SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Ekvationssystem i $\mathbb{Z}_2[x_1, \ldots, x_n]$

av

Tobias Andersen

2013 - No 1

Ekvationssystem i $\mathbb{Z}_2[x_1, \ldots, x_n]$

Tobias Andersen

Självständigt arbete i matematik 15 högskolepoäng, Grundnivå

Handledare: Ralf Fröberg

2013

Abstract

Vi betraktar ringen $R = \mathbb{Z}_2[x_1, \ldots, x_n]/(x_1^2 - x_1, \ldots, x_n^2 - x_n)$. Vi visar att det finns en naturlig 1-1-motsvarighet mellan elementen i R och delmängder till $\mathbb{Z}_2^n$, där $f \in R$ svarar mot $\{p \in \mathbb{Z}_2^n; f(p) = 0\}$.

Ekvationssystem i $\mathbb{Z}_2[x_1, \ldots, x_n]$

Tobias Andersen

January 28, 2013

1 Inledning

I det första avsnittet behandlas Gröbnerbaser och vi beskriver hur man räknar ut dem. I det andra avsnittet bevisar vi vårt huvudresultat att det finns en naturlig 1-1 motsvarighet mellan delmängder till $\mathbb{Z}_2^n$ och element i $\mathbb{Z}_2[x_1, \ldots, x_n]/(x_1^n - x_1, \ldots, x_n^2 - x_n)$. Vi kan definiera en addition och multiplikation på mängden av delmängder till $\mathbb{Z}_2^n$ så att man får en ring. I det sista avsnittet har vi att denna ring är isomorf med en ring som har mängden av delmängder till $\mathbb{Z}_2^n$ som element och additionen $A + B = (A \cap B^c) \cup (A^c \cap B)$, (det vill säga den symmetriska produkten av A och B) och multiplikationen $A \cdot B = A \cap B$.

2 Gröbnerbaser

Låt $\Bbbk$ vara en kropp. Monom i en polynomring $\Bbbk[x_1, \ldots, x_n]$ är element på formen $x_1^{e_1} \cdots x_n^{e_n}$.

Definition En monomordning definerar vi som

- För varje par av monom m, n har vi $m \prec n$ eller $n \prec m$ eller $m = n$.
- Om $m_1 \prec m_2$ och $m_2 \prec m_3$ då är $m_1 \prec m_3$.
- $1 \prec m$ för varje monom $m \neq 1$.
- Om $m_1 \prec m_2$ då är $mm_1 \prec mm_2$ för varje monom m.

Ett exempel på en monomordning är den lexikografiska ordningen (lex). Här gäller att $x_1^{i_1} \cdots x_n^{i_n} \prec x_1^{j_1} \cdots x_n^{j_n}$ om $i_1 = j_1, \ldots, i_k = j_k, i_{k+1} < j_{k+1}$ för något k.

Sats 1. *Lex är en monomordning*

Bevis Det gäller att

- Lex är en totalordning är klart. Det vill säga, om m och n är monom så är $m \prec n$ eller $m = n$ eller $m \succ n$
- Låt $m_1 = x_1^{a_1} \cdots x_n^{a_n}, m_2 = x_1^{b_1} \cdots x_n^{b_n}, m_3 = x_1^{c_1} \cdots x_n^{c_n}$. Eftersom $m_1 \prec m_2$ finns ett k så att $a_1 = b_1, \ldots, a_k = b_k, a_{k+1} < b_{k+1}$. Eftersom $m_2 \prec m_3$ finns ett l så att $b_1 = c_1, \ldots, b_l = c_l, b_{l+1} < c_{l+1}$. Då är $a_1 = c_1, \ldots, a_s = c_s, a_{s+1} < c_{c+1}$, om $s = \min(k, l)$. Alltså är $m_1 \prec m_3$.
- $1 = x_1^0 \cdots x_n^0 \prec m$ om $m \neq 1$.
- Antag att $m_1 \prec m_2$ där $m_1 = x_1^{a_1} \cdots x_n^{a_n}$ och $m_2 = x_1^{b_1} \cdots x_n^{b_n}$. Då gäller att $a_1 = b_1, \ldots, a_i = b_i, a_{i+1} < b_{i+1}$ för något i. Låt $m = x_1^{c_1} \cdots x_n^{c_n}$. Då är $mm_1 = x_1^{a_1+c_1} \cdots x_n^{a_n+c_n}$ och $mm_2 = x_1^{b_1+c_1} \cdots x_n^{b_n+c_n}$. Och $a_1 + c_1 = b_1 + c_1, \ldots, a_i + c_i = b_i + c_i, a_{i+1} + c_{i+1} < b_{i+1} + c_{i+1}$. Alltså om $m_1 \prec m_2$ så är $mm_1 \prec mm_2$. □

Antag nu att vi har en polynomring $S = \Bbbk[x_1, \ldots, x_n]$ och en monomordning $\prec$. Då definieras $l(f)$ för $f \in \Bbbk[x_1, \ldots, x_n]$ som det största monomet som har koefficient inte lika med noll.

Vi kommer bara betrakta ordningen lex i fortsättningen.

Exempel: $f = x^7y^2z^3 + 2x^7y^3z^5 + x^8z$. Då är $l(f) = x^8z$.

Om I är ett ideal i $S = \Bbbk[x_1, \ldots, x_n]$ då definieras $l(I)$ som det ideal som genereras av alla $l(f)$ för alla $f \in I$.

En Gröbnerbas för ett ideal i en polynomring är en uppsättning polynom i idealet sådana att de ledande monomen i dessa polynom genererar de ledande monomen för alla polynom i idealet. Det finns en algoritm för att konstruera Gröbnerbasen för ett ideal. Den har två ingredienser:

- Beräkning av S-polynom.
- Reduktion.

Man startar med ett generatorsystem för idealet och en monomordning. Sedan beräknar man S-polynomet för ett par av generatorer. Om $f = m + f_1$ och $g = n + g_1$, där m respektive n är de ledande monomen, så är S-polynomet av f och g $S(f,g) = (lcm(m,n)/m)f - (lcm(m,n)/n)g$. Sedan beskriver vi reduktion. Låt $f = m + f_1$ vara ett polynom i basen, där m är det ledande monomet. Antag att g är ett annat polynom i basen som innehåller ett monom som är delbart med m, dvs av formen mm_1. Då ersätter man mm_1 med $-f_1m_1$. Algoritmen går nu till så att man beräknar S-polynomen av alla par av element i basen och reducerar dem. Om ett S-polynom inte reduceras till 0, så lägger man till det till basen och fortsätter. Man är klar när alla S-polynom reduceras till 0. Algoritmen kallas för Bucherbergers algoritm och Buchberger var en elev till Gröbner.

Exempel: Låt $I = (f,g)$ där $f = x^2 + y^2, g = xy + y^2$, där x^2 resp. xy är ledande monom. Då är $lcm(x^2, xy) = x^2y$ och $S(f,g) = yf - xg = y^3 - xy^2$. I $y^3 - xy^2$ ersätts xy med $-y^2$, så xy^2 blir $-y^3$ och resultatet blir $y^3 - (-y^3) = 2y^3$, som inte kan reduceras. Man lägger till y^3 till basen som nu är $x^2 + xy, xy + y^2, y^3$ (i stället för $2y^3$ kan man lägga till y^3 som genererar samma sak). Sedan räknar man ut S-polynomen av alla par som inte redan räknats ut och reducerar dem med alla ledande monom. Så fortsätter man tills alla S-polynom reduceras till 0. Då har man en Gröbnerbas. $S(xy + y^2, y^3) = y^2(xy + y^2) - xy^3 = y^4$ reduceras till noll. Slutligen är $S(x^2 + xy, y^3) = y^3(x^2 + xy) - x^2y^3 = xy^4$, som reduceras till 0 med y^3. Alltså är $x^2 + xy, xy + y^2, y^3$ en Gröbnerbas för idealet.

Vi såg att $S(x^2 + xy, y^3)$ reduceras till 0. Det är ingen tillfällighet som nästa sats visar.

Sats 2. *Om $I = (f_1, \ldots, f_k)$ och $gcd(f_i, f_j) = 1$ då $i \neq j$ så är $\{l(f_1) \ldots l(f_k)\}$ en Gröbnerbas för I. Det räcker att bevisa fallet då jag har f_1, f_2 och $l(f_1), l(f_2)$ relativt prima. Då kommer $S(f_1, f_2)$ reduceras till 0.*

Bevis Låt $f_1 = \underbrace{m}_{l(f_1)} + g_1$ och $f_2 = \underbrace{n}_{l(f_2)} + g_2$. $S(f_1, f_2) = n(m + g_1) - m(n + g_2) = mn + ng_1 - mn - mg_2 = ng_1 - mg_2$. Detta ger att $(-g_2)g_1 - g_2(-g_1) = -g_1g_2 + g_1g_2 = 0$ ifall man sätter $n = -g_2$ och $m = -g_1$. □

Sats 3. *Alla monom som inte ligger i $l(I)$ utgör en k-bas för S/I.*

Bevis Alla monom som ligger i $l(I)$ kan reduceras. Kvar blir bara linjärkombinationer av monom utanför $l(I)$, så monomen utanför $l(I)$ genererar S/I. Dessa monom är också linjärt oberoende för de kan inte reduceras. De utgör alltså en bas för S/I. □

3 Huvudresultatet

Låt $S = \mathbb{Z}_2[x_1, ..., x_n]$ vara en polynomring i n variabler och låt $I = (x_1^2 - x_1, ..., x_n^2 - x_n)$.

Sats 4. *Generatorerna för I utgör en Gröbnerbas.*

Bevis x_i^2 och x_j^2 är relativt prima om $i \neq j$ så vi kan använda Sats 2. Vi har alltså $l(I) = (x_1^2, \ldots, x_n^2)$. De monom som ligger utanför $l(I)$ är alltså de kvadratfria monomen. □

Sats 5. *Antalet nollskilda monom i S/I är 2^n.*

Bevis Varje monom utanför $l(f)$ är på formen $x_{i_1} \cdots x_{i_k}$ där inga värden på index kan förekomma mer än en gång. Det finns n variabler att välja mellan, och varje variabel är antingen med i monomet eller inte. Detta ger 2^n möjligheter. □

Sats 6. *Antalet element i S/I är 2^{2^n}.*

Bevis Elementen i S/I är $1, x_1, x_2, \ldots, x_n$ samt alla parvisa produkter $x_1x_2, \ldots$, samt alla trippelprodukter $x_1x_2x_3, \ldots$, osv. Totalt finns alltså

$$\binom{2^n}{0} + \binom{2^n}{1} + \ldots + \binom{2^n}{2^n} = 2^{2^n}$$

element. □

Sats 7. *Antalet element i $\mathbb{Z}_2^n$ är 2^n.*

Bevis Varje element i $(Z_2)^n$ är på formen $(a_1, \ldots, a_n)$ där a_i är antingen 0 eller 1. Alltså finns det 2^n element. □

Sats 8. *Antalet delmängder i $\mathbb{Z}_2^n$ är 2^{2^n}*

Bevis Jag väljer ut alla 0-delmängder, 1-delmängder, ..., 2^n-delmängder. Det finns totalt

$$\binom{2^n}{0} + \binom{2^n}{1} + \ldots + \binom{2^n}{2^n} = 2^{2^n}$$

delmängder. □

Punkterna i $\mathbb{Z}_2^n$ kan exempelvis utgöra nollställen till ovannämnda polynom. Antalet delmängder i $\mathbb{Z}_2^n$ är också 2^{2^n} st och jag vill undersöka om det finns en naturlig 1-1 motsvarighet mellan alla polynom i S/I och alla delmängder i $\mathbb{Z}_2^n$. Kalla dessa delmängder för M.

Låt

$$f = \sum_{(a_1,\ldots,a_n)\in R} x_1^{a_1} \cdots x_n^{a_n}$$

där $R = \mathbb{Z}_2^n \setminus \{(0,\ldots,0)\}$.

Jag vill visa att f har punkten $(0,0,\ldots,0)$ som enda nollställe.

Lemma 1. *f har origo som enda nollställe.*

Bevis Det är klart att $f(0,\ldots,0) = 0$. Antag nu att $t \in S$ är ett nollställe där $t = (\underbrace{1,1,\ldots,1}_{i \text{ st}},\underbrace{0,0,\ldots,0}_{n-i \text{ st}})$. Följande gäller även om ettorna är placerade på något annat sätt. $f(t) = i + \binom{i}{2} + \binom{i}{3} + \ldots + \binom{i}{i} = 2^i - 1$ vilket är kongruent med 1 modulo 2, vilket innebär att $f(a) = 1$ för alla $a \neq (0,\ldots,0)$. □

Det är nu enkelt att bestämma ett polynom som bara har en enda punkt som nollställe. Exempelvis har $g_{(1,1,0,\ldots,0)} = f(x_1 - 1, x_2 - 1, x_3, \ldots, x_n)$ ett enda nollställe $(1,1,0,\ldots,0)$. Polynom med ett enda nollställe i en punkt p kallar vi för e_p.

Om $f \in \mathbb{Z}_2[x_1,\ldots,x_n]/(x_1^2 - x_1, \ldots, x_n^2 - x_n]$ betecknas $\{p \in \mathbb{Z}_2^n; f(p) = 0\}$ med $V(f)$ och vi kallar $V(f)$ för nollställemängden för f.

Lemma 2. *För varje delmängd $M \subset \mathbb{Z}_2^n$ finns $f \in S/I$ så att $V(f) = M$, dvs f har precis punkterna i M som nollställen.*

Bevis Låt M bestå av $p_1, p_2, \ldots, p_k$. Då har polynomet $e_{p_1} \cdots e_{p_k}$ alla punkter i M som nollställe och inga andra. □

Eftersom $\mathbb{Z}_2[x_1,\ldots,x_n]/(x_1^2 - x_1, \ldots, x_n^2 - x_n)$ är en ring ger detta möjligheten att göra mängden av delmängder till $\mathbb{Z}_2^n$ till en ring.

Sats 9. *Givet $f, g \in S/I$ samt mängderna $A = V(f), B = V(g)$. Då är $V(fg) = A \cup B$.*

Bevis $fg = 0$ om $f = 0$ eller $g = 0$ så $V(fg) = V(f) \cup V(g)$. □

Sats 10. $V(f + g) = (A \cap B) \cup (A^c \cap B^c)$.

Bevis Om $f(p) = g(p) = 0$ så är $(f + g)(p) = 0$. Alltså $p \in V(f) \cap V(g)$. Om $f(p) = 0, g(p) = 1$ eller $f(p) = 1, g(p) = 0$ så är $(f + g)(p) = 1$. Om $f(p) = g(p) = 1$ så är $(f + g)(p) = 0$. Alltså $p \in V(f)^c \cap V(g)^c$. Alltså är $V(f + g) = (V(f) \cap V(g)) \cup (V(f)^c \cap V(g)^c)$. □

Vi har sett att det finns lika många element som S/I som antalet delmängder av $\mathbb{Z}_2^n$. Det finns alltså en bijektion mellan dessa, specifikt avbildningen $\Phi : S/I \longrightarrow M$ där M är mängden av delmängder till $\mathbb{Z}_2^n$, definierad av $\Phi(f) = V(f)$. Det följer nu att mängden av delmängder till $\mathbb{Z}_2^n$ blir en ring som är isomorf med S/I om vi för delmängder A och B definierar $A + B = (A \cap B) \cup (A^c \cap B^c)$ och $A \cdot B = A \cup B$.

Sats 11. *Avbildningen $\Phi : S/I \longrightarrow M$ där M är mängden av delmängder till $\mathbb{Z}_2^n$, definierad av $\Phi(f) = V(f)$ är en isomorfi.*

Bevis Detta följer av satserna 9, 10 och 11. □

Sats 12. *Nollan i S/I svarar mot hela mängden $\mathbb{Z}_2^n$. Ettan svarar mot tomma mängden. Mängden som svarar mot $1+f$ är komplementet till mängden som svarar mot f.*

Sats 13. *Alla element i S/I är idempotenta dvs $\forall f \in S/I$ så är $f^2 = f$.*

Bevis Eftersom $V(f^2) = V(f)$ gäller $f^2 = f$ då vi har en isomorfi mellan S/I och M. □

4 En annan ringstruktur

Om M är en mängd så finns det ett standardsätt att göra mängden av delmängder till M till en ring.

Sats 14. *Om A och B är delmängder till M definierar man $A \oplus B = S(A, B) = (A \cap B^c) \cup (A^c \cap B)$ (den symmetriska differensen av A och B), och $A \times B = A \cap B$. Då blir mängden av delmängder till M en ring med addition $\oplus$ och multiplikation $\times$.*

Bevis Eftersom $A \oplus \emptyset = S(A, \emptyset) = A$ är $\emptyset$ nollelement i R. Eftersom $A \times M = A \cap M = A$ är M enhetselement (etta) i R. Additionen är kommutativ eftersom $A \oplus B = S(A, B) = S(B, A) = B \oplus A$. Multiplikationen är kommutativ eftersom $A \times B = A \cap B = B \cap A = B \times A$. Additionen är associativ eftersom $(A \oplus B) \oplus C = S(A, B) \oplus C = S(S(A, B), C)$ och $A \oplus (B \oplus C) = A \oplus S(B, C) = S(A, S(B, C))$. Man övertygar sig lätt, t.ex. med ett Venndiagram, att både $S(S(A, B), C)$ och $S(A, S(B, C))$ består av de element som ligger i precis en av A, B, C tillsammans med $A \cap B \cap C$. Multiplikationen är associativ eftersom $(A \times B) \times C = A \cap B \times C = (A \cap B) \cap C = A \cap (B \cap C) = A \times (B \times C)$. Slutligen visar vi distributiviteten. $A \times (B \oplus C) = A \cap S(B, C)$ och $(A \times B) \oplus (A \times C) = S(A \cap B, A \cap C)$. Nu gäller att $A \cap S(B, C)$ består av de element som ligger i precis en av B, C och samtidigt i A, och $S(A \cap B, A \cap C)$ består av de element som ligger i precis en av $A \cap B, A \cap C$, vilket är samma sak. □

Om nu M är mängden av delmängder till $\mathbb{Z}_2^n$ betecknar vi denna ring med R. Den ring vi behandlade i förgående avsnitt med addition $A + B = (A \cap B) \cup (A^c \cap B^c)$ och multiplikation $A \cdot B = A \cup B$ kallar vi T.

Sats 15. *$\psi : R \longrightarrow T$, där $\psi(A) = A^c$ är en isomorfi.*

Bevis Vi måste visa att $\psi(A \oplus B) = \psi(A) + \psi(B)$, $\psi(A \times B) = \psi(A) \cdot \psi(B)$ och att ψ är en bijektion.

Nu är $\psi(A \oplus B) = \psi(S(A, B)) = (S(A, B))^c = ((A \cap B^c) \cup (A^c \cap B))^c = (A \cap B^c)^c \cap (A^c \cap B)^c = (A^c \cup B) \cap (A \cup B^c)$.$\psi(A) + \psi(B) = A^c + B^c = (A^c \cap B^c) \cup (A \cap B)$. Både $\psi(A \oplus B)$ och $\psi(A) + \psi(B)$ består alltså av de punkter som ligger i både A och B tillsammans med de punkter som ligger utanför både A och B. Att ψ är en bijektion följer av att det enda elementet som avbildas på $\emptyset$ (nollan i T) är $\mathbb{Z}_2^n$ (nollan i R). □

References

[1] Ralf Fröberg, *An Introduction to Gröbner Bases*. John Wiley & Sons, 1997.