SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Bildandet av en Gröbnerbas för den böjda funktionen $x_1x_2 + \ldots + x_{n-1}x_n$

av

Walter Berge

2021 - No K9

Bildandet av en Gröbnerbas för den böjda funktionen $x_1x_2 + \ldots + x_{n-1}x_n$

Walter Berge

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Samuel Lundqvist

2021

Abstract

In this paper we study a particular bent function (bent functions defined by Rothaus in 1975) from a Groebner basis perspective. By generating an ideal from the chosen bent function in conjunction with a set of polynomials limiting the variety to Z_2^n we construct Groebner bases algorithmically in various dimensions and analyze them to find a pattern. From this pattern we construct a set of polynomials which we then prove to be a Groebner basis for this ideal. It is possible that other bent functions have Groebner bases that can be described in this way which may lead toward a general classification of bent functions.

Abstrakt

Detta arbete undersöker den böjda funktionen $x_1x_2+\cdots+x_{n-1}x_n : \mathbb{Z}_2^n \to \mathbb{Z}_2$ från ett Gröbnerbasperspektiv. Idealet $I_n = \langle x_1x_2 + \cdots + x_{n-1}x_n, x_1^2 + x_1, \ldots, x_n^2 + x_n\rangle$ bildas i polynomringen $\mathbb{Z}_2[x_1, \ldots, x_n]$ och en Gröbnerbas genereras med hjälp av datoralgebraprogram för flera n. Analys av resultaten leder till bildandet av en polynommängd som hypotetisk Gröbnerbas. Vi visar sedan att denna mängd är en Gröbnerbas för det givna idealet för godtyckliga jämna n.

Innehåll

1 Frågeställning

Vi vill undersöka **Gröbnerbasen** till den **böjda funktionen** $x_1x_2 + \cdots + x_{n-1}x_n$. Gröbnerbasen ger insikt i huruvida ett polynom i **polynomringen** $k[x_1, \ldots, x_n]$ ingår i **idealet** som genereras av en mängd polynom. För att bestämma Gröbnerbasen av ett ideal används **Buchbergers algoritm**. Vi kommer beräkna Gröbnerbasen till idealet $I_n = \langle x_1x_2 + \cdots + x_{n-1}x_n, x_1^2 + x_1, \ldots, x_n^2 + x_n \rangle \subseteq \mathbb{Z}_2[x_1, \ldots, x_n]$ med hjälp av ett datorprogram för att sedan bestämma formen på Gröbnerbasen. Vi vill beskriva hur denna Gröbnerbas ser ut i godtycklig dimension samt bevisa att det är en Gröbnerbas. Ett sådant resultat kommer tillåta oss att undvika Buchbergers algoritm och istället konstruera en Gröbnerbas utifrån en given form.

En vinst med detta är att vi kan beskriva Gröbnerbasen för mycket stora n och undviker begränsningar i beräkningskapacitet hos datorer.

En Gröbnerbas hjälper oss att se vissa egenskaper hos ett ideal, till exempel så ger det en metod för att avgöra hur många nollställen I_n har. Mängden nollställen betecknas **varieteten** $V(I)$.

Det finns ännu ingen klassificering [1] av böjda funktioner och vi hoppas att kunna utröna något mer om deras egenskaper genom att studera just dessa Gröbnerbaser. Böjda funktioner definieras i avsnitt **2.3**.

2 Teoretisk Bakgrund

2.1 Ringar och ideal

2.1.1 Ringar

En **ring** R är en algebraisk struktur med två binära operationer, $+$ och $\cdot$ med egenskaperna att:

a. ringen är en kommutativ grupp för $+$, och

b. den är sluten, associativ och distributiv för $\cdot$.

2.1.2 Polynomringar

En **polynomring** betecknas $k[x_1, \ldots, x_n]$ där k är en **kropp** och $x_1, \ldots, x_n$ är **variabler**. **Monom** m är en produkt av variabler $x_1, \ldots, x_n$ på formen $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n}$ där $\alpha_i \geq 0$; en **term** t är ett monom med en **koefficient** ur k så att $t = km$ och ett **polynom** p är en summa av termer. Vi kan skriva ett polynom f som $f(x_1, \ldots, x_n)$ för att visa att f beror på variablerna $x_1, \ldots, x_n$. Variabler kan ges en **tolkning** a där $x_i : i = 1, \ldots, n$ ges ett

värde $x_i = a_i,\ a_i \in k$. Vi får då att vårt polynom $f(a_1, \ldots, a_n) = b$. Att $k[x_1, \ldots, x_n]$ verkligen är en ring är lätt att verifiera.

Låt oss ge ett exempel. I detta arbete kommer vi röra oss i polynomringen $\mathbb{Z}_2[x_1, \ldots, x_n]$. Detta innebär att vi väljer koefficienter ur kroppen $\mathbb{Z}_2$ vilken består av elementen $\{0, 1\}$. Addition och multiplikation fungerar som vanligt i $\mathbb{Z}_2$ med undantaget att $1 + 1 = 0$ och $0 - 1 = 1$. Vi låter $n = 2$. Vi går nu vidare och konstruerar ett polynom i vår ring. Alla monom i $\mathbb{Z}_2[x_1, x_2]$ är produkter av variablerna x_1 och x_2, till exempel x_1^2, x_1x_2. Vi tar sedan koefficienter ur kroppen $\mathbb{Z}_2$ och bildar termer. Vi kan till sist kombinera våra termer till ett polynom som nedan:

$$f(x_1, x_2) = x_1^3x_2 + x_1x_2^2 + x_1 + x_2.$$

Vi kan nu ge f en tolkning a så att $f(a) = b$.
Tag $a = (0, 1)$. Vi får då

$$f(0, 1) = 0^3 \cdot 1 + 0 \cdot 1^2 + 0 + 1 = 1.$$

2.1.3 Ideal

Definition 2.1 (Ideal)**.** *Ett ideal I är en delmängd av en kommutativ ring R med egenskaperna att*

a. mängden är en additiv delgrupp

b. för varje element i av idealet och $x \in R$ gäller att $ix \in I$. [i]

Ett ideal I är en delmängd av en ring R men kan också vara lika med ringen. Om $1 \in I$ så är $I = R$ då $1 \cdot r : r \in R \Rightarrow r \in I$. Man kan säga att 1 **genererar** I och betecknar detta $\langle 1 \rangle = I$. Mer generellt kan man säga att ett ideal genereras från en mängd polynom $P = \{p_1, \ldots, p_m\}$ genom att skriva $I = \langle p_1, \ldots, p_m \rangle$. I består i detta fall av alla möjliga summor av polynom som kan bildas genom att multiplicera $p \in P$ med polynom ur $k[x_1, \ldots, x_n]$. Att multiplicera ett element i idealet med ett element ur ringen kallas en **R-kombination**.

Ta till exempel polynomringen $\mathbb{Z}_2[x_1, \ldots, x_n]$ och låt $n = 2$. Bilda idealet $I = \langle x_1 \rangle$. Vi har i detta fall att $x_1x_2 + x_1 \in I$ då $x_1(x_2 + 1) = x_1x_2 + x_1$ men $x_1 + x_2$ är *inte* i I då vi inte kan välja ett polynom p sådant att $x_1p = x_1 + x_2$.

[i] För ringar som inte är kommutativa måste definitionen utökas för att inkludera höger och vänstermultiplikation, det vill säga att för varje element i av idealet och $x, y \in R$ gäller att $ix, yi \in I$

Ett viktigt problem i kommutativ algebra är att avgöra ifall ett polynom f i en polynomring är del av ett ideal givet av en genererande mängd polynom P. Då vi i detta arbete kommer att jobba med ringen $\mathbb{Z}_2[x_1, \ldots, x_n]$ så är det här problemet liktydigt med att avgöra ifall det finns några $q_i : q_i \in \mathbb{Z}_2[x_1, \ldots, x_n]$ så att $f = q_1p_1 + \cdots + q_mp_m$.

2.1.4 Kroppspolynom

I det här arbetet kommer vi se på ideal som genereras av något polynom p ur polynomringen $\mathbb{Z}_2[x_1, \ldots, x_n]$ tillsammans med polynomen $x_1^2 + x_1, \ldots, x_n^2 + x_n$. Dessa kallas **kroppspolynom**. Konsekvensen av detta är att betraktandet av polynom i idealet så kommer det var analogt med att betrakta polynom i **kvotringen**

$$\frac{\mathbb{Z}_2^n[x_1, \ldots, x_n]}{\langle x_1^2 + x_1, \ldots, x_n^2 + x_n \rangle}.$$

En kvotring delar upp en ring i **ekvivalensklasser** där $a \sim b$ om a och b ingår i samma ekvivalensklass. I det här fallet får vi de restklasser som bildas vid division med $x_k^2 + x_k$ för $k = 1, \ldots, n$. Rent praktiskt innebär det att $x_k^t \equiv x_k (\text{mod } x_k^2 + x_k)$ för $t \geq 1$. En mer teknisk genomgång av detta följer i resultatdelen.

2.1.5 Några satser om ideal och polynomringar

Sats 2.1 (Hilberts bassats)**.** *Varje ideal $I \subseteq k[x_1, \ldots, x_n]$ har en ändlig genererande mängd. Det vill säga att $I = \langle g_1, \ldots, g_n \rangle$ där $g_1, \ldots, g_n \in I$ [2].*

Satsen påstår alltså att varje ideal I i en polynomring kan genereras av en ändlig mängd polynom, även i de fall då idealet självt är en oändlig mängd. Ta till exempel $I = \langle 1 \rangle, I \subseteq \mathbb{R}[x_1, \ldots, x_n]$. Då gäller att alla de reella talen ingår i I. I innehåller alltså överuppräkneligt många element men genereras av ett enda tal.

Definition 2.2 (Algebraisk tillslutning)**.** *En algebraiskt tillslutning $\bar{k}$ av k är en utvidgning av k så att alla polynom i en variabel av grad > 1 med koefficienter ur k kan faktoriseras i linjära faktorer.*

Denna sats kan också formuleras som att alla polynom i en variabel med koefficienter ur k har ett nollställe i $\bar{k}$. Tänk på de reella talen: polynomet x^2+1 har inga nollställen bland de reella talen. Polynomet har dock lösningen $x = \{i, -i\}$ bland de komplexa talen, vilket också råkar vara den algebraiska slutningen till de reella talen. Det går att visa att varje kropp har en algebraisk tillslutning.

Definition 2.3 (Varietet)**.** *Varieteten av ett ideal* $V(I), I = \langle f_1, \ldots, f_m \rangle$ *över en polynomring* $k[x_1, \ldots, x_n]$ *är mängden punkter* $(a_1, \ldots, a_n) \in \bar{k}^n$ *för vilka det gäller att* $f(a) = 0,\ \forall f \in I$.

Varieteten är alltså lösningsmängden som ger $f(x) = 0$ för alla polynom i idealet. Viktigt är att varieteten tar element ur den algebraiska slutningen till den kropp vår polynomring tar koeffecienter ur vilket innebär att $(a_1, \ldots, a_n)$ inte nödvändigtvis ligger i k^n.

Nästa sats beskriver dock ett fall när vi inte måste ta hänsyn till den algebraiska slutningen av en kropp, och har särskild betydelse i detta arbete där vi rör oss i $\mathbb{Z}_2$.

Sats 2.2. *Om* $I = \langle f_1, \ldots, f_m, x_1^p - x_1, \ldots, x_n^p - x_n \rangle \subseteq \mathbb{Z}_p[x_1, \ldots, x_n]$ *där* p *är ett primtal så är* $V(I) = \{(a_1, \ldots, a_n) \in \mathbb{Z}_p^n | f_i(a_1, \ldots, a_n) = 0\ \forall i\}$.

Bevis. Satsen påstår att vi endast behöver betrakta nollställen i $\mathbb{Z}_p^n$ till polynomen $f_1, \ldots, f_m$ för att finna varieteten. Detta kommer sig av att $\mathbb{Z}_p = (\mathbb{Z}/p\mathbb{Z})^* \cup \{0\}$ för primtal p. Vi kan då utnyttja Fermat's lilla sats

$$a^{p-1} \equiv_p 1 \Leftrightarrow a^p - a \equiv_p 0,\ \forall a \in (\mathbb{Z}/p\mathbb{Z})^*$$

och att $0^p + 0 \equiv_p 0$ alltid är sant. Vi får att polynomet $x_i^p - x_i$ har exakt p nollställen. I $\mathbb{Z}_p[x_1, \ldots, x_n]$ kan vi kan alltså ignorera polynomen $x_i^p - x_i,\ 1 \leq i \leq n$ när vi beräknar varieten för I då de alltid är lika med 0.

Satsen påstår även att varieteten är en delmängd av $\mathbb{Z}_p^n$. Varieteten är snittet

$$V(\langle f_1, \ldots, f_m \rangle) \cap V(\langle x_1^p - x_1 \ldots, x_n^p - x_n \rangle)$$

då vi inte kan ha några nollställen som inte uppfyller kravet på att vara nollställen för båda ideal. Vi vill visa att $V(\langle x_1^p - x_1 \ldots, x_n^p - x_n \rangle) = \mathbb{Z}_p[x_1, \ldots, x_n]$. Från argumentet ovan vet vi att alla punkter i $\mathbb{Z}_p^n$ är nollställen till $\langle x_1^2 + x_1 \ldots, x_n^2 + x_n \rangle$. Vi vill nu visa att det inte finns fler.

Betrakta polynomet $p(x) = x_i^p - x_i$. Tag a_i som ett av dess p nollställen. Då har vi att

$$p(x) = (x_i - a_i)q(x) + r(x)$$

där $r(x)$ är av strikt lägre grad än $x_i - a_i$, alltså en konstant. Utvärdering av $p(a_i)$ ger att den första termen blir noll, och antagandet att a_i är en rot till $p(x)$ leder till slutsatsen att även resttermen är noll. Alltså delar $(x - a_i)\ p(x)$. Vi får då att $p(x)$ har en delare $(x - a_i)$ för var och en av våra p rötter, och då produkten av dessa ger ett polynom av grad p så kan vi inte heller ha fler nollställen. Alltså är det just tolkningarna $a_i = 0, \ldots, p-1,\ 1 \leq i \leq n$ som ger varieteten för $\langle x_1^p - x_1 \ldots, x_n^p - x_n \rangle$ vilket är exakt $\mathbb{Z}_p^n$. □

Definition 2.4 (Nolldimensionellt ideal)**.** *Ett ideal I är* ***nolldimensionellt*** *om $V(I)$ är en ändlig mängd.*

Följdsats 2.2.1. *Ett ideal $I = \langle f_1, \ldots, f_m, x_1^p - x_1, \ldots, x_n^p - x_n \rangle \subseteq \mathbb{Z}_p[x_1, \ldots, x_n]$ är nolldimensionellt.*

Bevis. Satsen följer från **2.2** då $V(I) \subseteq \mathbb{Z}_p^n$ och $\mathbb{Z}_p^n$ är en ändlig mängd. □

Här ser vi igen **kroppspolynomen** $x_1^p - x_1, \ldots, x_n^p - x_n$ som diskuterades i anslutning till polynomringar. I $\mathbb{Z}_2$ blir polynomen just $x_1^2 + x_1, \ldots, x_n^2 + x_n$. En vidare konsekvens av att vi använder kroppspolynomen är att vi inte behöver ta hänsyn till den algebraiska tillslutningen.

En annan egenskap vi får när vi genererar ett ideal med kroppspolynomen i $\mathbb{Z}_2$ är att varieteteten begränsas till $\mathbb{Z}_2^n$ vilket är precis vad som utnyttjas i datavetenskap. Vi får möjlighet att tillämpa våra matematiska resultat i praktiken.

Definition 2.5. *Ett ideal I är* ***radikalt*** *om $f^s \in I \Rightarrow f \in I$.*

Sats 2.3 (Hilberts weak nullstellensatz [2])**.** *Om $I \subseteq k[x_1, \ldots, x_n]$ så gäller att $V(I) = \emptyset \Leftrightarrow 1 \in I$.*

Satsen ovan beskriver fallet då $f(x) = 1$ ingår i idealet. Det är tydligt att det inte finns några lösningar om $1 \neq 0$.

2.2 Gröbnerbaser

Givet ett ideal I så vill vi veta om ett visst element i en ring R är del av detta ideal. Om vi har en mängd som genererar I så innebär detta att man vill avgöra ifall vårt element är en R-kombination av en eller flera element i den genererande mängden med element ur ringen.

Tag en polynomring som exempel: givet en ring $R = k[x_1, \ldots, x_n]$ så kan vi definiera ett ideal $I = \langle p_1, \ldots, p_m \rangle$. Ett polynom $f \subseteq I$ om det finns $q_1, \ldots, q_m$ så att $f = q_1 p_1 + \cdots + q_m p_m$. Detta ser ut som att vi vill dela f med elementen i I och få rest 0. Detta problem är relativt enkelt i de fall vi jobbar med heltal och i polynomringar med en variabel. Dock kräver det efter hand en del tekniska förberedelser när vi dividerar i polynomringar med flera variabler och generande mängder som innehåller linjärt obereoende polynom.

En av de frågor vi behöver lösa är att bestämma gradordning av monom i fler variabler. Det är inte omedelbart tydligt vilket av monomen $x_1^2, x_1 x_2$, och x_2^2 som har lägst grad. Går det att bestämma?

2.2.1 Ordning av monom

Vi vill hitta ett sätt att jämföra graden av monom i flera variabler. En **ordning** av två monom m_1, m_2 tillåter oss att säga att $m_1 \prec m_2, m_1 \succ m_2$ eller $m_1 = m_2$.

Definition 2.6 (Tillåten ordning av monom)**.** *För att en ordning av monom ska vara* ***tillåten*** *måste den vara*

a. ***total****: för alla monom m_1, m_2 så gäller att $m_1 \prec m_2, m_1 \succ m_2$ eller att $m_1 = m_2$*

b. ***transitiv****: om $m_1 \prec m_2$ och $m_2 \prec m_3$ så gäller att $m_1 \prec m_3$*

c. ***kompatibel med multiplikation av monom****: om $m_1 \prec m_2$ så gäller att $mm_1 \prec mm_2$*

d. *ha egenskapen att $1 \prec m$ för alla monom $m \neq 1$.*

Det finns tre standardordningar för monom i flera variabler

1. **Lexikografisk Ordning**

   Givet två monom $m_1 = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ och $m_2 = x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$ så är $m_1 \succ m_2$ i det fall det finns ett k så att för alla $i < k, \alpha_i = \beta_i$ och $\alpha_k > \beta_k$.

2. **Gradordnad Lexikografisk Ordning**

   Givet två monom $m_1 = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ och $m_2 = x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$ så är $m_1 \succ m_2$ om $\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$ eller i det fall då $\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$ så gäller att det finns ett k så att för alla $i < k, \alpha_i = \beta_i$ och $\alpha_k > \beta_k$.

3. **Gradordnad Omvänd Lexikografisk Ordning**

   Givet två monom $m_1 = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ och $m_2 = x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$ så är $m_1 \succ m_2$ om $\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$ eller i det fall då $\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$ så gäller att det finns ett k så att för alla $i > k, \alpha_i = \beta_i$ och $\alpha_k < \beta_k$. Här räknar man bakifrån och jämför först graden av variablerna med högst index.

Lexikografisk ordning ger prioritet till variabler med lägre index. Vi jämför graden av variablerna var för sig och letar efter variabler av lägsta möjliga index. Det monom som har en variabel av högst grad av det lägsta index

som finns bland de jämförda monomen sägs leda det andra. Gradordnad lexikografisk jämförelse tar i första hand hänsyn till den totala graden av alla variabler i monomet och i det fall graden är lika så används lexikografisk ordning. På samma sätt fungerar gradordnad omvänd lexikografisk ordning med den viktiga skillnaden att i de fall den totala graden av två polynom är lika så används lexikografisk ordning men vi jämför först variablerna med lägst prioritet. Märk att ingen ordning tar hänsyn monomets koefficient.

I ett polynom p sägs den term t med högst ordning enligt någon given ordning vara **ledande** och betecknas **lt(p)**.

2.2.2 Reduktion

Vi återvänder nu till vår diskussion om hur man kan avgöra ifall ett polynom ingår i ett visst ideal.

I heltalsaritmetiken är division av ett tal med ett annat en algoritm för två tal a och b som ger tal k och r sådana att $a = kb+r$ där $r < b$. På samma sätt kan man för två polynom i en variabel $p, q \in k[x], q \neq 0$ finna polynom k, r så att $p = kq + r$ där r är av lägre grad än q. Man kallar k **kvot** och r **rest**.

Att subtrahera en multipel av ett polynom från ett annat kallas för **reduktion** och betecknas $p \xrightarrow{\text{q}} p - kq$. Vid reduktion vill vi välja k på ett sätt så att $p - kq$ har så låg grad som möjligt, vilket sammanfaller med att utföra polynomdivision på det sätt som står beskrivet ovan: vi får att $p - kq = r$.

Vi kan också använda utrycket reduktion för att visa att ett polynom f_1 kan reduceras via ett polynom p till ett annat polynom f_2. I det här fallet gäller det inte nödvändigtvis att f_2 är av lägsta möjliga grad utan endast att f_1 kan skrivas som $pk + f_2$ där k är ett polynom. Vi skriver då $f_1 \xrightarrow{\text{p}} f_2$. Reduktion är alltså inte synonymt med polynomdivision.

Vad händer när vi försöker generalisera denna operation till polynom av flera variabler?

2.2.3 Division av polynom med flera variabler

Division av ett polynom $f \in k[x_1, \ldots, x_n]$ med ett annat polynom p i samma ring är en algoritm för att få f på formen $f = qp+r$ där r är ett polynom av så låg grad som möjligt. I avsnittet ovan introducerades ett antal ordningar vilka ger oss möjlighet att jämföra graden av r och p. Vid division med polynom av flera variabler väljer vi en sådan ordning. Det bör påpekas att resultatet beror på vilken ordning vi väljer och är på så vis inte unik.

Då arbetet kommer att utföras i polynomringen $\mathbb{Z}_2[x_1, \ldots, x_n]$ så får vi att alla monom är **moniska**, det vill säga att koefficienten är lika med 1.

Divisionsalgoritmen går att generalisera till koefficienter ur andra kroppar men vi begränsar oss till $\mathbb{Z}_2$.

Algoritm för division med polynom med flera variabler:

Välj en tillåten ordning $\prec$ av monom. Låt $f, p \in k[x_1, \ldots, x_n]$. Tag den ledande termen av p och bilda mängden S bestående av alla termer i f som är delbara med $lt(p)$. Om S är tom så är $f = r$, vi kan alltså inte reducera f med p. Om däremot S innehåller en eller fler termer väljer vi $t : t \in S$ med högst grad och utför beräkningen

$$f_1 = f - \frac{t}{lt(p)}p.$$

Givet att t och p är moniska kommer denna operation kommer att ta bort t från från f men eventuellt lämna oss med nya termer i f_1. Dessa termer är dock av lägre grad än t. Vi upprepar nu samma steg med f_1: vi bildar S utav alla de termer i f_1 som är delbara med $lt(p)$. Om S är tom är $f_1 = r$, annars utför vi beräkningen

$$f_2 = f_1 - \frac{t}{lt(p)}p$$

där t är den ledande termen i S. Vi fortsätter algoritmen fram till dess att $f_i = 0$ eller att S är tom. Termen som återstår är vår rest.

Vi kan förenkla notationen genom att avända reduktionspilar och skriva

$$f \xrightarrow{\text{p}} f_1 \xrightarrow{\text{p}} \ldots \xrightarrow{\text{p}} r.$$

Vi har nu en möjlighet att se ifall ett polynom kan fås från ett annat polynom genom multiplikation. Det här tar oss en bit på vägen mot att kunna avgöra ifall ett visst polynom f är del av ett ideal I givet en genererande mängd polynom P.

2.2.4 Fallet för division med flera polynom

Om vi då har en mängd P med flera polynom som genererar ett ideal I så bör vi kunna dividera ett polynom f med de genererade polynomen och genom att få resten 0 avgöra ifall $f \in I$. Det första vi behöver är en algoritm för denna division. Denna algoritm behöver ta hänsyn till att polynomen i P kan vara linjärt oberoende och därför hantera dessa separat. Vi söker en algoritm som ger oss f på formen $f = q_1p_1 + \cdots + q_mp_m + r$ där r är av så låg grad som möjligt.

Algoritm för division med polynom med flera variabler av flera polynom

Välj en tillåten ordning av monom. Vi vill utföra en division av ett polynom f med ett flertal polynom ur en mängd P. Ge dessa polynom en ordning så att vi har $p_1, \ldots, p_m$. Associera med varje polynom en mängd S_i som innehåller de termer i f som delas av den ledande termen i p_i. Av de icke-tomma mängder S som bildas börja med den som har lägst index. Välj termen i S_i av högst grad och ställ upp beräkningen

$$f_1 = f - \frac{t}{lt(p)}p.$$

Gå nu tillbaka till det tidigare steget och beräkna S_i med avseende på f_1 för alla polynom i P och välj på nytt den icketomma mängd S_i med lägst index för att berökna f_2. Algoritmen avslutar när alla $S_i = \emptyset$.

Nu ser det ut som att vi har allt vi behöver för att avgöra ifall f ingår i I. Om vi utför divisionen som ovan med alla polynom i P så ska f ingå i idealet när vi får rest noll. Det visar sig dock vara svårare än så, vilket vi belyser med ett exempel.

Tag $\mathbb{Z}_2[x_1, x_2, x_3]$ med polynomen

$$f = x_1^3x_2 + x_2,\ p_1 = x_1 + x_3,\ p_2 = x_1^2 + 1$$

och antag $x_1 \succ x_2 \succ x_3$ med lexikografisk ordning. Vi ser att $S_1 = S_2 = \{x_1^3x_2\}$ och börjar med att reducera f med p_1.

$$f_1 = x_1^3x_2 + x_2 - \frac{x_1^3x_2}{x_1}(x_1 + x_3) = x_1^3x_2 + x_2 - x_1^3x_2 - x_1x_2x_3 = x_1x_2x_3 + x_2.$$

Lägg märke till att vi tar koefficienter ur $\mathbb{Z}_2$ så addition och subtraktion ger samma resultat. Vi går vidare. Nu har vi att $S_1 = \{x_1x_2x_3\}$ och $S_2 = \emptyset$. Vi delar på nytt med p_1

$$f_2 = x_1x_2x_3 + x_2 - \frac{x_1x_2x_3}{x_1}(x_1 + x_3) = x_1x_2x_3 + x_2 - x_1x_2x_3 - x_2x_3^2 = x_2x_3^2 + x_2.$$

Vi har nu rest $x_2x_3^2 + x_2$ och algoritmen avslutas då $S_1 = S_2 = \emptyset$

Tag nu motsatt ordning på polynomen och räkna med

$$f = x_1^3x_2 + x_2, p_1 = x_1^2 + 1, p_2 = x_1 + x_3.$$

Vi får nu liksom förut att $S_1 = S_2 = \{x_1^3x_2\}$ och börjar med att reducera f med p_1.

$$f_1 = x_1^3x_2 + x_2 - \frac{x_1^3x_2}{x_1^2}(x_1^2 + 1) = x_1^3x_2 + x_2 - x_1^3x_2 - x_2. = 0$$

Nu är resten 0. Vad innebär det här för vår divisionsalgoritm? Problemet är att vi inte får en unik rest, och särskilt gäller att en nollskild rest inte utesluter att vårt polynom f kan skrivas som en R-kombination av p med andra polynom ur $\mathbb{Z}_2[x_1, \ldots, x_n]$.

Att divisionen inte ger unik rest bereder oss problem: om vi utför divisionen och får rest 0 kan vi sluta oss till att $f \in I$ men om resten inte är 0 betyder det inte nödvändigtvis att så inte är fallet. Konsekvensen av detta är att vi inte enkelt kan avgöra ifall ett polynom f ingår i ett ideal I endast genom att dividera f med de polynom p som genererar I.

Utifrån denna observation närmar vi oss ett av de viktigaste verktygen i detta arbete: Gröbnerbasen.

2.2.5 Gröbnerbaser

Givet ett ideal I genererat av polynomen $P = \{p_1, \ldots, p_m\}, \langle p_1, \ldots, p_m\rangle = I$ vill vi avgöra ifall ett polynom $f \in I$. Om vi reducerar f med polynomen i P och får rest 0 så vet vi att $f \in I$. Detta då en rest 0 implicerar att f är en multipel av något eller flera $p \in P$: alltså att det finns $q_i, q_i \in k[x_1, \ldots, x_n], i = 1, \ldots, n$ så att $f = q_1p_1 + \cdots + q_mp_m$. Tyvärr visar det sig att reduktionen är beroende av vilken ordning vi väljer p_i och ett resultat där $r \neq 0$ inte nödvändigtvis betyder att f inte tillhör I.

Gröbnerbaser löser det här problemet. En **Gröbnerbas** har egenskapen att ifall vi har ett ideal I och en Gröbnerbas G för I så får vi en *unik* rest när vi reducerar f med $g : g \in G$. Om f är del av I så får vi $p \xrightarrow{g} 0$, och i det fall $f \notin I$ ger samma reduktion en nollskild och unik rest [2].

Definition 2.7 (Gröbnerbas [2])**.** *Låt $k[x_n, \ldots, x_n]$ vara en polynomring och fixera en monomordning. Om I är ett ideal i $k[x_n, \ldots, x_n]$ så definierar vi $l(I)$ som idealet genererat av de ledande monomen av elementen i*

$$l(I) = \langle lm(f) : f \in I\rangle.$$

*En ändlig mängd $G = \{g_1, \ldots, g_m\} \subseteq I$ kallas för en **Gröbnerbas** för I om*

$$\langle lm(g_1), \ldots, lm(g_m)\rangle = l(I).$$

Särskilt kallar vi $l(I)$ för **initialidealet** av I.

Exempel 2.1. *Betrakta idealet* $I = \langle x^2, xy + y^2 \rangle$ *i* $\mathbb{Z}_2[x, y]$*. Generatorerna har ledande monom* x^2 *respekitve* xy*. Vi kan se att* y^3 *ligger i idealet, för* $y^3 = (x+y)(xy+y^2)+y\cdot x^2$*. Men* y^3 *har ledande monom* y^3 *som inte genereras av* x^2 *och* xy*. Det räcker alltså inte att ta ledande monom av generatorerna för att få ledande monom för alla element i idealet. Man kan se Gröbnerbaser som ett sätt att skaffa sig ett generatorsystem som är tillräckligt stort för att dess ledande monom ska generera alla ledande monom för element i idealet.*

2.2.6 Buchbergers Algoritm

Nu återstår endast ett problem: givet ett ideal hur kan vi skapa en Gröbnerbas? För detta problem finns det tacksamt nog en algoritm som givet en mängd genererande polynom för ett ideal räknar fram en Gröbnerbas. Det första steget av att demonstrera denna algoritm är att definiera **S-polynom**.

Definition 2.8 (S-polynom)**.** *Givet två polynom* p_i *och* p_j *definierar vi S-polynomet* $S_{i,j}$ *som*

$$S_{i,j} = \frac{lcm(lt(p_i), lt(p_j)}{lt(p_i)} p_i - \frac{lcm(lt(p_i), lt(p_j)}{lt(p_j)} p_j$$

där $lcm(a, b)$ *syftar på den minsta gemensamma multipeln av* a *och* b

Då S-polynomen är en R-kombination av p_i och p_j så befinner de sig i idealet som genereras av p_i, p_j. Vi är nu redo att beskriva själva algoritmen.

Buchbergers Algoritm

Fixera en monomordning och börja med en ett polynomideal I givet av en genererande mängd polynom $G = \{p_1, \ldots, p_n\}$. låt L vara en mängd av oordnade talpar från 1 till n som inte innehåller par med samma tal. L är då i utgångsläget

$$L = \{\{1, 2\}, \ldots, \{1, n\}, \{2, 3\}, \ldots, \{2, n\}, \{3, 4\}, \ldots, \{n - 1, n\}\}.$$

Välj ett godtyckligt element $\{i, j\}$ i L och avlägsna det från mängden. Beräkna det associerade S-polynomet och låt $r_{i,j}$ var resten när $S_{i,j}$ reduceras med polynom ur G i godtycklig ordning. Om $r_{i,j} = 0$ går vi vidare till nästa talpar ur L. Annars, ifall G innehåller m element låt $p_{m+1} = r_{i,j}$ och lägg till elementen $\{1, m + 1\}, \ldots, \{m, m + 1\}$ till L. Algoritmen avslutas då L är tomt.

Vi kommer inte bevisa korrektheten av algoritmen i detta arbete utan hänvisar till [2].

2.2.7 Några satser om Gröbnerbaser

Definition 2.9 (Standardmonom)**.** ***Standardmonomen*** *till ett ideal I är de monom som inte finns i initialidealet $l(I)$.*

Definition 2.10 (Reducerad Gröbnerbas)**.** *En* ***reducerad Gröbnerbas*** *G av ett ideal I är en Gröbnerbas med egenskaperna att för varje polynom $g \in G$ så gäller att det är moniskt och att det har ett unikt ledande monom i G.*

En reducerad Gröbnerbas innehåller alltså endast så många polynom som behövs för att generera intitialidealet till I.

Sats 2.4. *Låt I vara ett ideal i $k[x_1, \ldots, x_n]$. $1 \in I \Leftrightarrow 1 \in G(I)$ där $G(I)$ är en reducerad Gröbnerbas till I.*

Sats 2.5. *Låt $I = \langle f_1, \ldots, f_m, x_1^2 + x_1, \ldots, x_n^2 + x_n \rangle \subseteq \mathbb{Z}_2[x_1, \ldots, x_n]$. Då är $|V(I)|$ lika med antalet monom utanför initialidealet till I, med avseende på någon monomordning,det vill säga antalet standardmonom för en Gröbnerbas till I.*

Denna sats är en specialisering av följande sats:

Sats 2.6. *Låt $I = \langle f_1, \ldots, f_m \rangle$ vara ett radikalt nolldimensionellt ideal. Då är $|V(I)|$ lika med antalet monom utanför initialidealet till I.*

Bevis. Från Cox [2] så har vi att i en algebraiskt sluten kropp så gäller för nolldimensionella radikala ideal I att antalet punkter i $V(I)$ motsvarar dimensionen av kvotringen $\bar{k}[x_1, \ldots, x_n]/I$. Cox uttrycker detta över de komplexa talen men använder just egenskapen att $\mathbb{C}$ är en algebraiskt sluten kropp och kan modifieras för att gälla alla sådana kroppar. Vidare i [2] så gäller att vektorrummet över denna kvotring är isomorf till spannet av standardmonomen till I. Basen till detta span, vilket är just standardmonomen, måste då alltså vara av samma storlek som $V(I)$. □

I detta arbete kommer vi tack vare sats **2.2** inte behöva gå till den algebraiska tillslutningen av $\mathbb{Z}_2[x_1, \ldots, x_n]$ och kan använda satsen direkt på ideal som genereras av kroppspolynomen i polynomringen.

2.3 Böjda funktioner

Nu ska vi betrakta den typ av funktion utifrån vilken vi kommer beräkna Gröbnerbaser. **Böjda funktioner** är en typ av funktioner på formen

$$P : \mathbb{Z}_2^n \to \mathbb{Z}_2.$$

Böjda funktioner, eller **bentfunktioner** fick detta namn av Rothaus i [3] då de ligger på maximalt avstånd från de linjära funktionerna [4]. De har flera intressanta egenskaper, till exempel att det uppfyller det som kallas *the* **Strict Avalanche Criterion** vilket innebär att en ändring av en bit i ingångsvektorn så ändras funktionsvärdet med sannolikhet 1/2 [4]. En annan egenskap hos böjda funktioner är att de är **obalanserade**, det vill säga att mängden nollställen inte är lika med mängden punkter med funktionsvärden 1 [5]. I resultatdelen kommer detta vara relevant då vi kommer studera storleken på varieteten av ideal genererade av denna typ av funktioner, och storleken på varieteten ges av antalet nollställen för de generande polynomen och deras K-kombinationer i polynomringen.

Först ska vi betrakta funktionen $x_1x_2 + \cdots + x_{n-1}x_n$. Vi kommer ge en motivation till dess konstruktion och visa att det är en böjd funktion.

2.3.1 Definition av böjda funktioner

För definitionerna nedan antag att $v \cdot w,\ v, w \in \mathbb{Z}_2^n$ betyder **skalärprodukt** $v_1w_1 + \cdots + v_nw_n$.

Definition 2.11 (Fourierkoefficient [3])**.** *En* ***Fourierkoefficient*** *av en funktion*

$$P : \mathbb{Z}_2^n \to \mathbb{R}$$

är det tal som ges av formeln

$$c(\lambda) = \frac{1}{2^{\frac{n}{2}}} \sum_{x \in \{0,1\}^n} (-1)^{P(x)+\lambda \cdot x} \quad \textit{för} \quad \lambda \in \mathbb{Z}_2^n.$$

I ord beskrivet är funktionen ovan antalet jämna resultat minus antalet udda resultat av funktionen $P(x) + \lambda \cdot x$. Vi beräknar ett exempel för att förklara lite tydligare:

Exempel 2.2. *Betrakta $\mathbb{Z}_2[x_1, x_2]$ och tag funktionen x_1x_2. Vi vill beräkna Fourierkoefficienterna av denna funktion. De λ som ingår i $\mathbb{Z}_2^2$ är*

$$\lambda = \{(0,0), (0,1), (1,0), (1,1)\}.$$

Låt $\lambda_1 = (0,0)$. Fourierkoefficienten för λ_1 blir då

$$c(\lambda_1) = \frac{1}{2} \sum_{x \in \{0,1\}^2} (-1)^{P(x)+\lambda \cdot x} =$$

$$= \frac{1}{2}((-1)^{0 \cdot 0+(0,0)\cdot(0,0)} + (-1)^{0 \cdot 1+(0,0)\cdot(0,1)} +$$
$$+(-1)^{1 \cdot 0+(0,0)\cdot(1,0)} + (-1)^{1 \cdot 1+(0,0)\cdot(1,1)}) =$$

$$= \frac{1}{2}((-1)^0 + (-1)^0 + (-1)^0 + (-1)^1) = 1.$$

Om vi fortsätter beräkna $\lambda_2 = (0,1), \lambda_3 = (1,0)$ *och* $\lambda_4 = (1,1)$ *får vi*

$$c(\lambda_1) = 1$$
$$c(\lambda_2) = 1$$
$$c(\lambda_3) = 1$$
$$c(\lambda_4) = -1.$$

Definition 2.12 (Böjda funktioner [3])**.** *En* ***böjd funktion****, eller en* ***bent-funktion*** *är en funktion*

$$P : \mathbb{Z}_2^n \to \mathbb{Z}_2$$

med egenskapen att dess ***Fourierkoefficienter*** *alla är lika med* ± 1*:*

$$c(\lambda) = \pm 1, \quad \forall \lambda \in \mathbb{Z}_2^n.$$

Om vi tittar på exemplet ovan kan vi se att x_1x_2 är en böjd funktion då alla fourierkoeffiecienter är lika med ± 1.

Följdsats 2.6.1. *En böjd funktion existerar endast i jämna dimensioner* $n = 2m$ *där* m *är ett heltal.*

Bevis. Vi ser att n måste vara jämnt då $2^{n/2}c(\lambda)$ är ett heltal [3]. □

2.3.2 Böjda funktioner på formen $x_1x_2 + \cdots + x_{n-1}x_n$.

Vi har nu fått ett exempel på en böjd funktion, nämligen $f = x_1x_2$. Som vi ser så påminner den om den böjda funktionen vi identifierade i vår frågeställning: $x_1x_2 + \cdots + x_{n-1}x_n$. Kan vi utifrån detta exempel vi räknat fram nå fram till en sådan böjd funktion i godtycklig jämn dimension? Neumann [4] ger en sats som står oss bi:

Sats 2.7. *Låt $f : W \to \mathbb{Z}_2$ och $g : U \to \mathbb{Z}_2$, då är $f + g : W \oplus U \to \mathbb{Z}_2$ böjd om och endast om f och g är böjda [4].*

För att utnyttja den här satsen tittar vi närmre på polynomringen $\mathbb{Z}_2[x_1, \ldots, x_n]$ som är en **algebra** över en kropp, det vill säga att det är ett vektorrum med en en multiplikativ operation. Detta ger oss möjlighet att använda satsen direkt på polynomringar.

Tag då vår funktion $x_1x_2 : \mathbb{Z}_2[x_1, x_2] \to \mathbb{Z}_2$ tillsammans med samma funktion $x_3x_4 : \mathbb{Z}_2[x_3, x_4] \to \mathbb{Z}_2$. Direktsumman av polynomringarna blir då $\mathbb{Z}_2[x_1, x_2, x_3, x_4]$ och funktionen

$$x_1x_2 + x_3x_4 : \mathbb{Z}_2[x_1, x_2, x_3, x_4] \to \mathbb{Z}_2.$$

Enligt satsen ovan är detta en böjd funktion, och vi ser även hur vi enkelt kan konstruera den böjda funktionen $x_1x_2 + \cdots + x_{n-1}x_n$ i godtycklig jämn dimension n.

3 Experiment

3.1 Beräkning av Gröbnerbas för den böjda funktionen $x_1x_2 + \cdots + x_{n-1}x_n$

Experimentdelen av detta arbete går ut på att med hjälp av ett datorprogram beräkna Gröbnerbasen till idealet I_n genererat av den böjda funktionen $x_1x_2 + \cdots + x_{n-1}x_n$ och tillhörande kroppspolynom $x_1^2 + x_1, \ldots, x_n^2 + x_n$. För beräkning används Macaulay2 [6].

Macaulay2 skriver med Buchbergers algoritm ut en Gröbnerbas för det angivna idealet utifrån Buchbergers algoritm. Vi benämner Gröbnerbasen associerad med ett visst ideal I_n

$$\text{Gröbnerbas}(I_n) = GB_n.$$

3.1.1 Storleken på Gröbnerbasen

För funktioner på denna form beräknades Gröbnerbasens storlek för $n = \{2, 4, 6, 8, 10, 12, 14, 16\}$.

n	$\lvert GB\rvert$
2	3
4	7
6	13
8	23
10	41
12	75
14	141
16	271

3.1.2 Polynom i Gröbnerbasen

Polynomen i Gröbnerbaserna för $n = 2, 4, 6, 8$ finns redovisade i appendix.

4 Resultat

Nu när vi har experimenterat med Gröbnerbaser av den böjda funktionen i flera dimensioner vill vi försöka se om vi kan beskriva resultaten mer formellt. Vi ser närmre på de polynom som utgör Gröbnerbasen för den böjda funktionen i dimension n och försöker finna och beskriva ett mönster i dess konstruktion. Vi vill sen visa att om vi väljer polynom efter det mönster vi observerat så utgör de en Gröbnerbas. För detta kommer vi behöva en del resultat:

1. vi vill visa att alla polynom konstruerade efter detta mönster ingår i idealet I_n genererat av den böjda funktionen och tillhörande kroppspolynom;
2. vi ska också visa att antalet monom i polynomringen $\mathbb{Z}_2[x_1, \ldots, x_n]$ som **inte** delas av de ledande monomen i Gröbnerbasen är lika många som storleken på varieteten av idealet I_n och;
3. för detta behöver vi veta storleken på varieteten för idealet I_n.

4.1 Beräkning av $\lvert V(I_n)\rvert$

Nu betraktar vi $x_1x_2 + \cdots + x_{n-1}x_n$ och gör en ansats att beräkna varieteten av ett ideal genererat av denna i godtycklig jämn dimension n. Vi börjar med att göra ett påstående om att storleken på varieten i dimension n beror på storleken av varieteten i dimension $n - 2$.

Sats 4.1. *Låt* $I_n = \langle x_1x_2+\cdots+x_{n-1}x_n, x_1^2+x_1, \ldots, x_n^2+x_n\rangle \subseteq \mathbb{Z}_2[x_1, \ldots, x_n]$ *vara ett ideal. Antag att* n *är jämnt och* $n \geq 4$. *Beteckna* $v_n = |V(I_n)|$. *Då är storleken på varieteten lika med*

$$2 \cdot v_{n-2} + 2^{n-2}.$$

Bevis. Från **2.2** vet vi att varieteten är en delmängd av $\mathbb{Z}_2^n$ och vi behöver inte gå till den algebraiska tillslutningen.

Vi visar satsen genom ett induktionsbevis. Beteckna funktionen $x_1x_2 + \ldots + x_{n-1}x_n$ som p_n. Låt $A_n = \{a_1, \ldots a_m\}$ vara mängden tolkningar i varieteten av $I_n = \langle x_1x_2 + \cdots + x_{n-1}x_n, x_1^2 + x_1, \ldots, x_n^2 + x_n\rangle \subseteq \mathbb{Z}_2[x_1, \ldots, x_n]$. Ta som induktionsbas fallet där $n = 2$. Vi betraktar då varieteten för $I_2 = \langle x_1x_2, x_1^2 + x_1, x_2^2 + x_2\rangle$ i dimension 2. . Det innebär då att $f_i(a_j) = 0$ för $f_i \in I_2$ och $a_j \in A_2$. Storleken på A_2 är detsamma som storleken på varieteten och vi betecknar den v_2. Vi vill nu finna alla $a_j \in A_2$. Det första vi kan konstatera är att alla funktioner $x_k^2 + x_k = 0$ (sats **2.2**). Vi behöver alltså bara ta $p_2 = x_1x_2$ i beaktning. Vi beräknar funktionsvärdet av alla möjliga tolkningar i $\mathbb{Z}_2^2$:

$$\begin{aligned} p_2(0,0) &= 0 \\ p_2(0,1) &= 0 \\ p_2(1,0) &= 0 \\ p_2(1,1) &= 1. \end{aligned}$$

Vi ser att $A_2 = \{(0,0),(0,1),(1,0)\}$ och då är $v_2 = 3$. Nu vill visa att $v_4 = 2 \cdot v_2 + 2^2$. Vi beräknar p_4 för de 2^4 möjliga tolkningarna av $\mathbb{Z}_2^4$:

$$\begin{aligned} &p_4(0,0,0,0) = 0, \quad p_4(0,0,0,1) = 0, \quad p_4(0,0,1,0) = 0, \quad p_4(0,0,1,1) = 1 \\ &p_4(0,1,0,0) = 0, \quad p_4(0,1,0,1) = 0, \quad p_4(0,1,1,0) = 0, \quad p_4(0,1,1,1) = 1 \\ &p_4(1,0,0,0) = 0, \quad p_4(1,0,0,1) = 0, \quad p_4(1,0,1,0) = 0, \quad p_4(1,0,1,1) = 1 \\ &p_4(1,1,0,0) = 1, \quad p_4(1,1,0,1) = 1, \quad p_4(1,1,1,0) = 1, \quad p_4(1,1,1,1) = 0. \end{aligned}$$

Vi har $|V(I_4)| = 10$ vilket är exakt $2 \cdot v_2 + 2^2 = 2 \cdot 3 + 4$. Satsen gäller alltså i basfallet.

Vi vill nu se om det gäller för godtyckligt jämnt n. Tag $a_i = (\alpha_1, \ldots, \alpha_n)$. Det finns då två fall: det ena då $p_{n-2}(\alpha_1, \ldots, \alpha_{n-2}) = 0$ och det andra då $p_{n-2}(\alpha_1, \ldots, \alpha_{n-2}) = 1$. I det båda fallen måste vi ha att tolkningen av

$$p_n(\alpha_1, \ldots, \alpha_n) = p_{n-2}(\alpha_1, \ldots, \alpha_{n-2}) + x_{n-1}x_n = 0$$

för att a_i ska ligga i A_n. I det första fallet är detta sant exakt när tolkningen av $x_{n-1}x_n = 0$. Om vi utnyttjar resultatet ovan då vi beräknade p_2 så ser vi att det finns tre möjliga tolkningar av $x_{n-1}x_n$ som ger detta resultat. Det betyder att för varje $a_j \in A_{n-2}$ existerar tre tolkningar i A_n som ger att $p_n(\alpha_1, \ldots, \alpha_n) = p_{n-2}(\alpha_1, \ldots, \alpha_{n-2}) + x_{n-1}x_n = 0$. Vi har då att A_n innehåller $3 \cdot v_{n-2}$ tolkningar av det här slaget.

I det andra fallet har vi alla tolkingar som inte ligger i A_{n-2}. Det finns totalt 2^{n-2} tolkingar i $\mathbb{Z}_2^{n-2}$ och därför har vi $2^{n-2} - v_{n-2}$ tolkingar så att $p_{n-2} = 1$. För varje sådan tolkning så gäller att $p_{n-2}(\alpha_1, \ldots, \alpha_{n-2}) + x_{n-1}x_n = 0$ omm $x_{n-1}x_n = 1$. Det finns endast en sådan tolking av $x_{n-1}x_n$ vilket ger att för varje tolking som av $p_{n-2}(\alpha_1, \ldots, a_{n-2})$ som inte ligger i A_{n-2} så finns en tolkning i A_n så att $p_n(a_1, \ldots, \alpha_n) = 0$. Vi får ett tillskott av $2^{n-2} - v_{n-2}$ tolkningar i $\mathbb{Z}_2^n$ som ger $p_n(\alpha_1, \ldots, \alpha_n) = 0$. Vi har nu totalt

$$3 \cdot v_{n-2} + 2^{n-2} - v_{n-2} = 2 \cdot v_{n-2} + 2^{n-2}$$

tolkingar i A_n vilket var vårt påstående. □

Nu vill vi försöka hitta ett explicit uttryck för storleken på varieteten av $I_n = \langle x_1x_2 + \cdots + x_{n-1}x_n, x_1^2 + x_1, \ldots, x_n^2 + x_n \rangle \subseteq \mathbb{Z}_2[x_1, \ldots, x_n]$ för godtyckligt jämnt n. Vi kan utnyttja den rekursiva strukturen ovan för att hitta en sådan formel. Vi betraktar storleken på varieteten för några n.

n	$\lvert V(I_n)\rvert$		
2	3		
4	$2 \cdot 3 + 2^2$		
6	$2 \cdot (2 \cdot 3 + 2^2) + 2^4$	$=$	$2^2 \cdot 3 + 2^3 + 2^4$
8	$2 \cdot (2^2 \cdot 3 + 2^3 + 2^4) + 2^6$	$=$	$2^3 \cdot 3 + 2^4 + 2^5 + 2^6$
10	$2 \cdot (2^3 \cdot 3 + 2^4 + 2^5 + 2^6) + 2^8$	$=$	$2^4 \cdot 3 + 2^5 + 2^6 + 2^7 + 2^8$
12	$2 \cdot (2^4 \cdot 3 + 2^5 + 2^6 + 2^7 + 2^8) + 2^{10}$	$=$	$2^5 \cdot 3 + 2^6 + 2^7 + 2^8 + 2^9 + 2^{10}$

Här framträder ett mönster. Storleken på varieteten verkar kunna uttryckas som en serie. Vi kan skriva om mönstret på följande sätt:

$$\begin{aligned} 3 \cdot 2^{\frac{n}{2}-1} + 2^{\frac{n}{2}} + \cdots + 2^{n-2} = \\ (2+1) \cdot 2^{\frac{n}{2}-1} + (2-1) \cdot (2^{\frac{n}{2}} + \cdots + 2^{n-2}) = \\ 2^{\frac{n}{2}} + 2^{\frac{n}{2}-1} + (2^{\frac{n}{2}+1} + \cdots + 2^{n-1}) - (2^{\frac{n}{2}} + \cdots + 2^{n-2}) = \\ 2^{\frac{n}{2}} + 2^{\frac{n}{2}-1} + 2^{n-1} - 2^{\frac{n}{2}} = 2^{n-1} + 2^{\frac{n}{2}-1} \end{aligned}$$

och formulerar det i en sats:

Sats 4.2. *Låt* $I_n = \langle x_1x_2+\cdots+x_{n-1}x_n, x_1^2+x_1, \ldots, x_n^2+x_n\rangle \subseteq \mathbb{Z}_2[x_1, \ldots, x_n]$ *där* n *är jämnt vara ett ideal. Då gäller att*

$$|V(I_n)| = 2^{n-1} + 2^{\frac{n}{2}-1}.$$

Bevis. Vi använder åter igen ett induktionsbevis som bygger på satsen ovan. Vi ser att i fallet för 2 dimensioner så gäller att

$$2^1 + 2^0 = 3$$

vilket är exakt storleken på varieteten beräknad ovan. Vi ser på dimension n och kontrollerar att storleken på varieteten ges av formeln genom att anta att det gäller för $n-2$. Vi har då att varieteten v_{n-2} för $n-2$ är

$$2^{n-3} + 2^{\frac{n-2}{2}-1}.$$

Från tidigare sats gäller att varieteten v_n i dimension n ges av

$$2 \cdot v_{n-2} + 2^{n-2}.$$

Vi skriver om det med hjälp av vår formel

$$v_n = 2 \cdot (2^{n-3} + 2^{\frac{n-2}{2}-1}) + 2^{n-2} = 2^{n-2} + 2^{\frac{n-2}{2}} + 2^{n-2} = 2^{n-1} + 2^{\frac{n}{2}-\frac{2}{2}} = 2^{n-1} + 2^{\frac{n}{2}-1}$$

vilket ger det önskade uttrycket.

□

4.2 Formen på Gröbnerbasen för $x_1x_2 + \cdots + x_{n-1}x_n$

Vad kan vi säga om polynomen i Gröbnerbasen GB_n? Uppgiften vi tagit oss an är att utröna ett mönster i basens konstruktion. Vi ska därför betrakta GB_n noggrant för att finna och beskriva ett sådant mönster. En observation kan vi göra direkt när vi betraktar storleken på GB_n i våra experiment. Storleken växer med n och verkar följa ett visst mönster, nämligen att

$$|GB_n| = n + 2^{\frac{n}{2}} - 1.$$

Vi tar med oss denna observation i genomgången av Gröbnerbasens polynom.

4.2.1 Faktorisering av polynomen i Gröbnerbasen

Ett sätt att få tydlighet i strukturen är att faktorisera polynomen i Gröbnerbasen. Vi har som exempel tagit polynomen i grad $n = 6$. Från Buchbergers algoritm vet vi att både vår böjda funktion och kroppspolynomen ingår i basen och betraktar istället de polynomen som tillkommit:

$$x_1x_3x_4 + x_1x_5x_6 + x_3x_4 + x_5x_6 \quad (1)$$
$$x_2x_3x_4 + x_2x_5x_6 + x_3x_4 + x_5x_6 \quad (2)$$
$$x_1x_3x_5x_6 + x_1x_5x_6 + x_3x_5x_6 + x_5x_6 \quad (3)$$
$$x_2x_3x_5x_6 + x_2x_5x_6 + x_3x_5x_6 + x_5x_6 \quad (4)$$
$$x_1x_4x_5x_6 + x_1x_5x_6 + x_4x_5x_6 + x_5x_6 \quad (5)$$
$$x_2x_4x_5x_6 + x_2x_5x_6 + x_4x_5x_6 + x_5x_6. \quad (6)$$

Ordningen av monomen är bestämt av gradordnad omvänd lexikografisk ordning då detta är standard i Macaulay2. Om vi tittar närmre på (1) och (2) så ser vi att det kan skrivas om som

$$(x_1 + 1)(x_3x_4 + x_5x_6)$$
$$(x_2 + 1)(x_3x_4 + x_5x_6).$$

Faktorn vi får ut är från det första paret variabler x_1x_2 från den böjda funktionen och svansen är de övriga paren $x_3x_4 + x_5x_6$. I den monomordning vi utnyttjar så är monomet x_1x_2 det av lägst ordning i den böjda funktionen. Vi går vidare och ser på (3), (4), (5) och (6):

$$(x_1 + 1)(x_3 + 1)(x_5x_6)$$
$$(x_2 + 1)(x_3 + 1)(x_5x_6)$$
$$(x_1 + 1)(x_4 + 1)(x_5x_6)$$
$$(x_2 + 1)(x_4 + 1)(x_5x_6).$$

Mönstret fortsätter här.
Vi har då polynom med faktorerna

$$\begin{array}{ccc} & & (x_1x_2 + x_3x_4 + x_5x_6) \\ & \{(x_2 + 1), (x_1 + 1)\} & (x_3x_4 + x_5x_6) \\ \{(x_4 + 1), (x_3 + 1)\} & \{(x_2 + 1), (x_1 + 1)\} & (x_5x_6) \end{array}$$

där en faktor väljs ur varje kolumn. Vi kan kalla polynomen i den sista kolumnen för **svansen** i faktoriseringen. Om vi ser tillbaka på våra resultat på storleken av Gröbnerbasen så ser vi ett intressant mönster: vi fick då uttrycket

$$|GB_n| = n + 2^{\frac{n}{2}} - 1.$$

Om vi ser närmre på det observerade mönstret så får vi att n ges av kroppspolynomen, i den första raden har vi 1 polynom, i det andra 2, och i den tredje 4. Vi skriver ut mönstret för $n = 6$ och letar efter en koppling.

$$6 + 1 + 2 + 4 = 6 + 2^0 + 2^1 + 2^2 = 6 + 2^3 - 1.$$

Det betraktade mönstret verkar stämma överens med vår observation om Gröbnerbasernas storlek. Vi ser vidare på Gröbnerbasen i $n = 8$. De faktoriserade polynomen där (utöver kroppspolynomen) är:

$$\begin{gathered}
x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8 \\
(x_1 + 1)(x_3x_4 + x_5x_6 + x_7x_8) \\
(x_2 + 1)(x_3x_4 + x_5x_6 + x_7x_8) \\
(x_1 + 1)(x_3 + 1)(x_5x_6 + x_7x_8) \\
\vdots \\
(x_1 + 1)(x_4 + 1)(x_6 + 1)(x_7x_8) \\
(x_2 + 1)(x_4 + 1)(x_6 + 1)(x_7x_8).
\end{gathered}$$

Mönstret upprepar sig. Vi har återigen att $8+1+2+4+8 = 8+2^4-1 = 23$. Vi ser en möjlighet att beskriva detta mönster i godtycklig dimension, och i samma anda visa att en mängd polynom konstruerade efter detta mönster också är en Gröbnerbas för vår böjda funktion.

4.2.2 Struktur av polynomen i Gröbnerbasen, mängden Γ_m

Vi gör en ansats att beskriva mönstret vi observerat mer generellt. Vi inför nu beteckningen Γ_n för en mängd polynom på den form vi kommer beskriva och tar som hypotes att Γ_n utgör en Gröbnerbas för I_n. Vi skriver om den böjda funktionen på följande vis:

$$x_1y_1 + x_2y_2 + \cdots + x_{m-1}y_{m-1} + x_my_m \in \mathbb{Z}_2[x_1, \ldots, x_m, y_1, \ldots, y_m],$$

där $m = \frac{n}{2}$. Beteckningen är inspirerad av Rothaus formulering i [3].

Vi har i första fallet att svansen är lika med den böjda funktionen själv och polynomet ser likadant ut i faktoriserad form. Nästa fall är när svansen är lika med $x_2y_2+\ldots+x_{m-1}y_{m-1}+x_my_m$. Vi har då två polynom i Gröbnerbasen med den här svansen, nämligen

$$(x_1+1)(x_2y_2+\cdots+x_{m-1}y_{m-1}+x_my_m)$$

och

$$(y_1+1)(x_2y_2+\cdots+x_{m-1}y_{m-1}+x_my_m).$$

Vi följer mönstret och ger en generell definition av Γ_m.

Definition 4.1. *Mängden Γ_m i $\mathbb{Z}_2[x_1,\ldots,x_m,y_1,\ldots,y_m]$ är alla polynom på formen*

$$(z_1+1)\cdots(z_{k-1}+1)(x_ky_k+\cdots+x_my_m)$$

för $k=1,\ldots,m$ och där $z_i\in x_i,y_i, 1\leq i\leq m$ tillsammans med kroppspolynomen $x_1^2+x_1,\ldots,x_m^2+x_m,y_1^2+x_1,\ldots,y_m^2+x_m$.

Det finns då $\sum_{j=0}^{m-1}2^j=2^m-1$ polynom på den här formen borträknat kroppspolynomen. Detta ger storleken på Γ_m och leder till följande uttryck:

Sats 4.3. *Storleken på Γ_m för med idealet I_m ges av uttrycket*

$$|\Gamma_m|=2m+2^m-1.$$

Vi ser att $2m$ förklaras av de $2m$ kroppspolynomen som ingår i idealet I_m. De resterande 2^m-1 polynom ges en förklaras av konstruktionen av Γ_m.

4.2.3 De ledande monomen i Γ_m

För varje polynom i Γ_m ser vi närmre på de ledande monomen. Längre fram kommer vår förståelse av dessa leda oss mot ett viktigt resultat om monomen utanför Γ_m och därför tar vi tid till att klassificera dem här. För en fullständig redogörelse av de ledande monomen för $m=2,3,4$ se appendix.

Hur de ledande monomen ser ut följer direkt från faktorisering vi gjorde ovan. För $m=1$ får vi de ledande monomen:

$$x_1^2,\ y_1^2,\ x_1y_1.$$

För $m=2$ har vi de ledande monomen från $m=1$ och även

$$x_2^2,\ y_2^2,\ x_1x_2y_2,\ y_1x_2y_2.$$

Vi lägger alltså till två andragradspolynom $x_2^2,\ y_2^2$ och ett tredjegradspolynom för varje variabel i $m = 1$. Detta tredjegradspolynom beror på svansen i faktoriseringen ovan. Allmänt är de ledande polynomen i Γ_m på följande form:

$$\begin{array}{ll} x_1^2 & x_1y_1 \\ y_1^2 & \\ \vdots & \\ x_k^2 & \{\mu_k : \mu_k = z_1 \cdots z_{k-1}x_ky_k\} \\ y_k^2 & \\ \vdots & \\ x_m^2 & \{\mu_n : \mu_n = z_1 \cdots z_{m-1}x_my_m\} \\ y_m^2 & \end{array}$$

där μ är monom. Särskilt är monomen μ_k av grad $k+1$ och det finns 2^{k-1} sådana monom.

4.2.4 Bevis av att polynom i Γ_m ingår i idealet

Nu vill att komma närmre vårt önskade resultat: att visa att polynomen beskrivna ovan verkligen utgör en Gröbnerbas för idealet I_m. Ett viktigt kriterium är att polynomen i Γ_m ingår i idealet I_m.

Det första vi visar är att varieteten $V(I_m)$ också ger nollställen till Γ_m.

Lemma 4.4. *För Γ_m är alla polynom $p_k(x) \in \Gamma_m$ lika med noll för alla tolkningar där $x_1y_1+x_2y_2+\cdots+x_{m-1}y_{m-1}+x_my_m = 0$ i $\mathbb{Z}_2[x_1, \ldots, x_m, y_1, \ldots, y_m]$.*

Bevis. Det finns två fall. För tolkningen a så är antingen svansen $(x_ky_k+\cdots+x_my_m) = 0$ och då är $p_k(a) = 0$ omedelbart. Tag då fallet där $(x_ky_k + \cdots + x_my_m) = 1$. Då måste tolkningen av minst ett par variabler $x_iy_i = 1,\ i < k$ och då får vi $(z_i + 1) = 0$ vilket ger $p_k(a) = 0$. □

Detta innebär att Γ_m ingår i idealet av varieteten för I_m, alltså att $\Gamma_m \subseteq I(V(I_m)) = \{f : f(x) = 0\ \forall x \in V(I_m)\}$ [2].

Lemma 4.5. *Idealet $I_m = \langle x_1y_1 + \cdots + x_my_m, x_1^2 + x_1, \ldots, x_m^2 + x_m, y_1^2 + x_1, \ldots, y_m^2 + x_m\rangle$ i polynomringen $\mathbb{Z}_2[x_1, \ldots, x_m, y_1, \ldots, y_m]$ är radikalt.*

Bevis. Beviset av detta lemma kommer att genomföras i tre delar. Vi vill visa att

1. om ett monom $x_1^{a_1} \cdots x_m^{a_m}y_1^{b_1} \cdots y_m^{b_m} \in I_n$ så är även $x_1^{\alpha_1} \cdots x_m^{\alpha_m}y_1^{\beta_1} \cdots y_m^{\beta_m} \in I_m$ där $\alpha_i, \beta_j = 1$ om $a_i, b_j \geq 1$ och $\alpha_i, \beta_j = 0$ om $a_i, b_j = 0$, $1 \leq i, j \leq m$.

2. Att $f^2 \in I_m \Rightarrow f \in I_m$, och sist att

3. $f^s \in I_m \Rightarrow f \in I_m$.

För 1. betraktar vi $x_1^2 \in I_m \Rightarrow x_1 \in I_m$. Vi har då att

$$x_1^2 + (x_1^2 + x_1) = x_1 \in I_m$$

eftersom att I_m är slutet under addition och $x_1^2 + x_1 \in I_m$. Antag nu att $x_1^n \in I_m$. Vi ser då att

$$x_1^n + (x_1^2 + x_1)x_1^{n-2} = x_1^n + x_1^n + x_1^{n-1} = x_1^{n-1} \in I_m$$

då $f \in I_m,\ p \in \mathbb{Z}_2[x_1, \ldots, x_m, y_1, \ldots, y_m] \Rightarrow f \cdot p \in I_m$. Vi kan upprepa denna operation till dess att exponenten är 1. För monom m i flera variabler kan vi tänka oss fallet att $x_1^{a_1} \cdots x_k^t \cdots x_m^{a_m} y_1^{b_1} \cdots y_m^{b_m} \in I_m$ och $t \geq 2$. Tag då

$$x_1^{a_1} \cdots x_k^t \cdots x_n^{a_n} y_1^{b_1} \cdots y_m^{b_m} + (x_k^2 + x_k)x_1^{a_1} \cdots x_k^{t-2} \cdots x_n^{a_n} y_1^{b_1} \cdots y_m^{b_m} = x_1^{a_1} \cdots x_k^{t-1} \cdots x_n^{a_n} y_1^{b_1} \cdots y_m^{b_m}.$$

Enligt samma resonemang som i fallet för en variabel har vi att högerledet ligger i I_m. Vi kan upprepa operationen på alla $a_i, b_j \geq 1$ till vi får $x_1^{\alpha_1} \cdots x_m^{\alpha_m} y_1^{\beta_1} \cdots y_m^{\beta_m} \in I_m$.

För 2. tar vi $f = \mu_1 + \ldots + \mu_l$ där $\mu_k,\ 1 \leq k \leq l$ är monom och antar att $f^2 \in I_m$. Betrakta då

$$f^2 = (\mu_1 + \cdots + \mu_l)(\mu_1 + \cdots + \mu_l) = \mu_1^2 + \cdots + \mu_l^2$$

i $\mathbb{Z}_2[x_1, \ldots, x_m, y_1, \ldots, y_m]$. Från 1. har vi att $\mu_k^2 \in I_m \Rightarrow \mu_k \in I_m$. Operationen beskriven där kan användas på varje monom för sig och ger att

$$\mu_1^2 + \cdots + \mu_l^2 \in I_m \Rightarrow \mu_1 + \cdots + \mu_l \in I_m$$

vilket ger $f^2 \in I_m \Rightarrow f \in I_m$. Vidare från 1. har vi att om $f \in I_m$ så gäller att $f' \in I_m$ där alla monom har variabler av högst grad 1.

Slutligen gäller för 3. att visa att $f^s \in I_m \Rightarrow f \in I_m$. Tag 2. som basfall och som induktionsantagande att $f^{s-1} \in I_m \Rightarrow f \in I_m$. Vi har då att

$$f^s = f^{s-2}f^2 = f^{s-2}(\mu_1^2 + \cdots + \mu_l^2) = \mu_1^2 f^{s-2} + \cdots + \mu_l^2 f^{s-2}$$

$$f^s \in I_m \Rightarrow \mu_1 f^{s-2} + \cdots + \mu_l f^{s-2} = f^{s-1} \in I_m$$

vilket från antagandet ger att $f \in I_m$. Idealet I_m är radikalt. □

Sats 4.6 (Hilberts Nullstellensatz [2])**.** *Låt k vara en algebraiskt sluten kropp. Om $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ är sådana att $f \in I(V(f_1, \ldots, f_s))$ så existerar ett heltal $k \geq 1$ sådant att*

$$f^k \in \langle f_1, \ldots, f_s \rangle.$$

Vi vill nu visa att detta innebär att Γ_n ingår i idealet I_m.

Sats 4.7. *Polynommängden Γ_m ingår i idealet $I_m = \langle x_1y_1 + \cdots + x_my_m, x_1^2 + x_1, \ldots, x_m^2 + x_m, y_1^2 + x_1, \ldots, y_m^2 + x_m \rangle$ i polynomringen $\mathbb{Z}_2[x_1, \ldots, x_m, y_1, \ldots, y_m]$.*

Bevis. Vi utnyttjar sats **2.2** och noterar att

$$V(I) = V(\langle x_1y_1 + \cdots + x_my_m \rangle) \cap V(\langle x_1^2 + x_1, \ldots, x_m^2 + x_m, y_1^2 + x_1, \ldots, y_m^2 + x_m \rangle) = V(\langle x_1y_1 + \cdots + x_my_m \rangle) \cap \mathbb{Z}_2^{2m}$$

vilket innebär att varieteten inte påverkas av att vi går från $\mathbb{Z}_2[x_1, \ldots, x_m, y_1, \ldots, y_m]$ till dess algebraiska slutning $\bar{\mathbb{Z}}_2[x_1, \ldots, x_m, y_1, \ldots, y_m]$.

Från lemma **4.4** har vi att $\Gamma_m \subseteq I(V(I_m))$. Sats **4.6** ger då att för alla polynom ur $\{g_1, \ldots, g_l\} = \Gamma_m$ finns positiva heltal $k_i,\ i = 1, \ldots, l$ sådana att

$$g_1^{k_1}, \ldots, g_l^{k_l} \in I_m.$$

Lemma **4.5** ger då att $g_1, \ldots, g_l$ ingår i idealet vilket visar satsen.

□

4.2.5 Mängden monom utanför Γ_m

Mängden standardmonom till en Gröbnerbas ska ha samma storlek som varieteten (sats **2.5**). Vi vill hitta ett sätt att räkna monomen utanför Γ_m. Särskilt vill vi visa att mängden monom S_m utanför Γ_m är av samma storlek som varieteten $V(I_m)$[ii].

Lemma 4.8. *Låt oss beteckna med S_m standardmonomen till mängden Γ_m i polynomringen $\mathbb{Z}_2[x_1, \ldots, x_m, y_1, \ldots, y_m]$ som tillhör idealet I_m för $m \geq 2$. De monom som inte delas av de ledande monomen i Γ_m finns i tre klasser:*

1. *Alla monom i S_{m-1}.*
2. *$S_{m-1} \cdot x_m$ och $S_{m-1} \cdot y_m$ och till sist:*

[ii] I appendix finns en lista över alla standardmonom associerade till $m = 2, 3, 4$ vilken kan ge en inblick i hur de tre klasserna beskrivna här upptäcktes.

3. *mängden* $S'_{m-1} \cdot x_m y_m$ *där* S'_{m-1} *är alla monom i* S_{m-1} *förutom de av grad* $m-1$ *som har exakt en variabel från varje variabelpar* $x_1y_1, x_2y_2, \ldots x_ky_k, \ldots x_{m-1}y_{m-1}$.

Vi har att mängden S_m *beror på* S_{m-1} *på följande vis:*

$$S_m = S_{m-1} \ \cup \ S_{m-1} \cdot x_m \ \cup \ S_{n-2} \cdot y_m \ \cup \ S'_{m-1} \cdot x_m y_m. \tag{7}$$

Vi får också uttrycket

$$|S_m| = 4 \cdot |S_{m-1}| - 2^{m-1} \tag{8}$$

vilket ger det exakta antalet standardmonom till Γ_m.

Bevis. För en ingående beskrivning av de ledande monomen i Γ_m hänvisas till avsnitt **4.2.3**. Vi visar lemmat genom ett induktionsbevis. I basfallet gäller att Γ_1 innehåller de ledande monomen

$$x_1^2, \ y_1^2, \ x_1y_1.$$

I polynomringen $\mathbb{Z}_2[x_1, y_2]$ har vi då att

$$S_1 = \{1, x_1, y_1\}$$

är standardmonom. Tag nu de ledande monomen i Γ_2 i polynomringen $\mathbb{Z}_2[x_1, y_1, x_2, y_2]$. De är

$$\begin{array}{llll} x_1^2, & y_1^2, & x_2^2, & y_2^2, \\ x_1y_1, & & & \\ x_1x_2y_2, & y_1x_2y_2. & & \end{array}$$

Nu konstruerar vi S_2 enligt reglerna ovan. Genom att ta 1. får vi $S_2 = \{1, x_1, y_1\}$. Vi kan snabbt se att ingen av dessa delas av något ledande monom i Γ_2. Det kan inte heller finnas fler av den här typen då alla ledande monom som ingår i Γ_1 även ingår i Γ_2.

Vi går vidare till klass 2. och får mängden $\{x_2, x_1x_2, y_1x_2, y_2, x_1y_2, y_1y_2\}$. Inte heller något av dessa monom delas av de ledande monomen ovan. Skulle det kunna tillkomma fler monom av den här typen? Det skulle innebära att vi behöver lägga till någon av variablerna x_1, y_1 till monomen i den här mängden, vilket omedelbart gör dem delbara med något ledande monom i Γ_1 och följaktligen i Γ_2.

Då kommer vi sist till klass 3. Genom att multiplicera alla monom i S_2 med x_2y_2 så får vi $\{x_2y_2, x_1x_2y_2, y_1x_2y_2\}$. Nu får vi dock två monom som delas av ett ledande monom ur Γ_2. De råkar vara de fallen där vi har multiplicerat med monom som innehåller en variabel från varje variabelpar x_iy_i för $1 \leq i < m$, nämligen monomen x_1 och y_1. Vi ska alltså ta $S_2 \setminus \{x_1, y_1\} = S_2'$ och multiplicera dessa monom med x_2y_2 för att få fram standardmonomen av klass 3. Vi får $\{x_2y_2\}$ vilket inte delas av något av de ledande monomen i Γ_2. Enligt samma argument som för 1. och 2. så kan det inte heller finnas fler monom som vi skulle kunna multiplicera med x_2y_2 och få ett nytt monom utanför Γ_2.

Insättning i vårt ursprungliga uttryck ger att

$$\begin{aligned} S_4 &= \{1, x_1, y_1\} \cup \{x_2, x_1x_2, y_1x_2\} \cup \{y_2, x_1y_2, y_1y_2\} \cup \{x_2y_2\} \\ &= \{1, x_1, y_1, x_2, y_2, x_1x_2, y_1x_2, x_1y_2, y_1y_2, x_2y_2\}. \end{aligned}$$

Då målet är att visa att dessa är exakt monomen utanför Γ_2 är vi klara med (7). För att visa (8) räcker påståendet

$$4 \cdot |S_1| - 2^{m-1} = 4 \cdot 3 - 2 = 10 = |S_2|.$$

Vi har alltså visat basfallet. Vi antar nu att S_{m-1} är standardmonom till mängden Γ_{m-1} och visar att sambanden (7) och (8) håller då vi betraktar standardmonomen S_m.

För 1. vet vi att alla ledande monom som tillkommer när vi går från Γ_{m-1} till Γ_m innehåller variablerna x_my_m och därför kan dessa inte heller dela några av standardmonomen i S_{m-1}. Detta kommer sig helt enkelt av att inga av monomen i S_{m-1} innehåller några av dessa variabler. Det kan inte heller finns fler monom av den här typen utanför Γ_m då vi fortfarande har kvar alla ledande monom från Γ_{m-1}.

För 2. så gäller samma argument som ovan. Monomen i den här gruppen kan inte heller delas av monom som innehåller både x_m och y_m då de endast beror på en av dessa variabler. Vi kan inte heller hitta fler monom än just de som beskrivs i klass 2 då det skulle ge monom på formen

$$z_1z_2 \cdots x_ky_k \cdots z_m \quad \text{eller} \quad z_1 \cdots z_k^2 \cdots z_m$$

för något $k, 1 \leq k < m$ vilket kommer delas av ett ledande monom i Γ_{m-1} och därför också av något ledande monom av Γ_m.

I det sista fallet 3. så vill vi visa att det finns monom som beror på både x_m och y_m som ändå inte delas av de nya ledande monom i Γ_n. De nya ledande monomen är på formen

$$z_1 \cdots z_{m-1} x_m y_m$$

där $z_i = \{x_i, y_i\}$. Därför måste vi se om det finns några monom på den formen i mängden $S_{n-1} \cdot x_m y_m$. Om vi ser på hur monomen S_{n-1} är konstruerade så inser vi snart att klassen 2. innehåller alla monom på formen $z_1 \dots z_{m-1}$. Det finns 2^{m-1} sådana monom och därför räknar vi bort dem från den tredje klassen. Enligt samma argument som för 2. så finns det inte heller fler monom in den här klassen.

Slutligen kan vi nämna att något monom x_m^l, y_m^l av grad $l \geq 2$ inte kan ingå i S_m då det delas av x_m^2 eller y_m^2.

Vi har nu beroendet

$$S_m = S_{m-1} \ \cup \ S_{m-1} \cdot x_m \ \cup \ S_{n-2} \cdot y_m \ \cup \ S'_{m-1} \cdot x_m y_m.$$

Sist vill vi visa att de tre klasserna är disjunkta för att (8) ska gälla. Det är enkelt att se då klass 2. och 3. utnyttjar variabler som inte finns till hands vid konstruktionen av S_{m-1}. Vi vet också att de 2^{m-1} monom som räknas bort vid konstruktionen av S'_{m-1} finns i S_m och får på så vis uttrycket

$$|S_m| = 4 \cdot |S_{m-1}| - 2^{m-1}$$

som minsta möjliga mängd standardmonom för S_m. Argumentet ovan visar att vi inte förlorar eller missar att lägga till några monom längs vägen och garanterar att det existerar precis så många för varje Γ_m.

□

Om vi ser på det rekursiva uttrycket vi har fått så kan vi göra ett försök att hitta ett explicit uttryck för $|S_m|$. Vi betraktar några av de första mängderna monom utanför Γ_m.

m	$4 \cdot \lvert S_{m-1}\rvert - 2^{m-1}$				$\lvert S_m\rvert$
1					3
2	$4 \cdot 3 - 2^1$	$=$	$2^2 \cdot 3 - 2$	$=$	10
3	$4 \cdot 10 - 2^2$	$=$	$2^3 \cdot 5 - 4$	$=$	36
4	$4 \cdot 36 - 2^3$	$=$	$2^4 \cdot 17 - 8$	$=$	136
5	$4 \cdot 136 - 2^3$	$=$	$2^5 \cdot 33 - 16$	$=$	528.

Vi märker ett mönster, storleken på S_m kan skrivas som uttrycket $2^m(2^{m-1}+1) - 2^{m-1}$. Här dyker ett intressant samband upp: genom lite manipulation får vi

$$2^m(2^{m-1}+1) - 2^{m-1} = 2^{2m-1} + 2^m - 2^{m-1} = 2^{2m-1} + 2^{m-1}$$

vilket ju är uttrycket för storleken på varieteten $V(I_m)$ [iii]. Det visar sig att det här uttrycket även ger antalet monom utanför Γ_m.

Lemma 4.9. *Storleken på mängden monom S_m utanför Γ_m ges av uttrycket*

$$2^{2m-1} + 2^{m-1}.$$

Bevis. Basfallet ges av tabellen ovan. För induktionsantagandet antag $|S_m| = 2^{2m-1} + 2^{m-1}$. Då ska $|S_{m+1}| = 2^{2(m+1)-1} + 2^m = 2^{2m+1} + 2^m$. Från lemma **4.8** gäller då att

$$|S_{m+1}| = 4 \cdot |S_m| - 2^m = 4 \cdot (2^{2m-1} + 2^{m-1}) - 2^m = 2^{2m+1} + 2^{m+1} - 2^m = \\ = 2^{2m+1} + 2^m + 2^m - 2^m = 2^{2m+1} + 2^m$$

vilket visar satsen. När vi nu har utgått från mängden S_1 så får vi ett explicit uttryck för mängden monom utanför Γ_m för $m \geq 2$. □

Uttrycket vi härlett hjälper oss att knyta ihop två väldigt viktiga resultat, nämligen att mängden monom utanför Γ_m är lika stor som mängden nollställen till I_m. Vi ger satsen nedan.

Sats 4.10. *Mängden nollställen $V(I_m)$ till idealet $I_m = \langle x_1y_1 + \cdots + x_my_m, x_1^2 + x_1, \ldots, x_m^2 + x_m, y_1^2 + x_1, \ldots, y_m^2 + x_m \rangle$ är lika många som antalet monom utanför Γ_m i $\mathbb{Z}_2[x_1, \ldots, x_m, y_1, \ldots, y_m]$.*

Bevis. Från sats **4.2** och lemma **4.9** får vi uttrycken

$$|S_m| = 2^{2m-1} + 2^{m-1} = |V(I_m)|.$$

Vi vet då att att mängden monom utanför Γ_m är lika stor som varieteten av I_m. □

4.2.6 Γ_m är en Gröbnerbas för I_m

Vi når nu slutsatsen i arbetet: att polynommängden Γ_m verkligen är en Gröbnerbas för I_m.

Sats 4.11. *Γ_m är en Gröbnerbas till idealet $I_m = \langle x_1y_1 + \cdots + x_my_m, x_1^2 + x_1, \ldots, x_m^2 + x_m, y_1^2 + x_1, \ldots, y_m^2 + x_m \rangle$*

[iii] Kom ihåg att $n = 2m$

Bevis. Definition **2.7** kräver att Γ_m är en ändlig delmängd av I_m samt att $l(\Gamma_m) = l(I_m)$.

För det första villkoret har vi från sats **4.7** att Γ_m ingår i idealet, och sats **4.3** visar att Γ_m är ändligt.

Vi har från sats **4.10** att mängden monom utanför Γ_m motsvarar storleken på $V(I_m)$. Från lemma **4.5** och följdsats **2.2.1** vet vi att I_m är radikalt och nolldimensionellt. Sats **2.6** ger då att standardmonomen till I_m motsvarar storleken på varieteten om vi går till den algebraiska tillslutningen av polynomringen. Enligt samma argument som i sats **2.2** så vet vi att våra påståenden om I_m i $\mathbb{Z}_2[x_1, \ldots, x_m, y_1, \ldots, y_m]$ även gäller i $\bar{\mathbb{Z}}_2[x_1, \ldots, x_m, y_1, \ldots, y_m]$. Då Γ_m ingår i idealet är det givet att inga monom som inte ingår i $l(I_m)$ kan ingå i $l(\Gamma_m)$. När vi sedan har fallet att mängden monom utanför Γ_m är av samma storlek som varieteten så vet vi att dessa monom är just standardmonomen till I_m, och då har vi att de ledande monomen i Γ_m genererar $l(I_m)$. Γ_m uppfyller alltså kraven på att vara en Gröbnerbas. □

5 Slutsats

Vi har alltså lyckats hitta ett recept för att skriva ut en Gröbnerbas till I_m utan att behöva ta till Buchberger's algoritm. Vi har dock inte riktigt lyckats utröna nånting mer om de böjda funktionernas klassificering. En fråga som är värd att ställa är ifall Gröbnerbaser för andra böjda funktioner går att beskriva på liknande sätt som för den böjda funktionen $x_1x_2+\cdots+x_{n-1}x_n$. En sådan undersökning skulle eventuellt kunna leda oss närmre en klassificering. Det vore också intressant att fortsätta titta på Gröbnerbaser generellt när man har ideal genererade av kroppspolynomen i $\mathbb{Z}_2[x_1, \ldots, x_n]$.

Referenser

[1] S. Hodzic, E. Pasalic och Y. Wei, "A general framework for secondary constructions of bent and plateaued functions", *Des. Codes Cryptogr.*, 88. ser., s. 2007–2035, 2020. URL: `https://doi.org/10.1007/s10623-020-00760-9`.

[2] D. Cox, J. Little och D. O'Shea, *Ideals, Varieties, and Algorithms*, 3. utg. Springer, 2007.

[3] O. S. Rothaus, "On Bent Functions", *Journal of Combinatorial Theory*, 1976. URL: `https://www.sciencedirect.com/science/article/pii/0097316576900248`.

[4] T. Neumann, "Bent Functions", Diploma Thesis, University of Kaiserslauten, 2006. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.85.8731.

[5] W. Meier och O. Staffelbach, "Nonlinearity criteria for cryptographic functions", *EUROCRYPT*, 1989. URL: https://www.semanticscholar.org/paper/Nonlinearity-Criteria-for-Cryptographic-Functions-Meier-Staffelbach/50dd61841e03a92b4de46244a27f446c924b887f.

[6] D. Grayson och M. Stillman. (8 nov. 2020). Macaulay2, a software system for research in algebraic geometry, URL: www.math.uiuc.edu/Macaulay2.

6 Appendix

`Appendix i`

Gröbnerbaser $|GB_n|$ från Macaulay2 för $I_n,\ n = 2, 4, 6, 8$

$$\underline{n = 2,\ |GB_2| = 3}$$

$$x_2^2 + x_2,\ x_1^2 + x_{,}\ x_1x_2$$

$$\underline{n = 4,\ |GB_4| = 7}$$

$$x_4^2 + x_4,\ x_3^2 + x_3,\ x_2^2 + x_2,\ x_1^2 + x_1,\ x_1x_2 + x_3x_4,\ x_2x_3x_4 + x_3x_4x_1,\ x_3x_4 + x_3x_4$$

$$\underline{n = 6,\ |GB_6| = 13}$$

$$x_6^2 + x_6,\ x_5^2 + x_5,\ x_4^2 + x_4,\ x_3^2 + x_3,\ x_2^2 + x_2,\ x_1^2 + x_1,\ x_1x_2 + x_3x_4 + x_5x_6$$
$$x_2x_3x_4 + x_2x_5x_6 + x_3x_4 + x_5x_6,\ x_1x_3x_4 + x_1x_5x_6 + x_3x_4 + x_5x_6$$
$$x_2x_4x_5x_6 + x_2x_5x_6 + x_4x_5x_6 + x_5x_6,\ x_1x_4x_5x_6 + x_1x_5x_6 + x_4x_5x_6 + x_5x_6$$
$$x_2x_3x_5x_6 + x_2x_5x_6 + x_3x_5x_6 + x_5x_6,\ x_1x_3x_5x_6 + x_1x_5x_6 + x_3x_5x_6 + x_5x_6$$

$$\underline{n = 8,\ |GB_8| = 23}$$

$$x_8^2 + x_8,\ x_7^2 + x_7,\ x_6^2 + x_6,\ x_5^2 + x_5,\ x_4^2 + x_4,\ x_3^2 + x_3,\ x_2^2 + x_2,\ x_1^2 + x_1$$

$$x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8,\ x_2x_3x_4 + x_2x_5x_6 + x_2x_7x_8 + x_3x_4 + x_5x_6 + x_7x_8$$

$$x_1x_3x_4 + x_1x_5x_6 + x_1x_7x_8 + x_3x_4 + x_5x_6 + x_7x_8$$

$$x_2x_4x_5x_6 + x_2x_4x_7x_8 + x_2x_5x_6 + x_4x_5x_6 + x_2x_7x_8 + x_4x_7x_8 + x_5x_6 + x_7x_8$$

$$x_1x_4x_5x_6 + x_1x_4x_7x_8 + x_1x_5x_6 + x_4x_5x_6 + x_1x_7x_8 + x_4x_7x_8 + x_5x_6 + x_7x_8$$

$$x_2x_3x_5x_6 + x_2x_3x_7x_8 + x_2x_5x_6 + x_3x_5x_6 + x_2x_7x_8 + x_3x_7x_8 + x_5x_6 + x_7x_8$$

$$x_1x_3x_5x_6 + x_1x_3x_7x_8 + x_1x_5x_6 + x_3x_5x_6 + x_1x_7x_8 + x_3x_7x_8 + x_5x_6 + x_7x_8$$

$$x_2x_4x_6x_7x_8 + x_2x_4x_7x_8 + x_2x_6x_7x_8 + x_4x_6x_7x_8 + x_2x_7x_8 + x_4x_7x_8 + x_6x_7x_8 + x_7x_8$$

$$x_1x_4x_6x_7x_8 + x_1x_4x_7x_8 + x_1x_6x_7x_8 + x_4x_6x_7x_8 + x_1x_7x_8 + x_4x_7x_8 + x_6x_7x_8 + x_7x_8$$

$$x_2x_3x_6x_7x_8 + x_2x_3x_7x_8 + x_2x_6x_7x_8 + x_3x_6x_7x_8 + x_2x_7x_8 + x_3x_7x_8 + x_6x_7x_8 + x_7x_8$$

$$x_1x_3x_6x_7x_8 + x_1x_3x_7x_8 + x_1x_6x_7x_8 + x_3x_6x_7x_8 + x_1x_7x_8 + x_3x_7x_8 + x_6x_7x_8 + x_7x_8$$

$$x_2x_4x_5x_7x_8 + x_2x_4x_7x_8 + x_2x_5x_7x_8 + x_4x_5x_7x_8 + x_2x_7x_8 + x_4x_7x_8 + x_5x_7x_8 + x_7x_8$$

$$x_1x_4x_5x_7x_8 + x_1x_4x_7x_8 + x_1x_5x_7x_8 + x_4x_5x_7x_8 + x_1x_7x_8 + x_4x_7x_8 + x_5x_7x_8 + x_7x_8$$

$$x_2x_3x_5x_7x_8 + x_2x_3x_7x_8 + x_2x_5x_7x_8 + x_3x_5x_7x_8 + x_2x_7x_8 + x_3x_7x_8 + x_5x_7x_8 + x_7x_8$$

$$x_1x_3x_5x_7x_8 + x_1x_3x_7x_8 + x_1x_5x_7x_8 + x_3x_5x_7x_8 + x_1x_7x_8 + x_3x_7x_8 + x_5x_7x_8 + x_7x_8$$

Appendix ii

Ledande monom $n = 4$ ur Gröbnerbasen

x_1^2	x_2^2	x_3^2	x_4^2
x_1x_2			
$x_1x_3x_4$	$x_2x_3x_4$		

Monom i $\mathbb{Z}_2[x_1, \ldots, x_4]$ som inte delas av ledande monom i Gröbnerbasen

Grad 0	1	2	3
1	x_1	x_1x_3	
	x_2	x_1x_4	
	x_3	x_2x_3	
	x_4	x_2x_4	
		x_3x_4	
1	4	5	0

Totalt: 10

$$|V(I_4)| = 2^{4-1} + 2^{\frac{4}{2}-1} = 2^3 + 2^1 = 10$$

Ledande monom $n = 6$ ur Gröbnerbasen

x_1^2	x_2^2	x_3^2	x_4^2
x_5^2	x_6^2		
x_1x_2			
$x_1x_3x_4$	$x_2x_3x_4$		
$x_1x_3x_5x_6$	$x_2x_3x_5x_6$	$x_1x_4x_5x_6$	$x_2x_4x_5x_6$

Monom i $\mathbb{Z}_2[x_1, \ldots, x_6]$ som inte delas av ledande monom i Gröbnerbasen

Grad 0	1	2	3	4
1	x_1	x_1x_3	$x_1x_3x_5$	$x_3x_4x_5x_6$
	x_2	x_1x_4	$x_1x_3x_6$	
	x_3	x_1x_5	$x_1x_4x_5$	
	x_4	x_1x_6	$x_1x_4x_6$	
	x_5	x_2x_3	$x_1x_5x_6$	
	x_6	x_2x_4	$x_2x_3x_5$	
		x_2x_5	$x_2x_3x_6$	
		x_2x_6	$x_2x_4x_5$	
		x_3x_4	$x_2x_4x_6$	
		x_3x_5	$x_2x_5x_6$	
		x_3x_6	$x_3x_4x_5$	
		x_4x_5	$x_3x_4x_6$	
		x_4x_6	$x_3x_5x_6$	
		x_5x_6	$x_4x_5x_6$	
1	6	14	14	1

Totalt: 36

$$|V(I_6)| = 2^{6-1} + 2^{\frac{6}{2}-1} = 2^5 + 2^2 = 36$$

Ledande monom $n = 8$ ur Gröbnerbasen

x_1^2	x_2^2	x_3^2	x_4^2
x_5^2	x_6^2	x_7^2	x_8^2
x_1x_2			
$x_1x_3x_4$	$x_2x_3x_4$		
$x_1x_3x_5x_6$	$x_1x_4x_5x_6$	$x_2x_3x_5x_6$	$x_2x_4x_5x_6$
$x_1x_3x_5x_7x_8$	$x_1x_3x_6x_7x_8$	$x_1x_4x_5x_7x_8$	$x_1x_4x_6x_7x_8$
$x_2x_3x_5x_7x_8$	$x_2x_3x_6x_7x_8$	$x_2x_4x_5x_7x_8$	$x_2x_4x_6x_7x_8$

Monom i $\mathbb{Z}_2[x_1, \ldots, x_8]$ som inte delas av ledande monom i Gröbnerbasen
Totalt: 136

$$|V(I_8)| = 2^{8-1} + 2^{\frac{8}{2}-1} = 2^7 + 2^3 = 136$$

Grad				
0	1			
1	x_1	x_2	x_3	x_4
	x_5	x_6	x_7	x_8
2	x_1x_3	x_1x_4	x_1x_5	x_1x_6
	x_1x_7	x_1x_8		
	x_2x_3	x_2x_4	x_2x_5	x_2x_6
	x_2x_7	x_2x_8		
	x_3x_4	x_3x_5	x_3x_6	x_3x_7
	x_3x_8			
	x_4x_5	x_4x_6	x_4x_7	x_4x_8
	x_5x_6	x_5x_7	x_5x_8	
	x_6x_7	x_6x_8		
	x_7x_8			Tot: 27
3	$x_1x_3x_5$	$x_1x_3x_6$	$x_1x_3x_7$	$x_1x_3x_8$
	$x_1x_4x_5$	$x_1x_4x_6$	$x_1x_4x_7$	$x_1x_4x_8$
	$x_1x_5x_6$	$x_1x_5x_7$	$x_1x_5x_8$	
	$x_1x_6x_7$	$x_1x_6x_8$		
	$x_1x_7x_8$			
	$x_2x_3x_5$	$x_2x_3x_6$	$x_2x_3x_7$	$x_2x_3x_8$
	$x_2x_4x_5$	$x_2x_4x_6$	$x_2x_4x_7$	$x_2x_4x_8$
	$x_2x_5x_6$	$x_2x_5x_7$	$x_2x_5x_8$	
	$x_2x_6x_7$	$x_2x_6x_8$		
	$x_2x_7x_8$			
	$x_3x_4x_5$	$x_3x_4x_6$	$x_3x_4x_7$	$x_3x_4x_8$
	$x_3x_5x_6$	$x_3x_5x_7$	$x_3x_5x_8$	
	$x_3x_6x_7$	$x_3x_6x_8$		
	$x_3x_7x_8$			
	$x_4x_5x_6$	$x_4x_5x_7$	$x_4x_5x_8$	
	$x_4x_6x_7$	$x_4x_6x_8$		
	$x_4x_7x_8$			
	$x_5x_6x_7$	$x_5x_6x_8$		
	$x_5x_7x_8$			
	$x_6x_7x_8$			Tot: 48

Grad				
4	$x_1x_3x_5x_7$	$x_1x_3x_5x_8$	$x_1x_3x_6x_7$	$x_1x_3x_6x_8$
	$x_1x_3x_7x_8$			
	$x_1x_4x_5x_7$	$x_1x_4x_5x_8$	$x_1x_4x_6x_7$	$x_1x_4x_6x_8$
	$x_1x_4x_7x_8$			
	$x_1x_5x_6x_7$	$x_1x_5x_6x_8$	$x_1x_5x_7x_8$	
	$x_1x_6x_7x_8$			
	$x_2x_3x_5x_7$	$x_2x_3x_5x_8$	$x_2x_3x_6x_7$	$x_2x_3x_6x_8$
	$x_2x_3x_7x_8$			
	$x_2x_4x_5x_7$	$x_2x_4x_5x_8$	$x_2x_4x_6x_7$	$x_2x_4x_6x_8$
	$x_2x_4x_7x_8$			
	$x_2x_5x_6x_7$	$x_2x_5x_6x_8$	$x_2x_5x_7x_8$	
	$x_2x_6x_7x_8$			
	$x_3x_4x_5x_6$	$x_3x_4x_5x_7$	$x_3x_4x_5x_8$	
	$x_3x_4x_6x_7$	$x_3x_4x_6x_8$		
	$x_3x_4x_7x_8$			
	$x_3x_5x_6x_7$	$x_3x_5x_6x_8$	$x_3x_5x_7x_8$	
	$x_3x_6x_7x_8$			
	$x_4x_5x_6x_7$	$x_4x_5x_6x_8$	$x_4x_5x_7x_8$	
	$x_4x_6x_7x_8$			
	$x_5x_6x_7x_8$			Tot: 43
5	$x_1x_5x_6x_7x_8$	$x_2x_5x_6x_7x_8$		
	$x_3x_4x_5x_6x_7$	$x_3x_4x_5x_6x_8$	$x_3x_4x_5x_7x_8$	$x_3x_4x_6x_7x_8$
	$x_3x_5x_6x_7x_8$			
	$x_4x_5x_6x_7x_8$			Tot: 8
6	$x_3x_4x_5x_6x_7x_8$			Tot: 1