge 2$ temos que $kp/(p-1) \le 2$, donde

$$kp + (kp)^2 + \cdots + (kp)^{r-1} < 2(kp)^{r-1}.$$

Desse modo , para $p > k^{2r+2}$ obtemos

$$\Sigma^* < p^{r+(1/2)} \tag{20}$$

mostrando que (19) vale e garantindo a existência de solução não singular para o sistema de congruências (2).

Temos mostrado portanto que o resultado acima é válido para todo d_i, $i = 1, ..., r$. Tomando $d_i = 0, \forall i = 1, ..., r$ podemos então garantir a existência de solução p-ádica não trivial para o sistema de equações (1) através da seguinte versão do **Lema de Hensel**:

Lema 2. Se p não divide k e as congruências

$$\alpha_{l1}x_1^k + \cdots + \alpha_m x_m^k \equiv 0(\text{modp}), \; l = 1, ..., r \tag{21}$$

têm solução de posto r, mod p, então as equações

$$\alpha_{l1}x_1^k + \cdots + \alpha_m x_m^k = 0 \tag{22}$$

têm solução p-ádica não trivial.

Bibliografia

[1] O.D. Atkinson, J. Bründern, R.J.Cook, *Simultaneous additive congruences to a large prime modulus.* Mathematika, 39 (1992), 1-9.
[2] E. Dörner, *Simultaneous diagonal equations over certain p-adic fields.* J. Number Theory, 36 (1990), 1-11.
[3] I.D. Meir, *Simultaneous Diagonal p-adic Equations.* Mathematika, 45 (1998), 337-349.
[4] T.D. Wooley, *On simultaneous additive equations III.* Mathematika, 37 (1990), 85-96. [5] O. D. Atkinson, R. J. Cook, *Pairs of additive congruences to a large prime modulus.* J. Austral. Math. Soc., 46A (1989), 438-455.
[6] H. Davenport, D. J. Lewis, *Simultaneous equations of additive type.* Phil. Trans. Roy. Soc. London,264A (1969), 557-595.
[7] Borevich, Z. I.,Shafarevich, I. R., *Number Theory.*
[8] Godinho, H., Shokranian, S.,Soares, M., *Teoria dos números.*
[8] Rudolf Lidl and Harald Niederreiter, *Finite Fields.*

Apoio