Projektivitetseigenskapar til p-nivå design

av: Lars Tore Slettan, veileder: John Tyssedal

May 9, 2016

1. Problem.

Finn ut kor mange faktorar kvar med p-nivå, der p er eit primtal, ein kan eksperimentere med i p^k, der k=3, 4,... , enkeltforsøk og likevel ha at kvar undermengde av 3 faktorkolonner inneheld alle dei p^3 nivåkombinasjonane. Dersom p=3 vil ein altså vite kor mange faktorar ein kan eksperimentere med i 3^3=27, 3^4=81, osv. enkeltforsøk og ha denne eigenskapen.

2. Faktorkolonner i p^k-design og assosierte vektorer i $(\mathbb{Z}_p)^k$.

La oss først se på et p^k-design med enkeltfaktorene A_1, A_2, ...,A_k, hvor hver enkeltfaktor har p ulike nivåer. Vi lar disse nivåene være 0,1,2,...,(p-1). Vi må dermed teste p^k ulike nivåkombinasjoner. La oss ta som eksempel et nivåforsøk hvor enkeltfaktor A_i har nivå a_i, hvor $a_i \in \mathbb{Z}_p \ \forall i$, $\mathbb{Z}_p$ er mengden av heltall fra og med null til p, hvor p er ekskludert. Da vil faktoren $A_1^{b_1} A_2^{b_2} ... A_k^{b_k}$ ha nivå x, hvor x er gitt ved:

$$x \equiv a_1 b_1 + ... + a_k b_k \mod p$$

La oss nå assosiere en vektor $\mathbf{v}$=$(b_1, ..., b_k)$ med faktoren $A_1^{b_1} ... A_k^{b_k}$. Målet med å betrakte en vektor $\mathbf{v} \in (\mathbb{Z}_p)^k$, er at vi senere skal se at problemet med å finne en mengde faktorer i et p^k-design hvor alle undermengder av tre faktorkolonner gir alle p^3 nivåkombinasjonene, er ekvivalent med å finne en mengde vektorer i $(\mathbb{Z}_p)^k$ slik at alle undermengder av tre vektorer er lineært uavhengige.

La $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{a} \in (\mathbb{Z}_p)^k$, og $\mathbf{x} \in (\mathbb{Z}_p)^3$. Vi betrakter $\mathbf{v}_i$'ene som radvektorer og $\mathbf{a}$, $\mathbf{x}$ som kolonnevektorer. $\mathbf{v}_i$'ene er assosierte vektorer til faktorkolonner, $\mathbf{a}$ er vektoren bestående av de ulike nivåene til enkeltfaktorene A_i, og $\mathbf{x}$ er vektoren av nivåene av de ulike faktorkolonnene gitt nivåene til a_i'ene. La videre $\mathbf{V}$ være matrisen:

$$\mathbf{V} = \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \mathbf{v}_3 \end{bmatrix}$$

I et p^k-design så testes alle nivåer av a_i, for alle A_i. Dette er det samme som at $\mathbf{a}$ løper gjennom hele $(\mathbb{Z}_p)^k$. Vi ser nå at problemet med få alle de p^3 ulike nivåkombinasjonene med tre faktorkolonner er det samme som å finne tre vektorer $\mathbf{v}_1, \mathbf{v}_2$ og $\mathbf{v}_3$ slik at ligningssystemet under kan løses med hensyn på $\mathbf{a}$ for alle $\mathbf{x} \in (\mathbb{Z}_p)^3$.

$$\mathbf{Va} = \mathbf{x} \tag{1}$$

Da har vi at:

Tre faktorkolonner kan lage alle de p^3 ulike nivåkombinasjonene hvis og bare hvis $\mathbf{V}$ er konstruert av tre lineært uavhengige vektorer.

Bevis: *La oss anta at $\boldsymbol{V}$ består av tre lineært uavhengige vektorer. Da vet vi at dim(rad($\boldsymbol{V}$))= 3, hvor rad($\boldsymbol{V}$) er radrommet til $\boldsymbol{V}$. Alle matriser har samme dimensjon på radrommet og kolonnerommet. Dermed er dim(kol($\boldsymbol{V}$))=3, hvor kol($\boldsymbol{V}$) er kolonnerommet til $\boldsymbol{V}$. Vi har også at dim($(\mathbb{Z}_p)^3$) = 3. Dette medfører at kolonnerommet til $\boldsymbol{V}$ er hele $(\mathbb{Z}_p)^3$. Dette gjør at $\boldsymbol{x}$ er i kolonnerommet til $\boldsymbol{V}$ og vi kan dermed løse ligning (1) med hensyn på $\boldsymbol{a}$ for alle $\boldsymbol{x} \in (\mathbb{Z}_p)^3$. Dette vil medføre at faktorkolonnene assosiert med $\boldsymbol{v}_i$'ene vil gi alle de p^3 ulike nivåkombinasjonene når vi tester alle p^k nivåkombinasjonene for $\boldsymbol{a}$.*

La oss anta at $\boldsymbol{V}$ ikke består av tre lineært uavhengige vektorer. Det vil si at dim(kol($\boldsymbol{V}$))<3. Siden dim($(\mathbb{Z}_p)^3$)=3, så finnes $\boldsymbol{x} \in (\mathbb{Z}_p)^3$ slik at ligningssystemet (1) ikke har en løsning for noen $\boldsymbol{a} \in (\mathbb{Z}_p)^k$. Dermed har vi ikke egenskapen at faktorkolonnene assosiert med $\boldsymbol{v}_i$'ene inneholder alle de p^3 ulike nivåkombinasjonene.

□

3. Bilineært uavhengige vektorer.

Definisjon: La $\mathbf{v}_i, \mathbf{v}_j, \mathbf{v}_k \in (\mathbb{Z}_p)^k$. Da er $\mathbf{v}_i$ **bilineært uavhengig** av $\mathbf{v}_j$ og $\mathbf{v}_k$, forutsatt at det ikke finnes $\alpha_j, \alpha_k \in \mathbb{Z}_p$ slik at $\mathbf{v}_i = \alpha_j \mathbf{v}_j + \alpha_k \mathbf{v}_k$. Altså er $\mathbf{v}_i$ bilineært uavhengig av $\mathbf{v}_j$ og $\mathbf{v}_k$ hvis $\mathbf{v}_i$ ikke er en lineærkombinasjon av de to andre vektorene. Hvis to vektorer er et skalarprodukt av den andre sier vi at de er bilineært avhengig. Nullvektoren er bilineært avhengig av alle vektorer.

Grunnen til at vi betrakter bilineært uavhengige vektorer, er at tre vektorer som er bilineært uavhengige av hverandre er også lineært uavhengige av hverandre. Vårt opprinnelige problem er å finne den maksimale mengden faktorkolonner slik at alle undermengder av tre faktorkolonner gir alle p^3 nivåkombinasjonene. Dette vet vi er det samme som å finne maksimalt antall vektorer hvor alle undermengder av tre vektorer er lineært uavhengig. Hvis vi har en mengde med bilineært uavhengige vektorer, vil denne mengden oppfylle kravet om at alle delmengder av tre vektorer er lineært uavhengig. Vi kommer dermed til å rette fokuset over mot mengder av bilineært uavhengige vektorer.

Altså, hvis vi har en mengde bilineært uavhengige vektorer og ser på en vilkårlig undermengde av størrelse tre, vil de tre vektorene være lineært uavhengige og dermed vil de assosierte faktorkolonnene tilfredstille betingelsen i vårt opprinnelige problemet. Hvis vi har en mengde vektorer som ikke er bilineært uavhengig så vil det finnes en vektor som er en lineærtkombinasjon av to andre vektorer i mengden, og følgelig vil denne undermengden av tre vektorer være lineært avhengig. Når tre vektorer er lineært avhengig, så vil de tre assosierte faktorkolonnene ikke generere alle de p^3 nivåkombinasjonene.

La oss nå betrakte en mengde Ω av vektorer $\mathbf{v}_i \in (\mathbb{Z}_p)^k$, slik at ingen $\mathbf{v}_i \in \Omega$ er en lineærkombinasjon av to andre vektorer i Ω. Altså er Ω en mengde av bilineært uavhengige vektorer. La $\mathbf{u} \in (\mathbb{Z}_p)^k$ være en vektor som ikke er i Ω, og er slik at $\mathbf{u}$ ikke er en lineærkombinasjon av to vektorer i Ω. Da vil Ω^* også være en mengde med bilineært uavhengige vektorer, hvor $\Omega^* = \Omega \cup \mathbf{u}$. Altså:

Hvis Ω er en mengde bilineært uavhengige vektorer i $(\mathbb{Z}_p)^k$, $\mathbf{u} \in (\mathbb{Z}_p)^k$, $\mathbf{u} \notin \Omega$ og $\mathbf{u}$ er bilineært uavhengige av alle vektorene i Ω. Da er Ω^* også en mengde av bilineært uavhengige vektorer, hvor $\Omega^* = \Omega \cup \mathbf{u}$.

Bevis: *La $\Omega^* = \Omega \cup \boldsymbol{u}$, hvor $\boldsymbol{u}$ ikke er en lineærkombinasjon av to vektorer i Ω, og Ω består av bilineært uavhengige vektorer. Anta så at det finnes en $\boldsymbol{v}_i \in \Omega^*$ slik at $\boldsymbol{v}_i = \alpha_j \boldsymbol{v}_j + \alpha_k \boldsymbol{v}_k$, hvor $\boldsymbol{v}_i, \boldsymbol{v}_j, \boldsymbol{v}_k \in \Omega^*$ og $\alpha_j, \alpha_k \in \mathbb{Z}_p$. Siden $\boldsymbol{u}$ ikke er en lineærkombinasjon av to vektorer i Ω, så må $\boldsymbol{v}_i$ være i Ω. Siden Ω består av bilineært uavhengige vektorer så medfører dette at enten $\boldsymbol{v}_j$ eller $\boldsymbol{v}_k$ er $\boldsymbol{u}$. Vi kan anta at $\boldsymbol{v}_j = \boldsymbol{u}$. Da er $\boldsymbol{v}_i = \alpha_j \boldsymbol{u} + \alpha_k \boldsymbol{v}_k$. Hvis $\alpha_j = 0$, så er $\boldsymbol{v}_i = \boldsymbol{v}_j$. Ellers er $\boldsymbol{u} = \alpha_j^{-1} \boldsymbol{v}_i - \alpha_j^{-1} \alpha_k \boldsymbol{v}_k$. Altså er $\boldsymbol{u}$ en lineærkombinasjon av to vektorer i Ω. Dette er en selvmotsigelse. Altså er Ω^* en mengde av bilineært uavhengige vektorer.*

□

Vi vil altså fortsatt ha en mengde Ω^* med bilineært uavhengige vektorer ved å legge til en ny vektor $\mathbf{u}$ til Ω, hvis $\mathbf{u}$ er bilineært uavhengig av vektorene i Ω. Dermed må vi undersøke hvor vi kan finne vektorer $\mathbf{u}$ bilineært uavhengig av Ω.

4. Det bilineære utspennet.

Definisjon: $\mathbf{H}_{\mathbf{v}_i, \mathbf{v}_j}$ er det **bilineære utspennet** til vektorene $\mathbf{v}_i$ og $\mathbf{v}_j$, hvor

$$\mathbf{H}_{\mathbf{v}_i \mathbf{v}_j} = \left\{ \alpha_i \mathbf{v}_i + \alpha_j \mathbf{v}_j \middle| \, \alpha_i, \alpha_j \in \mathbb{Z}_p, \, \mathbf{v}_i, \mathbf{v}_j \in (\mathbb{Z}_p)^k \right\}.$$

Altså er det bilineære utspennet til $\mathbf{v}_i$ og $\mathbf{v}_j$ alle lineærkombinasjoner av vektorene $\mathbf{v}_i$ og $\mathbf{v}_j$, hvor koeffisienten til hver vektor er et element i $\mathbb{Z}_p$. Hvis i=j,

så vil $\mathbf{H}_{\mathbf{v}_i\mathbf{v}_j}$ være alle lineærkombinasjoner av $\mathbf{v}_i$.

Videre definerer vi $\mathbf{H}_\Omega$ som det **bilineære utspennet** til mengden Ω , hvor

$$\mathbf{H}_\Omega = \bigcup_{\mathbf{v}_i,\mathbf{v}_j \in \Omega} \mathbf{H}_{\mathbf{v}_i\mathbf{v}_j}$$

Vi har at $\mathbf{H}_\Omega$ er alle lineærkombinasjoner av to eller færre vektorer fra Ω.

La Ω være en mengde som består av bilineært uavhengige vektorer. Ved å finne en $\mathbf{u} \in (\mathbb{Z}_p)^k \backslash \mathbf{H}_\Omega$, så vil $\Omega^* = \Omega \cup \mathbf{u}$ bestå av bilineært uavhengige vektorer. Vårt opprinnelige problem er dermed ekvivalent med å bestemme hvor mange bilineært uavhengige vektorer vi kan legge til Ω, før $\mathbf{H}_\Omega = (\mathbb{Z}_p)^k$. Vi vil altså finne maksimalt antall bilineært uavhengige vektorer slik at det bilineære utspennet av disse vektorene er hele rommet $(\mathbb{Z}_p)^k$. Vi har alltid at $\mathbf{H}_\Omega \subseteq (\mathbb{Z}_p)^k$. Videre har vi at $\mathbf{H}_\Omega \subset \mathbf{H}^*_\Omega$ hvis $\mathbf{u}$ er bilineært uavhengig av Ω. Dette kan vi se av at $\mathbf{u} \in \mathbf{H}^*_\Omega$, og $\mathbf{u} \notin \mathbf{H}_\Omega$.

5. Maksimalt antall bilineære vektorer i $(\mathbb{Z}_2)^k$.

La $\mathbf{V}^k_{odd}$ betegne mengden av alle vektorer i $(\mathbb{Z}_p)^k$ som er slik at en vektor $\mathbf{v}$ er i $\mathbf{V}^k_{odd}$, hvis $\mathbf{v}$ består av et odde antall 1'ere og resten av koordinatene er 0. La $\mathbf{v}_i, \mathbf{v}_j \in \mathbf{V}^k_{odd}$, og la $\mathbf{v}_k = \mathbf{v}_i + \mathbf{v}_j$. Da har $\mathbf{v}_k$ et partall antall 1'ere. Dermed er $\mathbf{v}_k \notin \mathbf{V}^k_{odd}$, og følgelig har vi vist at $\mathbf{v}^k_{odd}$ en bilineært uavhengig mengde i $(\mathbb{Z}_2)^k$.

La $\mathbf{x}$ være et vilkårlig element i $(\mathbb{Z}_2)^k$. Enten består $\mathbf{x}$ av et odde antall 1'ere, og da er $\mathbf{x} \in \mathbf{V}^k_{odd}$. Hvis $\mathbf{x}$ består av et partall antall 1'ere så kan vi finne $\mathbf{v}_i, \mathbf{v}_j \in \mathbf{V}^k_{odd}$ slik at $\mathbf{x} = \mathbf{v}_i + \mathbf{v}_j$. Dermed er det bilineære utspennet til $\mathbf{V}^k_{odd}$ i $(\mathbb{Z}_2)^k$, hele $(\mathbb{Z}_2)^k$.

Maksimal størrelse på en bilineært uavhengig mengde i $(\mathbb{Z}_2)^k$ er 2^{k-1}.

Bevis: *Fra resultatet ovenfor ser vi at $\boldsymbol{V}^k_{odd}$ er en bilineært uavhengig mengde i $(\mathbb{Z}^k_2$, og det bilineære utspennet til $\boldsymbol{V}^k_{odd}$ er hele rommet $(\mathbb{Z}_2)^k$. Vi har at $|\boldsymbol{V}^k_{odd}| = 2^{k-1}$. Anta nå at det finnes en mengde Ω med bilineært uavhengig vektorer slik at $\boldsymbol{H}_\Omega = (\mathbb{Z}_2)^k$, og hvor $|\Omega| > 2^{k-1}$. Da finnes $\boldsymbol{x} \in \Omega$ og en undermengde $\boldsymbol{A}_1$ av Ω, slik at $\boldsymbol{x} \notin \boldsymbol{A}_1$ og $|\boldsymbol{A}_1| = 2^{k-1}$. La oss konstruere mengden $\boldsymbol{A}_2$, hvor*

$$\boldsymbol{A}_2 = \{\boldsymbol{x} + \boldsymbol{v} \,|\, \boldsymbol{v} \in \boldsymbol{A}_1\}$$

Vi har at $|\boldsymbol{A}_2| = 2^{k-1}$. Anta $\boldsymbol{A}_1 \cap \boldsymbol{A}_2 = \emptyset$. Da er $\boldsymbol{A}_1 \cup \boldsymbol{A}_2 = (\mathbb{Z}_2)^k$. Siden nullvektoren er i $(\mathbb{Z}_2)^k$, så må nullvektoren enten være i $\boldsymbol{A}_1$ eller $\boldsymbol{A}_2$. Begge deler er umulig siden vi har antatt bilineæritet for Ω. Hvis $\boldsymbol{A}_1 \cap \boldsymbol{A}_2 \neq \emptyset$, så finnes $\boldsymbol{v}_i, \boldsymbol{v}_j \in \boldsymbol{A}_1$ slik at $\boldsymbol{v}_i = \boldsymbol{x} + \boldsymbol{v}_j$. Dette vil igjen motsi vår antagelse om at Ω er en bilineært uavhengig mengde. Fra dette følger at maksimal størrelse på

en bilineært uavhengig mengde i $(\mathbb{Z}_2)^k$ *er* 2^{k-1}.

□

La Ω_1 og Ω_2 være to mengder som enkeltvis er bilineært uavhengige. Da har vi at

$\mathbf{H}_{\Omega_1} = \mathbf{H}_{\Omega_2}$ medfører ikke at $|\Omega_1| = |\Omega_2|$.

Bevis: *Ta som et moteksempel mengdene* Ω_1 *og* Ω_2 *i* $(\mathbb{Z}_2)^k$*, hvor*

$$\Omega_1 = \begin{Bmatrix} (1,0,0,0) \\ (0,1,0,0) \\ (0,0,1,0) \\ (0,0,0,1) \\ (1,1,1,1) \end{Bmatrix}, \quad \Omega_2 = \begin{Bmatrix} (1,0,0,0) & (0,1,1,1) \\ (0,1,0,0) & (1,0,1,1) \\ (0,0,1,0) & (1,1,0,1) \\ (0,0,0,1) & (1,1,1,0) \end{Bmatrix}$$

Vektorene i Ω_1 *er åpenbart bilineært uavhengig, siden ingen vektor i* Ω_1 *er summen av to andre vektorer fra* Ω_1*. La* $\boldsymbol{V}_j$ *betegne mengden av vektorer i* $(\mathbb{Z}_2)^k$ *som består av j antall 1'ere, og resten av koordinatene er 0.* $\boldsymbol{V}_0$ *er kun nullvektoren, som alltid er i det bilineære utspennet. Hele* $\boldsymbol{V}_1$ *er i* Ω_1*, og er dermed også i det bilineære utspennet til* Ω_1*. Alle vektorer i* $\boldsymbol{V}_2$ *kan skrives som summen av to vektorer fra* $\boldsymbol{V}_1$*, og er dermed i det bilineære utspennet. Alle vektorer i* $\boldsymbol{V}_3$ *kan skrives som en sum av en vektor fra* $\boldsymbol{V}_1$ *og vektoren (1,1,1,1). Dermed er* $\boldsymbol{V}_3 \subseteq \boldsymbol{H}_{\Omega_1}$*. Tilslutt har vi at* $\boldsymbol{V}_4$ *er i* Ω_1*, og dermed er* $\boldsymbol{V}_4$ *i det bilineære utspennet. Altså er* $\boldsymbol{H}_{\Omega_1} = (\mathbb{Z}_2)^k$.

Vi gjenkjenner Ω_2 *som* $\boldsymbol{V}^4_{odd}$*. Vi har tidligere vist at mengden* $\boldsymbol{V}^k_{odd}$ *er bilineært uavhengig for alle k, og at det bilineære utspennet til* $\boldsymbol{V}^k_{odd}$ *er hele* $(\mathbb{Z}_2)^k$*. Dermed er* $\boldsymbol{H}_{\Omega_1} = \boldsymbol{H}_{\Omega_2}$*, og* $|\Omega_1| \neq |\Omega_2|$.

□

6. Bilineært uavhengig mengde for $(\mathbb{Z}_3)^k$.

$\mathbf{V}^k_{odd}$ er en mengde bilineært uavhengige vektorer i $(\mathbb{Z}_3)^k$.

Bevis: *La oss anta at* $\boldsymbol{V}^k_{odd}$ *ikke er en mengde bilineært uavhengige vektorer i* $(\mathbb{Z}_3)^k$*. Da finnes forskjellige* $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{x} \in \boldsymbol{V}^k_{odd}$ *og* $\alpha, \beta \in \mathbb{Z}_3$*, slik at* $\alpha\boldsymbol{v}_1 + \beta\boldsymbol{v}_2 = \boldsymbol{x}$*. Vi kan hele tiden anta at* $\alpha \geq \beta$*. Vi kan avskrive muligheten for at* $\beta = 0$*, siden dette vil medføre at* $\alpha\boldsymbol{v}_1 = \boldsymbol{x}$*, noe som er umulig for forskjellige* $\boldsymbol{v}_1, \boldsymbol{x} \in \boldsymbol{V}^k_{odd}$*. La* $\boldsymbol{v}_1 = (a_1, a_2, ..., a_k)$, $\boldsymbol{v}_2 = (b_1, b_2, ..., b_k)$ *og* $\boldsymbol{x} = (c_1, c_2, ..., c_k)$*. Da har vi relasjonen* $\alpha a_i + \beta b_i = c_i$ *som må holde for alle i, hvor 1*$\leq i \leq$*k. Videre definerer vi*

$$\boldsymbol{I}_j(\boldsymbol{v}_1) = \{i | a_i = j\}, \ \boldsymbol{I}_j(\boldsymbol{v}_2) = \{i | b_i = j\}, \ \boldsymbol{I}_j(\boldsymbol{v}_3) = \{i | c_i = j\}$$

$\boldsymbol{I}_j(\boldsymbol{v}_1)$ *er dermed mengden av alle indekser til* $\boldsymbol{v}_1$*, slik at* $a_i = j$.

Anta $\alpha = \beta = 1$. Da er $a_i + b_i = c_i$ for alle i. Siden c_i enten er 0 eller 1, så kan ikke både a_i og b_i være 1. Dermed er $\boldsymbol{I}_1(\boldsymbol{v}_1) \cap \boldsymbol{I}_1(\boldsymbol{v}_2) = \emptyset$. Dette medfører at $\boldsymbol{x}$ består av et partall antall 1'ere, noe som motsier at $\boldsymbol{x} \in \boldsymbol{V}_{odd}^k$.

Anta $\alpha = 2$ og $\beta = 1$. Da er $2a_i + b_i = c_i$ for alle i. Hvis $a_i = 1$, så er $b_i = 1$. Altså er $\boldsymbol{I}_1(\boldsymbol{v}_1) \subseteq \boldsymbol{I}_1(\boldsymbol{v}_2)$. Vi har også at hvis $a_i = 1$, så er $c_i = 0$. Dette gir $\boldsymbol{I}_1(\boldsymbol{x}) = \boldsymbol{I}_1(\boldsymbol{v}_2) \backslash \boldsymbol{I}_1(\boldsymbol{v}_1)$. Vi kommer frem til en motsigelse siden $|\boldsymbol{I}_1(\boldsymbol{v}_2) \backslash \boldsymbol{I}_1(\boldsymbol{v}_1)|$ er et partall, og vi har antatt at $\boldsymbol{x} \in \boldsymbol{V}_{odd}^k$.

Anta $\alpha = \beta = 2$. Da er $2a_i + 2b_i = c_i$ for alle i. Dette holder kun hvis $a_i = b_i$. Altså er $\boldsymbol{v}_1 = \boldsymbol{v}_2$, noe som vil medføre at $4\boldsymbol{v}_1 = \boldsymbol{x}$. Siden vi opererer i $(\mathbb{Z}_3)^k$, så er da $\boldsymbol{v}_i = \boldsymbol{x}$. Vi har igjen oppnådd en motsigelse siden vi antok vektorene var bilineært uavhengige, og konkluderer med at $\boldsymbol{V}_{odd}^k$ er en bilineært uavhengig mengde i $(\mathbb{Z}_3)^k$.

□

Det bilineære utspennet til $\mathbf{V}_{odd}^k$ i $(\mathbb{Z}_3)^k$, er hele $(\mathbb{Z}_3)^k$.

Bevis: *La $\boldsymbol{z}$ være en vilkårlig vektor i $(\mathbb{Z}_3)^k$, la $\boldsymbol{I}_0, \boldsymbol{I}_1$ og $\boldsymbol{I}_2$ være definert tilsvarende som i beviset ovenfor, hvor vi har droppet notasjonen som angir hvilken vektor disse mengdene er avhengige av, siden vi i dette beviset kun betrakter vektoren $\boldsymbol{z}$. La $\boldsymbol{M}$ være en undermengde av mengden $\{1, 2, ..., k\}$. Da definerer vi $\boldsymbol{1}_{\boldsymbol{M}} = (a_1, a_2, ..., a_k)$ til å være $a_i = 1$ hvis $i \in \boldsymbol{M}$, og $a_i = 0$ hvis $i \notin \boldsymbol{M}$. Altså er $\boldsymbol{1}_{\boldsymbol{M}}$ vektoren med 1'ere i alle koordinater hvor indeksen til koordinatet er i $\boldsymbol{M}$, og har 0'ere i resten av koordinatene. Vi vil vise at alle $\boldsymbol{z} \in (\mathbb{Z}_3)^k$ kan skrives som en lineærkombinasjon av to vektorer $\boldsymbol{v}_1, \boldsymbol{v}_2$ fra $\boldsymbol{V}_{odd}^k$. Legg merke til at $\boldsymbol{1}_{\boldsymbol{M}} \in \boldsymbol{V}_{odd}^k$ hvis $|\boldsymbol{M}|$ er et oddetall.*

Anta at $|\boldsymbol{I}_1|$ og $|\boldsymbol{I}_2|$ begge er oddetall. Da er $\boldsymbol{z} = \boldsymbol{1}_{\boldsymbol{I}_1} + 2 * \boldsymbol{1}_{\boldsymbol{I}_2}$, og $\boldsymbol{1}_{\boldsymbol{I}_1}, \boldsymbol{1}_{\boldsymbol{I}_2} \in \boldsymbol{V}_{odd}^k$.

Hvis $|\boldsymbol{I}_1|$ er et partall og $|\boldsymbol{I}_2|$ er et oddetall, så er $\boldsymbol{1}_{\boldsymbol{I}_1 \cup \boldsymbol{I}_2}$ og $\boldsymbol{1}_{\boldsymbol{I}_2}$ i $\boldsymbol{V}_{odd}^k$, og $\boldsymbol{z} = \boldsymbol{1}_{\boldsymbol{I}_1 \cup \boldsymbol{I}_2} + \boldsymbol{1}_{\boldsymbol{I}_2}$.

Hvis $|\boldsymbol{I}_1|$ er et oddetall og $|\boldsymbol{I}_2|$ er et partall, så har vi at $\boldsymbol{z} = 2 * \boldsymbol{1}_{\boldsymbol{I}_1} + 2 * \boldsymbol{1}_{\boldsymbol{I}_1 \cup \boldsymbol{I}_2}$, og $\boldsymbol{1}_{\boldsymbol{I}_1}, \boldsymbol{1}_{\boldsymbol{I}_1 \cup \boldsymbol{I}_2} \in \boldsymbol{V}_{odd}^k$.

Til slutt tar vi for oss hvis både $|\boldsymbol{I}_1|$ og $|\boldsymbol{I}_2|$ er partall. Vi ser først på tilfellet hvor $\boldsymbol{I}_2$ er ikke-tom. La $a \in \boldsymbol{I}_2$. Da er $\boldsymbol{z} = 2 * \boldsymbol{1}_{\boldsymbol{I}_1 \cup a} + 2 * \boldsymbol{1}_{\boldsymbol{I}_1 \cup \boldsymbol{I}_2 \backslash a}$, og $\boldsymbol{1}_{\boldsymbol{I}_1 \cup a}, \boldsymbol{1}_{\boldsymbol{I}_1 \cup \boldsymbol{I}_2 \backslash a} \in \boldsymbol{V}_{odd}^k$. La nå $\boldsymbol{I}_2 = \emptyset$. Hvis også $\boldsymbol{I}_1 = \emptyset$, så er $\boldsymbol{z}$ nullvektoren. Anta derfor at $\boldsymbol{I}_1 \neq \emptyset$. Siden $|\boldsymbol{I}_1|$ er et partall, så er $|\boldsymbol{I}_1| \geq 2$. Vi kan dermed finne en partering av $\boldsymbol{I}_1$ slik at $\boldsymbol{I}_1 = \boldsymbol{A} \cup \boldsymbol{B}$, $\boldsymbol{A} \cap \boldsymbol{B} = \emptyset$, og både $|\boldsymbol{A}|$ og $|\boldsymbol{B}|$ er oddetall. Dermed er $\boldsymbol{z} = \boldsymbol{1}_{\boldsymbol{A}} + \boldsymbol{1}_{\boldsymbol{B}}$, hvor $\boldsymbol{1}_{\boldsymbol{A}}, \boldsymbol{1}_{\boldsymbol{B}} \in \boldsymbol{V}_{odd}^k$. Vi kan konkludere med at det bilineære utspennet til $\boldsymbol{V}_{odd}^k$ i $(\mathbb{Z}_3)^k$, er hele $(\mathbb{Z}_3)^k$.

□

7. Størrelsen på $\mathbf{H}_\Omega$ når Ω vokser.

La $|\mathbf{H}_\Omega|$ betegne kardinaliteten til det bilineære utspennet til Ω. Hvis $|\mathbf{H}_\Omega| \neq |(\mathbb{Z}_p)^k| = p^k$, så medfører dette at $(\mathbb{Z}_p)^k \backslash \mathbf{H}_\Omega \neq \emptyset$. Altså finnes $\mathbf{u} \in (\mathbb{Z}_p)^k \backslash \mathbf{H}_\Omega$

slik at $\mathbf{u}$ er bilineært uavhengig av vektorene i Ω. Dermed kan vi legge en vektor $\mathbf{u}$ til Ω, og enda ha en mengde med bilineært uavhengige vektorer. Under skal vi finne relasjonen mellom kardinaliteten til det bilineære utspennet til Ω, og til Ω^*, hvor $\Omega^* = \Omega \cup \mathbf{u}$, og $\mathbf{u}$ er bilineært uavhengig av vektorene i Ω.

La oss anta at Ω er en ikke-tom mengde av bilineært uavhengige vektorer i $(\mathbb{Z}_p)^k$, $\mathbf{u}$ er bilineært uavhengig av Ω. Altså er $\mathbf{u} \notin \mathbf{H}_\Omega$. La $\Omega^* = \Omega \cup \mathbf{u}$. Da er per definisjon

$$\mathbf{H}_{\Omega^*} = \bigcup_{\mathbf{v}_i,\mathbf{v}_j \in \Omega^*} \mathbf{H}_{\mathbf{v}_i,\mathbf{v}_j} = (\bigcup_{\mathbf{v}_i,\mathbf{v}_j \in \Omega} \mathbf{H}_{\mathbf{v}_i,\mathbf{v}_j}) \cup (\bigcup_{\mathbf{v} \in \Omega^*} \mathbf{H}_{\mathbf{u},\mathbf{v}}) = \mathbf{H}_\Omega \cup (\bigcup_{\mathbf{v} \in \Omega^*} \mathbf{H}_{\mathbf{u},\mathbf{v}})$$

Dermed vil

$$|\mathbf{H}_{\Omega^*}| = |\mathbf{H}_\Omega| + |\bigcup_{\mathbf{v} \in \Omega^*} \mathbf{H}_{\mathbf{u},\mathbf{v}}| - |\mathbf{H}_\Omega \cap \bigcup_{\mathbf{v} \in \Omega^*} \mathbf{H}_{\mathbf{u},\mathbf{v}}|.$$

La oss se nærmere på $|\bigcup_{\mathbf{v} \in \Omega^*} \mathbf{H}_{\mathbf{u},\mathbf{v}}|$.

Anta det finnes i,j forskjellige slike at $\mathbf{H}_{\mathbf{u},\mathbf{v}_i} \cap \mathbf{H}_{\mathbf{u},\mathbf{v}_j} \neq \emptyset$. Dette medfører at en relasjon av formen $\alpha_i\mathbf{u}+\beta_i\mathbf{v}_i = \alpha_j\mathbf{u}+\beta_j\mathbf{v}_j$ eksisterer, hvor $\alpha_i, \alpha_j, \beta_i, \beta_j \in \mathbb{Z}_p$. Fra dette får vi at $(\alpha_i - \alpha_j)\mathbf{u} = -\beta_i\mathbf{v}_i + \beta_j\mathbf{v}_j$. Hvis $\alpha_i = \alpha_j$, så er $\beta_i\mathbf{v}_i = \beta_j\mathbf{v}_j$. Dette er kun mulig hvis $\beta_i = \beta_j = 0$, siden vi har antatt at $\mathbf{v}_i$ og $\mathbf{v}_j$ er bilineært uavhengige. Hvis $\alpha_i \neq \alpha_j$, så medfører dette at

$$\mathbf{u} = (\alpha_i - \alpha_j)^{-1}(-\beta_i)\mathbf{v}_i + (\alpha_i - \alpha_j)^{-1}(\beta_j)\mathbf{v}_j.$$

På grunn av antagelsen om bilineæritet, så må igjen $\beta_i = \beta_j = 0$. Dette vil implisere at $\alpha_i = \alpha_j$. Vi har dermed at $\mathbf{H}_{\mathbf{u},\mathbf{v}_i} \cap \mathbf{H}_{\mathbf{u},\mathbf{v}_j} = \mathbf{H}_{\mathbf{u},\mathbf{u}}$ når i og j er forskjellige.

Vi har at $\bigcup_{\mathbf{v} \in \Omega^*} \mathbf{H}_{\mathbf{u},\mathbf{v}} = \mathbf{H}_{\mathbf{u},\mathbf{u}} \cup (\bigcup_{\mathbf{v} \in \Omega}(\mathbf{H}_{\mathbf{u},\mathbf{v}} \backslash \mathbf{H}_{\mathbf{u},\mathbf{u}}))$. For ulike i,j så er $(\mathbf{H}_{\mathbf{u},\mathbf{v}_i} \backslash \mathbf{H}_{\mathbf{u},\mathbf{u}})$ og $(\mathbf{H}_{\mathbf{u},\mathbf{v}_j} \backslash \mathbf{H}_{\mathbf{u},\mathbf{u}})$ disjunkte mengder. Altså er

$$|\bigcup_{\mathbf{v} \in \Omega^*} \mathbf{H}_{\mathbf{u},\mathbf{v}}| = |\mathbf{H}_{\mathbf{u},\mathbf{u}}| + \sum_{\mathbf{v} \in \Omega} |\mathbf{H}_{\mathbf{u},\mathbf{v}} \backslash \mathbf{H}_{\mathbf{u},\mathbf{u}}| = p + |\Omega|p(p-1).$$

Vi betrakter nå $|\mathbf{H}_\Omega \cap \bigcup_{\mathbf{v} \in \Omega^*} \mathbf{H}_{\mathbf{u},\mathbf{v}}|$. Vi ser at nullvektoren er i $\mathbf{H}_\Omega \cap \bigcup_{\mathbf{v} \in \Omega^*} \mathbf{H}_{\mathbf{u},\mathbf{v}}$. I tillegg er $\mathbf{H}_{\mathbf{v},\mathbf{v}} \subseteq (\mathbf{H}_\Omega \cap \bigcup_{\mathbf{v} \in \Omega^*} \mathbf{H}_{\mathbf{u},\mathbf{v}})$ for alle $\mathbf{v} \in \Omega$. La oss finne $\mathbf{y} \in \mathbf{H}_\Omega \cap \bigcup_{\mathbf{v} \in \Omega^*} \mathbf{H}_{\mathbf{u},\mathbf{v}}$ slik at $\mathbf{y}$ er forskjellig fra nullvektoren og $\mathbf{y} \notin \mathbf{H}_{\mathbf{v},\mathbf{v}}$ for $\mathbf{v} \in \Omega$. Dermed er $\mathbf{y} \in \mathbf{H}_{\mathbf{v}_i,\mathbf{v}_j} \cap \mathbf{H}_{\mathbf{u},\mathbf{v}_k}$, for forskjellige $\mathbf{v}_i, \mathbf{v}_j, \mathbf{v}_k \in \Omega$. Vi får dermed en relasjon av formen:

$$\mathbf{y} = \alpha_i\mathbf{v}_i + \alpha_j\mathbf{v}_j = \beta\mathbf{u} + \alpha_k\mathbf{v}_k \tag{2}$$

hvor $\alpha_i, \alpha_j, \alpha_k, \beta \in \mathbb{Z}_p \backslash 0$.

I $(\mathbf{H}_\Omega \cap \bigcup_{\mathbf{v} \in \Omega^*} \mathbf{H}_{\mathbf{v},\mathbf{u}})$ finnes dermed nullvektoren, alle enkeltutspenn av vektorer i Ω, og alle $\mathbf{y}$ på formen (2) med ikke-null koeffisienter. Altså har vi

at

$$|\mathbf{H}_\Omega \cap \bigcup_{\mathbf{v}\in\Omega^*} \mathbf{H}_{\mathbf{v},\mathbf{u}}| = 1 + |\Omega|(p-1) + |\mathbf{Y}|$$

hvor $\mathbf{Y}$ er mengden av alle $\mathbf{y}$ som finnes på formen (2) med ulike vektorer $\mathbf{v}_i, \mathbf{v}_j, \mathbf{v}_k, \mathbf{u}$, og hvor alle koeffisientene er ikke-null. Vi ser at for alle $\mathbf{y} \in \mathbf{Y}$ vil vi finne en ligning av type

$$\mathbf{u} = \alpha_i \mathbf{v}_i + \alpha_j \mathbf{v}_j + \alpha_k \mathbf{v}_k. \tag{3}$$

hvor vektorene er forskjellige og koeffisientene er ikke-null. Videre gir alle ligninger av type (3) opphav til $\mathbf{y} \in \mathbf{Y}$. Nemlig fra $\mathbf{u} = \alpha_i \mathbf{v}_i + \alpha_j \mathbf{v}_j + \alpha_k \mathbf{v}_k$ får vi at $\mathbf{y} = (\mathbf{u} - \alpha_k \mathbf{v}_k) = \alpha_i \mathbf{v}_i + \alpha_j \mathbf{v}_j$. Vi kan dermed rette fokus mot ligninger av formen (3) for å avgjøre størrelsen på $|\mathbf{Y}|$.

La oss liste opp alle mulige ligninger for $\mathbf{u}$ på formen (3) med vektorer $\mathbf{v}_i, \mathbf{v}_j, \mathbf{v}_k \in \Omega$. Vi betegner listen under for $\mathbf{L}$. Vi finner altså alle mulig måter vi kan skrive $\mathbf{u}$ på som en lineærkombinasjon av tre vektorer fra Ω.

$$\begin{aligned}
\mathbf{u} &= \alpha_{1i}\mathbf{v}_{1i} + \alpha_{1j}\mathbf{v}_{1j} + \alpha_{1k}\mathbf{v}_{1k} \\
&= \alpha_{2i}\mathbf{v}_{2i} + \alpha_{2j}\mathbf{v}_{2j} + \alpha_{2k}\mathbf{v}_{2k} \\
&= \quad \vdots \qquad\quad \vdots \qquad\quad \vdots \\
&= \alpha_{ni}\mathbf{v}_{ni} + \alpha_{nj}\mathbf{v}_{nj} + \alpha_{nk}\mathbf{v}_{nk}
\end{aligned}$$

Ved å betrakte kun den øverste ligningen for $\mathbf{u}$ i $\mathbf{L}$, kan vi se at $(\mathbf{u} - \alpha_{1k}\mathbf{v}_{1k}) = \alpha_{1i}\mathbf{v}_{1i} + \alpha_{1j}\mathbf{v}_{1j}$. Dette medfører at $\mathbf{H}_{\mathbf{u},\mathbf{v}_{1k}} \cap \mathbf{H}_{\mathbf{v}_{1i},\mathbf{v}_{1j}}$ er større enn bare nullvektoren. La $\mathbf{H}_{\mathbf{u},\mathbf{v}_{1k}} \cap \mathbf{H}_{\mathbf{v}_{1i},\mathbf{v}_{1j}} = \mathbf{S}$. Vi har at $\mathbf{H}_{\mathbf{u},\mathbf{v}_{1k}}$ og $\mathbf{H}_{\mathbf{v}_{1i},\mathbf{v}_{1j}}$ er underrom av vektorrommet $(\mathbb{Z}_p)^k$. Siden $\mathbf{S}$ er snittet mellom to underrom, er også $\mathbf{S}$ et underrom. Dim($\mathbf{S}$)= 2 medfører $\mathbf{H}_{\mathbf{u},\mathbf{v}_{1k}} = \mathbf{H}_{\mathbf{v}_{1i},\mathbf{v}_{1j}}$, noe som motsier antagelsen om bilineæritet. Dermed er dim($\mathbf{S}$)= 1, og følgelig er $|\mathbf{S}| = p$. Alle vektorene i $\mathbf{S}$, unntatt nullvektoren, er i $\mathbf{Y}$.

Ved å la β løpe gjennom $\mathbb{Z}_p\backslash 0$, så vil $\beta(\mathbf{u} - \alpha_{1k}\mathbf{v}_{1k}) = \beta(\alpha_{1i}\mathbf{v}_{1i} + \alpha_{1j}\mathbf{v}_{1j})$. Dermed er $\beta(\mathbf{u} - \alpha_{1k}\mathbf{v}_{1k}) \in \mathbf{Y}$, og tilsvarende er $\beta(\mathbf{u} - \alpha_{1i}\mathbf{v}_{1i})$ og $\beta(\mathbf{u} - \alpha_{1j}\mathbf{v}_{1j})$ også i $\mathbf{Y}$, hvor β løper gjennom $\mathbb{Z}_p\backslash 0$. For hver koeffisient-vektor-kombinasjon $\alpha\mathbf{v}$ som dukker opp i $\mathbf{L}$ vil dette gi et bidrag på $(p-1)$ til $|\mathbf{Y}|$. Altså hvis $\alpha\mathbf{v}$ dukker opp i $\mathbf{L}$, så vil $\beta(\mathbf{u} - \alpha\mathbf{v})$ være i $\mathbf{Y}$ for alle $\beta \in \mathbb{Z}_p\backslash 0$.

Anta at det finnes to koeffisient-vektor-kombinasjoner $\alpha_1\mathbf{v}_1$ og $\alpha_2\mathbf{v}_2$ i $\mathbf{L}$ som er slik at mengdene $\beta(\mathbf{u} - \alpha_1\mathbf{v}_1)$ og $\beta(\mathbf{u} - \alpha_2\mathbf{v}_2)$ er ikke-tomme, hvor β løper gjennom hele $\mathbb{Z}_p\backslash 0$. Dermed har vi at $\beta_1(\mathbf{u} - \alpha_1\mathbf{v}_1) = \beta_2(\mathbf{u} - \alpha_2\mathbf{v}_2)$ for noen $\beta_1, \beta_2 \in \mathbb{Z}_p\backslash 0$. Dette medfører $(\beta_1 - \beta_2)\mathbf{u} = \alpha_1\mathbf{v}_1 - \alpha_2\mathbf{v}_2$. Siden vi har antatt at α_1 og α_2 er ikke-null, og bilineæritet for $\mathbf{u}$, så må $\beta_1 - \beta_2 = 0$, og dermed er $\alpha_1\mathbf{v}_1 = \alpha_2\mathbf{v}_2$. Fra dette kan vi konkludere at alle ulike koeffisient-vektor-kombinasjoner som dukker opp i $\mathbf{L}$ gir et bidrag på $(p-1)$ til $\mathbf{Y}$, og alle mengder som blir generert fra to ulike koeffisient-vektor-kombinasjoneneved at β løper gjennom hele $\mathbb{Z}_p\backslash 0$, er disjunkte.

La λ betegne antall ulike koeffisient-vektor-kombinasjoner som forekommer i $\mathbf{L}$. Da har vi at $|\mathbf{Y}| = \lambda(p-1)$, og dette gir at

$$|\mathbf{H}_\Omega \cap \bigcup_{\mathbf{v}\in\Omega^*} \mathbf{H}_{\mathbf{v},\mathbf{u}}| = 1 + |\Omega|(p-1) + \lambda(p-1).$$

Vi kan nå samle resultatene ovenfor for å finne et uttrykk for $|\mathbf{H}_{\Omega^*}|$.

La Ω være en ikke-tom mengde av bilineært uavhengige vektorer i $(\mathbb{Z}_p)^k$, $\mathbf{u}$ er bilineært uavhengig av Ω, og $\Omega^* = \Omega \cup \mathbf{u}$. Da er:

$$|\mathbf{H}_{\Omega^*}| = |\mathbf{H}_\Omega| + (p-1) + |\Omega|(p-1)^2 - \lambda(p-1) \tag{4}$$

8. Bilineære utspennet til en basis.

Formel (4) kan kreve mange utregninger ved hele tiden å legge til nye bilineært uavhengige vektorer. For å minske antall regneoperasjoner er det mulig å starte med en basis $\mathbf{B}$, og så starte prosessen med å legge til bilineært uavhengige vektorer. Siden basisvektorene er lineært uavhengig er de også bilineært uavhengig. Altså, la $\mathbf{B}$ være en vilkårlig basis for $(\mathbb{Z}_p)^k$. Da er:

$$|\mathbf{H}_\mathbf{B}| = 1 + k(p-1) + \frac{k(k-1)}{2}(p-1)^2 \tag{5}$$

Bevis: *Det er tydelig at nullvektoren er i $\boldsymbol{H_B}$. Dette gir et bidrag på 1. For alle basisvektorer $\boldsymbol{v}_i \in \boldsymbol{B}$ er $|\boldsymbol{H}_{\boldsymbol{v}_i,\boldsymbol{v}_i}| = p$, og basisvektorenes lineærutspenn har kun nullvektoren til felles. Fra enkeltlineærutspennet til hver basisvektor får $|\boldsymbol{H_B}|$ et bidrag på $(p-1)$, hvor nullvektoren er ekskludert siden vi allerede har gjort rede for den. Altså gir enkeltlineærutspennene til alle basisvektorene et bidrag på $k(p-1)$ til $|\boldsymbol{H_B}|$.*

La

$$\boldsymbol{H}^*_{\boldsymbol{v}_i,\boldsymbol{v}_j} = \left\{ \alpha_i \boldsymbol{v}_i + \alpha_j \boldsymbol{v}_j |\ \alpha_i, \alpha_j \in \mathbb{Z}_p \backslash 0,\ \boldsymbol{v}_i, \boldsymbol{v}_j \in (\mathbb{Z}_p)^k \right\}.$$

og anta at det finnes en vektor $\boldsymbol{x} \in (\mathbb{Z}_p)^k$ slik at $\boldsymbol{x} \in (\boldsymbol{H}^*_{\boldsymbol{v}_i,\boldsymbol{v}_j} \cap \boldsymbol{H}^*_{\boldsymbol{v}_k,\boldsymbol{v}_l})$. Da får vi en relasjonen $\alpha_i \boldsymbol{v}_i + \alpha_j \boldsymbol{v}_j = \alpha_k \boldsymbol{v}_k + \alpha_l \boldsymbol{v}_l$. Dermed vil

$$\boldsymbol{0} = -\alpha_i \boldsymbol{v}_i - \alpha_j \boldsymbol{v}_j + \alpha_k \boldsymbol{v}_k + \alpha_l \boldsymbol{v}_l$$

Siden $\boldsymbol{B}$ er en basis så kan dette kun skje hvis alle koeffisientene er null, noe som vi har antatt ikke er tilfellet, eller så er parene $(\boldsymbol{v}_i, \boldsymbol{v}_j)$ og $(\boldsymbol{v}_k, \boldsymbol{v}_l)$ like. Vi har dermed at for ulike par $(\boldsymbol{v}_i, \boldsymbol{v}_j)$ og $(\boldsymbol{v}_k, \boldsymbol{v}_l)$, så er $(\boldsymbol{H}^*_{\boldsymbol{v}_i,\boldsymbol{v}_j} \cap \boldsymbol{H}^*_{\boldsymbol{v}_k,\boldsymbol{v}_l}) = \emptyset$. For hvert vektorpar $(\boldsymbol{v}_i, \boldsymbol{v}_j)$ er $|\boldsymbol{H}^*_{\boldsymbol{v}_i,\boldsymbol{v}_j}| = (p-1)^2$. Antall par man kan velge ut av k ulike vektorer er $\frac{k(k-1)}{2}$. Fra dette følger (5).

□

9. Oppsummering.

I denne oppgaven har vi sett at problemet med å finne maksimalt antall faktorer med p-nivå man kan eksperimentere med og likevel ha at hver undermengde av tre faktorkolonner inneholder de p^k nivåkombinasjonene, er ekvivalent med å finne den maksimale mengden med bilineært uavhengige vektorer i $(\mathbb{Z}_p)^k$. I et 2^k design kan vi maksimalt eksperimentere med 2^{k-1} faktorer. For et 3^k design har vi sett at det også er mulig å eksperimentere med 2^{k-1} faktorer, men det er ikke vist at dette er maksimal mengde faktorer. Til slutt er en formel for størrelsen på det bilineære utspennet til en generatormengde av bilineært uavhengige vektorer når generatormengden vokser med én bilineært uavhengig vektor. Dette er av interesse siden alle vektorer utenfor det bilineære utspennet er bilineært uavhengig av generatormengden, og kan følgelig legges til den opprinnelige generatormengden.