



UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

CORSO DI LAUREA MAGISTRALE IN MATEMATICA

TESI DI LAUREA

**ANALISI DEL PROTOCOLLO CHIMERA
PER LA PROTEZIONE DI INTEGRITÀ
DEI SEGNALI GNSS**

RELATORE: Prof. Alberto Tonolo

CORRELATORE: Prof. Nicola Laurenti

LAUREANDA: Anna Poltronieri

Mat. 1111372

20 Aprile 2018

Alla mia famiglia.

Indice

Introduzione	1
1 Il sistema GPS	5
2 Descrizione di Chimera	9
3 Modello del sistema	15
4 Modelli semplificati	19
4.1 Descrizione dei modelli	21
4.2 Confronto dei modelli	24
5 Analisi degli attacchi	29
5.1 Attacco 1: indovinare la sequenza di marker a partire dal primo intercettato	30
5.2 Attacco 2: indovinare solo i marker intercettabili	34
5.3 Attacco 3: ridurre il numero di plausibili righe di M	41
6 Risultati	45
6.1 Attacco 1	45
6.2 Attacco 2	46
6.2.1 Varianti dell'attacco	46
6.2.2 Modello semplificato	48
6.3 Attacco 3	50
7 Conclusioni	55
Appendice	57
Bibliografia	87

Introduzione

Negli ultimi anni abbiamo assistito ad una velocissima crescita del numero di applicazioni che utilizzano un sistema satellitare globale di navigazione (GNSS) come fornitore di un servizio di posizionamento.

Uno di questi sistemi di navigazione è GPS (*Global Positioning System*), in cui i ricevitori che lo utilizzano, misurando la quantità di tempo che il segnale impiega a viaggiare dai satelliti fino ad essi, riescono a determinare la propria distanza da ciascuno di questi veicoli spaziali e a ricavare quindi le proprie posizioni in termini di longitudine, latitudine ed altitudine [5].

Il segnale GPS civile è aperto, ossia chiunque dotato delle giuste competenze e dell'adeguata strumentazione può generare versioni sintetiche dei segnali *satnav*, potenzialmente per fini di *spoofing*; questa caratteristica del segnale motiva il bisogno di autenticare il segnale legittimo.

Lo *spoofing* è definito come l'introduzione volontaria di segnali di navigazione satellitare contraffatti al fine di soppiantare segnali *satnav* autentici, per indurre un utente ricevitore a generare un'informazione PNT (*Position, Navigation, Timing*) anomala; in particolare, lo scopo dell'attaccante è quello di riprodurre un segnale di *spoofing* che sia abbastanza simile al segnale legittimo, con lo scopo di passare il controllo effettuato dal ricevitore.

Gran parte della letteratura che si occupa di come contrastare potenziali tentativi di *spoofing* si concentra su metodi che abilitino il ricevitore ad evincere la legittimità di un segnale osservando caratteristiche della sua manifestazione fisica (quali la potenza o la direzione di provenienza del segnale ricevuto) o output anomali del ricevitore; altri metodi legano il segnale alla sua origine usando metodi crittografici, come ad esempio NMA (*Navigation Message*

Authentication), un metodo di autenticazione del segnale che prevede la firma digitale dei dati di navigazione, utilizzato dal sistema Galileo [1].

Un'ulteriore misura di sicurezza che si può adottare è l'autenticazione dello *spreading code* del segnale, ossia di quell'insieme di bit utilizzati per ampliare la banda del segnale trasmesso, al fine di permettere la condivisione della stessa frequenza di comunicazione a più dispositivi. Questa tecnica è più resistente allo *spoofing*, a meno che gli utenti fraudolenti non usino antenne direzionali per alzare il segnale sopra il livello del rumore e analizzino direttamente i chip dello *spreading code* autenticato (ma, essendo la frequenza di chip dello *spreading code* molto più alta della frequenza di simbolo dei dati di navigazione, questo è un tipo di attacco molto meno efficace) [2].

Lo scopo di Chimera (*Chips-Message Robust Authentication*), proposto in [1], è quello di legare il messaggio di navigazione allo *spreading code*, una soluzione innovativa che permette di ottenere un segnale autenticato complessivamente; l'autenticazione in Chimera è quindi un processo a due passaggi, poiché devono superare il controllo sia i dati di navigazione, sia lo *spreading code*.

Ciò che contraddistingue questo protocollo è il fatto che si serva di una particolare struttura, detta *look-up table*, per randomizzare un passaggio del processo di autenticazione dello *spreading code*.

Lo scopo di questa tesi è proprio quello di investigare in che modo questa *look-up table* utilizzata da Chimera influisca sulla sicurezza dello schema¹.

¹Parte di questo lavoro è stata sottoposta come sommario esteso (*extended abstract*) ed è in attesa del giudizio dei revisori per il convegno *31st International Technical Meeting of The Satellite Division of the Institute of Navigation, ION GNSS+ 2018*.

Capitolo 1

Il sistema GPS

GPS (*Global Positioning System*) è uno dei sistemi GNSS attualmente operativi, gestito dal governo degli Stati Uniti d'America e liberamente accessibile a chiunque sia dotato di un ricevitore GPS.

Questo sistema di posizionamento si compone di tre segmenti:

- il segmento spaziale (*space segment*), costituito dai satelliti in orbita;
- il segmento di controllo (*control segment*), costituito da una stazione di controllo principale e da altre stazioni di monitoraggio;
- il segmento utente (*user segment*), costituito dai ricevitori GPS.

Il principio di funzionamento di GPS si basa su un metodo di posizionamento sferico detto *triangolazione* (una tecnica che permette di calcolare distanze fra punti sfruttando le proprietà dei triangoli), che come punto di partenza adotta la misura del tempo impiegato da un segnale radio a percorrere la distanza satellite-ricevitore [9]. Poiché il ricevitore non sa quando sia stato trasmesso il segnale dal satellite, calcola questa quantità di tempo a partire dalla differenza tra l'orario pervenuto e quello del proprio orologio sincronizzato con quello (atomico) a bordo del satellite, tenendo conto della velocità di propagazione del segnale.

Ciascun satellite emette su due canali: L1, l'unico disponibile al servizio SPS (*Standard Positioning System*) per uso civile, ed L2, esclusivamente per il servizio PPS (*Precision Positioning System*) ad uso militare e, per consentire a tutti i satelliti di usare la stessa frequenza di trasmissione senza interferenze reciproche, GPS utilizza una tecnica *spread-spectrum* detta CDMA (*Code-Division Multiple Access*).

In una trasmissione a *spread-spectrum*, la banda del segnale trasmesso viene ampliata mediante dei codici detti *spreading-code*; questi codici sono indipendenti dai dati di navigazione *satnav* e servono a dividere la banda disponibile tra i vari utenti utilizzatori del servizio. Ad ogni satellite viene infatti assegnata un'unica sequenza di codice usata per codificare il segnale, permettendo così al ricevitore, che conosce i codici dei satelliti, di discriminare i vari segnali e di decodificare il segnale ricevuto per ricavare i dati originali [6].

La scelta di queste sequenze è fondamentale nella performance dei sistemi CDMA; il risultato migliore si ha quando c'è una buona distinzione tra il segnale desiderato da un utente specifico e i segnali destinati agli altri utenti. La separazione dei segnali, al momento della ricezione, si fa correlando il segnale ricevuto con la copia del codice generata localmente dell'utente. Ricordando che la *correlazione* indica la somiglianza tra due segnali, nel caso in cui il codice del segnale coincida con quanto generato dall'utente, la funzione di correlazione sarà alta e il sistema potrà estrarre il segnale; se invece il codice del segnale non avrà nulla in comune con quello dell'utente, la correlazione sarà il più vicino possibile a 0 [7] e il segnale in questione sarà interpretato come rumore.

Capitolo 2

Descrizione di Chimera

Il protocollo di autenticazione Chimera descritto in [1] implementa elementi di sicurezza interdipendenti espressi sia nei dati di navigazione, sia nello *spreading code* del segnale:

- i messaggi di navigazione vengono protetti firmando digitalmente gran parte o tutti i dati che li compongono;
- lo *spreading code* viene punturato con dei marker di autenticazione ad uno specifico *duty factor* del 10%, allocati sul segnale *pilot* al fine di sfruttarne la maggior potenza disponibile (infatti, al *pilot signal* di L1 è assegnato il 75% della potenza, mentre al *data signal* il restante 25%).

Chimera firma digitalmente il segnale di navigazione con ECDSA (*Elliptic Curve Digital Signature Algorithm*) ed effettua una punturazione dello *spreading code* utilizzando una sequenza segreta di marker crittografici, derivati dalla firma digitale dei dati di navigazione attraverso un processo che include *hashing* crittografico¹ e crittografia simmetrica², che viene rivelata solo successivamente (tecnica conosciuta come SSSC, ossia *Spread Spectrum Security Code*).

¹In crittografia, con *hash* si intende una funzione non invertibile resistente alle collisioni che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza minore per cifrarne il contenuto.

²Tecnica di cifratura in cui la chiave di cifratura e quella di decifratura coincidono.

Il periodo di tempo tra l'esposizione del *ciphertext* e la rivelazione della chiave deve essere sufficiente a rendere inutile qualunque tentativo da parte di uno *spoofers* di utilizzare la suddetta chiave per generare un *ciphertext* plausibile; nel contesto di GPS, dove il valore del segnale a livello di navigazione dura molto poco, qualche secondo di latenza è sufficiente. Nonostante sia necessaria alla sicurezza del sistema, questa latenza crea un periodo di incertezza tra il momento in cui il ricevitore comincia a tracciare il SIS (*Signal In Space*) e il momento in cui la sua autenticità può essere verificata; durante gli intervalli di autenticazione, il ricevitore conserva dei campioni ADC (*Analog-to-Digital Converter*) del segnale ricevuto prima della loro elaborazione e, una volta ricevuta l'intera firma, genera una versione locale dello *spreading code* sicuro e la correla ai campioni conservati in memoria.

In Chimera, lo SSSC è introdotto in posizioni aleatorie mediante l'ausilio di una *look-up table* e punta ad aumentare la difficoltà di costruire un segnale falsificato, impedendo all'attaccante di conoscere a priori quali chip dello *spreading code* siano noti e quali invece dovranno essere stimati.

Poiché molti utenti avranno bisogno di un sistema di autenticazione che sia interamente contenuto nel segnale (al fine di fornire il servizio a ricevitori singoli o in gruppi isolati), è necessario distinguere due diverse formulazioni di Chimera a seconda che ci si trovi in presenza di uno *slow channel* (dove la velocità alla quale le chiavi potranno essere distribuite è limitata) o di un *fast channel* (in caso di velocità di distribuzione più elevata).

In entrambi i casi il design di Chimera prevede l'uso di un volto a generare protezioni crittografiche sia nei dati di navigazione, sia nello *spreading code*; il ricevitore dovrà quindi ricevere la chiave pubblica attraverso canali ausiliari circa una volta l'anno.

Slow channel

In presenza di un canale di questo tipo, il trasmettitore usa la chiave privata per firmare digitalmente parte del messaggio di navigazione e passa poi la firma digitale attraverso un algoritmo di *hashing* sicuro al fine di creare un *hash*, che viene successivamente utilizzato come chiave per la generazione dei marker.

Questa chiave da 256 bit è poi usata in un motore crittografico AES (*Advanced Encryption Standard*) che opera su frame da 128 bit del *plaintext* al fine di generare due sequenze randomiche separate di *ciphertext* utili alla generazione dei marker: una servirà per stabilirne il valore e l'altra per determinarne la posizione nella fase di punturazione dello *spreading code*. In [1] non è specificato in quale modalità venga utilizzato questo motore AES, ma supponiamo sia in *Counter mode* (CTR); questo tipo di utilizzo, infatti, tratta i frame ai quali viene applicato in modo indipendente, non permettendo il propagarsi di eventuali errori. Come riportato in [3], per garantire la sicurezza di questo metodo è necessario cambiare la chiave di crittazione ogni $2^{n/2}$ blocchi crittati, dove n è il numero di bit costituenti ciascun blocco; nel nostro caso la chiave viene cambiata ogni qual volta si generi una nuova firma digitale (ossia ogni 10 messaggi), quindi siamo largamente entro i limiti raccomandati. Possiamo quindi considerare l'output di AES indistinguibile da quello di una sorgente randomica di bit, che rende questo passaggio sicuro ai fini della nostra analisi.

In seguito alla ricezione dell'intera firma digitale, un utente partecipante sarà capace di autenticare il contenuto del messaggio di navigazione e derivare quindi i marker e la loro posizione per creare un segnale di riferimento per i marker; gli utenti non partecipanti possono ignorare la firma digitale e usare il contenuto del messaggio di navigazione come sempre.

Fast channel

In questo scenario, le chiavi per la generazione dei marker sono prodotte, firmate e distribuite attraverso canali non-SIS agli utenti. Questo approccio elimina il bisogno per gli utenti di demodulare i dati del messaggio di navigazione e apre la possibilità al cambiamento più rapido della chiave per la generazione dei marker; anche i dati di navigazione potrebbero essere firmati e trasmessi agli utenti fuori banda.

Sia in presenza di uno *slow channel*, sia di un *fast channel*, gli utenti devono salvare i campioni ADC non processati che ricevono per un periodo di tempo sufficiente a rivelare i marker in modo affidabile.

Il processo di autenticazione di Chimera rimane sicuro fino al momento in cui la chiave dei marker (o la base per generarla) è rivelata; il suo rilascio deve attendere fino alla fine del Chimera *epoch*, ossia fino alla fine dell'intero flusso di simboli che porta la trasmissione (o la ricezione) completa della firma digitale e dei suoi marker derivati. Nel caso dello *slow channel* è definito in termini di frame di dati (circa 10 messaggi di navigazione, ossia 180 secondi), mentre nel caso del *fast channel* è il periodo di tempo nel quale vale una certa chiave per i marker (circa 2 secondi).

Dopo la ricezione della firma digitale o della chiave per i marker firmata, l'utente verifica la firma usando il certificato pubblico; l'utente dello *slow channel* usa poi l'*hash* sicuro per derivare la chiave per i marker. Ogni utente replica successivamente gli step descritti in precedenza per derivare i valori e le posizioni dei marker e correla la sequenza di riferimento dei marker con i campioni ADC raccolti in precedenza. Se la firma e la correlazione sono verificate, il SIS abilitato per Chimera è autenticato.

Nella pagina seguente si possono osservare i due schemi di trasmissione e di ricezione di un Chimera *epoch*, in cui vengono messi a confronto i procedimenti per lo *slow channel* e per il *fast channel*.

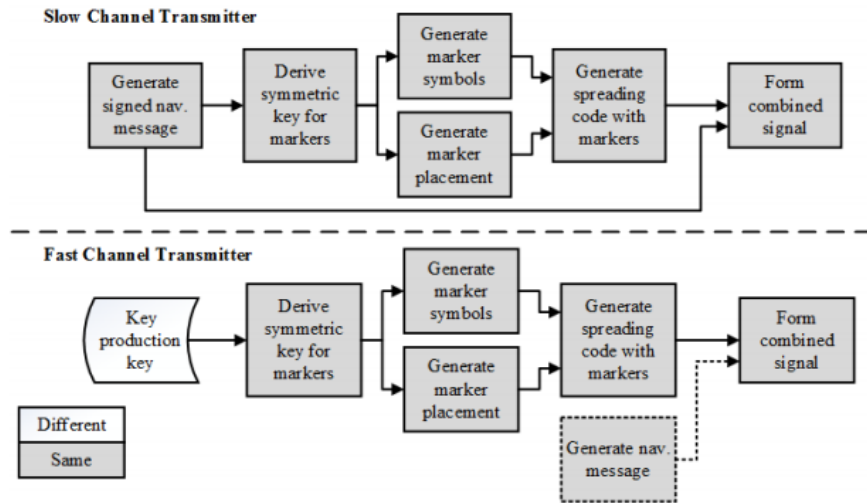


Figura 2: trasmissione di un Chimera epoch [1]

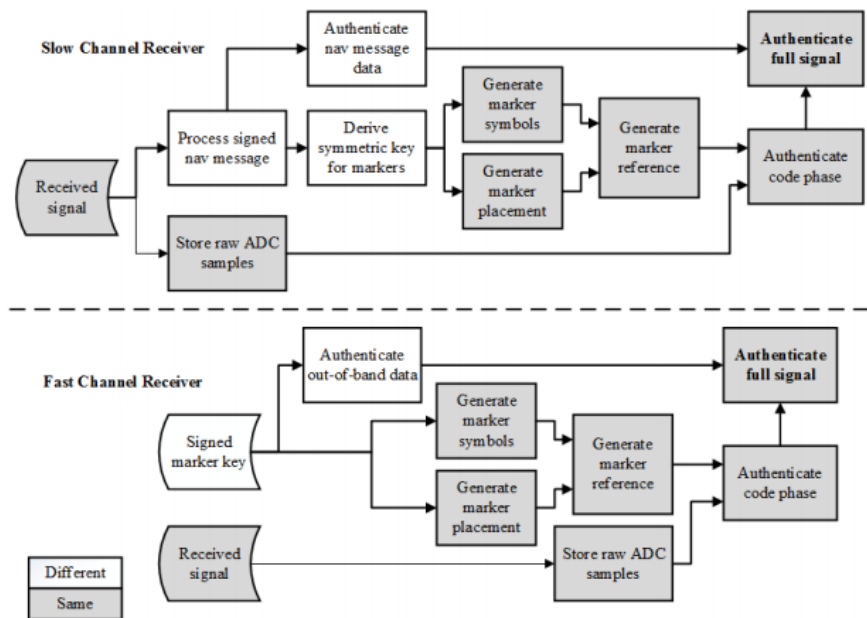


Figura 3: ricezione di un Chimera epoch [1]

Capitolo 3

Modello del sistema

Le specifiche SIS prevedono la divisione della sequenza dei 10230 chip dello *spreading code* in 310 segmenti da $L = 33$ chip ciascuno, detti *frame*, e stabiliscono inoltre che i chip nelle posizioni 0, 4, 6 e 29 di ciascun *frame* vengano modulati con BOC(6,1) e non possano essere quindi utilizzati per l'inserimento dei marker (lasciandone disponibili, quindi, solo 29)¹; dopo il processo di punturazione con i marker, chiameremo questi segmenti *marker frame*.

Questi *marker frame* vengono selezionati da una look-up table, ossia una matrice deterministica costituita da 512 righe e 33 colonne del tipo $M = \begin{bmatrix} M_3 \\ M_4 \end{bmatrix}$, dove le $r_3 = 256$ righe di M_3 sono scelte dall'insieme L_3 di tutte le possibili conformazioni dei marker frame contenenti 3 marker e analogamente le $r_4 = 256$ righe di M_4 dall'insieme L_4 relativo ai marker frame con 4 marker. La selezione del *marker frame* avviene sulla base di un pattern di 8 bit presi indipendentemente da ciascun segmento dell'output di AES.

Osserviamo che, dati 3 e 4 marker, questi possono essere distribuiti in $n = 29$ slot rispettivamente in $m_3 = \binom{29}{3} = 3654$ e in $m_4 = \binom{29}{4} = 23751$ modi diversi; di conseguenza, gli insiemi L_3 ed L_4 avranno cardinalità pari rispettivamente ad m_3 ed m_4 .

¹Questi quattro chip modulati con BOC(6,1) sono stati inseriti specificatamente per migliorare le proprietà di correlazione del segnale in presenza di *spreading code* [8] e per questo non possono essere modificati.

Non conoscendo la forma esplicita di M , né il procedimento mediante il quale viene costruita, ne utilizziamo un modello probabilistico al fine di mediare la performance del sistema su tutte le possibili costruzioni della suddetta matrice, andando a selezionare in modo casuale r_3 marker frame da 3 marker ed altrettanti r_4 da 4 rispettivamente dagli insiemi L_3 ed L_4 ; inoltre, volendo ottenere un *duty factor* del 10%, il sistema andrà a scegliere dalla nostra matrice nel 70% dei casi un marker frame da 3 marker e nel restante 30% dei casi un marker frame da 4 (valori ottenuti risolvendo per q_3 l'equazione $3 \cdot q_3 + 4 \cdot (1 - q_3) = 0.1 \cdot L$ e trovando che $q_3 = 0.7$ e $q_4 = 1 - q_3 = 0.3$).

La scelta di inserire 3 o 4 marker all'interno di un frame viene eseguita sulla base di una sequenza di 155 bit che non è ben chiaro da [1] se sia conosciuta o meno dall'attaccante al momento dell'attacco; per questo motivo nel resto della trattazione verranno presi in considerazione entrambi gli scenari.

A ciascuno dei k marker del frame selezionato viene poi assegnato in modo equiprobabile (sempre sulla base di una delle due sequenze di output di AES) il compito di andare a modificare o meno i chip dello *spreading code* in corrispondenza delle posizioni ricavate precedentemente.

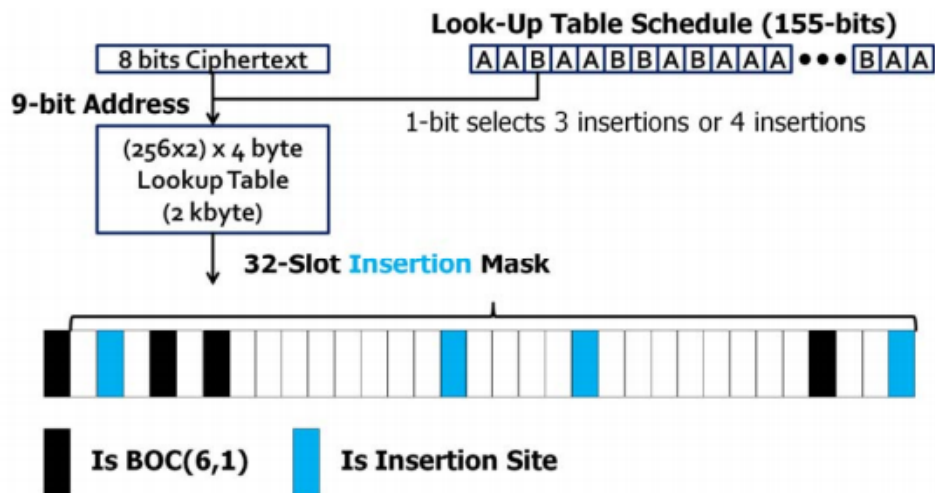


Figura 1: siti di inserimento dei marker [1]

Osserviamo che il ruolo di marker verrà assegnato in media a ciascun bit di M con una probabilità pari a $p = 1/10$ e, di conseguenza, il valore di ciascun bit dello *spreading code* verrà modificato, sempre in media, con probabilità $p/2 = 1/20$; andremo quindi anche a considerare uno scenario in cui non sia più presente la struttura della look-up table, ma dove si vadano a generare i frame considerando gli $n = 29$ bit che li compongono, e che sono disponibili per l'inserimento dei marker, come indipendenti ed identicamente distribuiti, assegnando a ciascuno di loro il ruolo di marker con probabilità pari a p . In questo modo potremo valutare se la presenza della look-up table contribuisca effettivamente a rendere più sicuro il sistema.

Introduciamo infine una breve notazione che sarà utile nel seguito della trattazione:

- \underline{c} : *spreading code* inalterato;
- \underline{c}' : *spreading code* punturato dal sistema;
- $\hat{\underline{c}}$: *spreading code* generato dall'attaccante;
- \underline{x} : posizioni dei marker nel segnale originale;
- $\hat{\underline{x}}$: posizioni dei marker generate dall'attaccante;
- \underline{d} : valori dei marker nel segnale originale;
- $\hat{\underline{d}}$: valori dei marker generati dall'attaccante;
- $w(\cdot)$: numero di marker in una data riga;

dove lo *spreading code* punturato \underline{c}' sarà ottenuto ponendo:

$$\begin{cases} c'_{x_i} = d_i, & i = 1, \dots, k \\ c'_y = c_y, & y \neq x_1, \dots, x_k \end{cases}$$

Capitolo 4

Modelli semplificati

Il problema alla base della formulazione di Chimera, con l'uso di una look-up table per identificare la posizione dei marker, è stato quello, partendo dalla sequenza binaria pubblicamente nota $\{c_\ell\}_{\ell=1,\dots,L}$, di trovare un'altra sequenza $\{c'_\ell\}_{\ell=1,\dots,L}$ in modo che:

- $\{c'_\ell\}$ fosse sufficientemente imprevedibile¹ anche a partire dalla conoscenza di $\{c_\ell\}$;
- $r_{cc'} = \sum_{\ell} (-1)^{c_\ell} (-1)^{c'_\ell} = \sum_{\ell} (-1)^{c_\ell + c'_\ell} \geq \rho r_{cc} = \rho \sum_{\ell} (-1)^{2c_\ell} = \rho L$, ossia si avesse una perdita di correlazione limitata.

Definiamo:

$$x_\ell := c_\ell \oplus c'_\ell = \begin{cases} 1, & c'_\ell \neq c_\ell \\ 0, & c'_\ell = c_\ell \end{cases}$$

e osserviamo che $r_{cc'} = L - 2 \sum_{\ell} x_\ell$; definendo $p := (1 - \rho)$, cerchiamo un vettore aleatorio \underline{x} imprevedibile in qualche senso da specificare successivamente, imponendo il vincolo che la correlazione sia rispettata in media, ovvero $\mathbb{E}[r_{cc'}] \geq \rho L$, da cui $\mathbb{E} \left[\sum_{\ell=1}^L x_\ell \right] \leq \frac{Lp}{2}$ (di cui, in seguito, considereremo l'uguaglianza).

¹Nella teoria dell'informazione, l'imprevedibilità di un segnale è misurata dall'*entropia*; all'aumentare dell'*entropia* della fonte, cresce l'imprevedibilità dei segnali emessi [4].

L'imprevedibilità di \underline{x} può essere misurata secondo diversi parametri, quali:

- il numero di possibili valori che può assumere, ossia la cardinalità del suo alfabeto $|\mathcal{A}_{\underline{x}}|$;
- la sua *entropia di Shannon* $\mathbb{H}(\underline{x}) = - \sum_{\alpha \in \mathcal{A}_{\underline{x}}} p_{\underline{x}}(\alpha) \log_2(p_{\underline{x}}(\alpha))$;
- la probabilità di collisione $P_{coll} = P[\underline{x} = \underline{x}']$, dove \underline{x} e \underline{x}' sono indipendenti ed identicamente distribuiti;
- la probabilità di essere indovinato con la migliore strategia possibile (o probabilità di *guessing*), ossia $P_{guess} = \max_{\alpha \in \mathcal{A}_{\underline{x}}} (p_{\underline{x}}(\alpha))$.

Tutti questi parametri possono essere messi in relazione con la cosiddetta *entropia di Rényi di ordine r* , definita come:

$$\mathbb{H}_r(\underline{x}) = \frac{1}{r-1} \log_{\frac{1}{2}} \left(\sum_{\alpha \in \mathcal{A}_{\underline{x}}} p_{\underline{x}}^r(\alpha) \right)$$

Al variare di r avremo:

- $\mathbb{H}_0(\underline{x}) = \log_2 |\mathcal{A}_{\underline{x}}|$;
- $\mathbb{H}_1(\underline{x})$, che coincide con l'*entropia di Shannon*;
- $\mathbb{H}_2(\underline{x}) = \log_{\frac{1}{2}}(P_{coll})$;
- $\mathbb{H}_{\infty}(\underline{x}) = \log_{\frac{1}{2}}(P_{guess})$.

L'*entropia di Rényi di ordine r* gode delle seguenti proprietà:

- per una stessa distribuzione, è funzione decrescente dell'ordine:
 $r \leq s \Rightarrow \mathbb{H}_r(\underline{x}) \geq \mathbb{H}_s(\underline{x})$;
- è nulla per distribuzioni degeneri (quasi certe) per qualsiasi ordine:
 $p_{\underline{x}}(\alpha) = 1 \Rightarrow \mathbb{H}_r(\underline{x}) = 0 \quad \forall r$;
- è massima e pari a $\log_2(M)$ per distribuzioni uniformi per qualsiasi ordine:
 $p_{\underline{x}}(\alpha) = \frac{1}{M} \quad \forall \alpha \Rightarrow \mathbb{H}_r(\underline{x}) = \log_2(M) \quad \forall r$;
- è additiva per variabili dipendenti per qualsiasi ordine: $\underline{x} = [x_1, \dots, x_n]$,
con gli x_{ℓ} indipendenti tra loro $\Rightarrow \mathbb{H}_r(\underline{x}) = \sum_{\ell=1}^L \mathbb{H}_r(x_{\ell}) \quad \forall r$.

4.1 Descrizione dei modelli

Andiamo ora a descrivere quattro modelli semplificati che imitano il meccanismo di Chimera, aventi distribuzioni analiticamente trattabili che soddisfano il vincolo $\mathbb{E} \left[\sum_{\ell=1}^L x_\ell \right] = \frac{Lp}{2}$ imposto precedentemente, e ricaviamo, per ciascuno di essi, l'espressione della loro *entropia di Rényi*.

Modello a bit indipendenti ed identicamente distribuiti

In questo modello tutti gli n bit componenti il frame e disponibili all'inserimento dei marker sono indipendenti tra loro ed identicamente distribuiti come $x_\ell \sim \mathcal{B}(\frac{p}{2})$, con $P[x_\ell = 1] = \frac{p}{2}$; avremo allora:

- $\mathbb{H}_0(\underline{x}) = \log_2 2^n = n$;
- $\mathbb{H}_1(\underline{x}) = \sum_{\ell=1}^n \mathbb{H}_1(x_\ell) = n \left(\frac{p}{2} \cdot \log_{\frac{1}{2}} \left(\frac{p}{2} \right) + \left(1 - \frac{p}{2} \right) \cdot \log_{\frac{1}{2}} \left(1 - \frac{p}{2} \right) \right)$;
- $\mathbb{H}_2(\underline{x}) = \sum_{\ell=1}^n \mathbb{H}_2(x_\ell) = n \cdot \log_{\frac{1}{2}} \left(\left(\frac{p}{2} \right)^2 + \left(1 - \frac{p}{2} \right)^2 \right)$;
- $\mathbb{H}_\infty(\underline{x}) = \sum_{\ell=1}^n \mathbb{H}_\infty(x_\ell) = n \cdot \log_{\frac{1}{2}} \left(1 - \frac{p}{2} \right)$.

Modello a marker fissati, dati indipendenti ed equiprobabili

In questo modello i marker si trovano in posizioni prestabilite all'interno del frame e possono assumere in modo indipendente ed equiprobabile il valore 1 o 0.

Sia $\mathcal{K} \subset \{1, \dots, n\}$ avente cardinalità $|\mathcal{K}| = k$ l'insieme delle posizioni prestabilite dei marker e sia

$$p_{x_\ell}(0) = \begin{cases} 1, & \ell \notin \mathcal{K} \\ \frac{1}{2}, & \ell \in \mathcal{K} \end{cases}$$

Avremo perciò $\mathbb{E} \left[\sum_{\ell=1}^L x_\ell \right] = \frac{k}{2}$, da cui, ricordando il vincolo $\mathbb{E} \left[\sum_{\ell=1}^L x_\ell \right] = \frac{Lp}{2}$ imposto in precedenza, possiamo ricavare $k = Lp$.

In questo caso, $\mathcal{A}_{\underline{x}} = \{\underline{\alpha} : \alpha_\ell = 0 \forall \ell \notin \mathcal{K}\}$ e \underline{x} è uniformemente distribuito su $\mathcal{A}_{\underline{x}}$, la cui cardinalità è 2^k ; avremo quindi, ricordando le proprietà dell'*entropia di Rényi*:

- $\mathbb{H}_0(\underline{x}) = \log_2 2^k = k$;
- $\mathbb{H}_1(\underline{x}) = \sum_{\ell=1}^k \mathbb{H}_1(x_\ell) = k \left(\frac{1}{2} \cdot \log_{\frac{1}{2}} \left(\frac{1}{2} \right) + \left(1 - \frac{1}{2} \right) \cdot \log_{\frac{1}{2}} \left(1 - \frac{1}{2} \right) \right) = k$;
- $\mathbb{H}_2(\underline{x}) = \sum_{\ell=1}^k \mathbb{H}_2(x_\ell) = k \cdot \log_{\frac{1}{2}} \left(\left(\frac{1}{2} \right)^2 + \left(1 - \frac{1}{2} \right)^2 \right) = k$;
- $\mathbb{H}_\infty(\underline{x}) = \sum_{\ell=1}^k \mathbb{H}_\infty(x_\ell) = k \cdot \log_{\frac{1}{2}} \left(1 - \frac{1}{2} \right) = k$.

Modello a marker uniformi in numero k fissato, dati fissati

In questo modello i k marker sono distribuiti uniformemente tra le n posizioni del frame disponibili per il loro inserimento e hanno tutti valore pari ad 1.

Ricordando il discorso fatto in precedenza riguardante il vincolo imposto sul valore atteso della somma degli x_ℓ , ricaviamo subito che $k = \frac{Lp}{2}$; inoltre, avremo $p_{\underline{x}}(\underline{\alpha}) = 1/\binom{n}{k} \forall \underline{\alpha} : \|\underline{\alpha}\|_H = k$, dove $\|\underline{\alpha}\|_H$ è il *peso di Hamming* di $\underline{\alpha}$, ossia il numero di bit uguali ad 1 che contiene.

Essendo gli $\underline{\alpha}$ equiprobabili e ricordando quanto detto in precedenza sulle proprietà dell'*entropia di Rényi*, avremo che:

- $\mathbb{H}_0(\underline{x}) = \log_2 \binom{n}{k}$;
- $\mathbb{H}_1(\underline{x}) = \mathbb{H}(\underline{x}) = \log_2 \binom{n}{k}$;
- $\mathbb{H}_2(\underline{x}) = \log_2 \binom{n}{k}$;
- $\mathbb{H}_\infty(\underline{x}) = \log_2 \binom{n}{k}$.

Modello a marker uniformi in numero k fissato, dati indipendenti ed equiprobabili

In questo modello i k marker sono distribuiti uniformemente all'interno delle n posizioni del frame disponibili per il loro inserimento e possono assumere in modo indipendente ed equiprobabile il valore 0 o 1.

Come in precedenza, avendo $\mathbb{E} \left[\sum_{\ell=1}^k x_\ell \right] = \frac{k}{2}$, possiamo ricavare che $k = Lp$.

Per trovare $p_{\underline{x}}(\underline{\alpha})$, osserviamo innanzitutto che $\binom{n}{k}$ è il numero delle diverse conformazioni che può assumere il frame contenente k marker e 2^k sono i diversi valori che possono assumere i marker al suo interno; consideriamo due casi in base al valore di $\|\underline{\alpha}\|_H$:

- $\|\underline{\alpha}\|_H = k$: l'evento $\{\underline{x} = \underline{\alpha}\}$ si può verificare solo se i k marker di \underline{x} sono esattamente nelle stesse posizioni dei bit uguali ad 1 di $\underline{\alpha}$ (che avviene con probabilità pari ad $1/\binom{n}{k}$) e se tutti i corrispondenti dati valgono 1 (che avviene con probabilità $1/2^k$);
- $\|\underline{\alpha}\|_H = h < k$: in questo caso, l'evento $\{\underline{x} = \underline{\alpha}\}$ si può verificare solo nel caso in cui h dei k marker di \underline{x} si trovino nelle stesse posizioni dei bit uguali ad 1 di $\underline{\alpha}$ (che avviene con probabilità pari ad $1/\binom{n}{h}$), se tutti i corrispondenti dati valgono 1 (che avviene con probabilità $1/2^h$) e se i rimanenti $k - h$ marker di \underline{x} , che possono disporsi in $\binom{n-h}{k-h}$ modi diversi, valgono tutti 0 (che avviene con probabilità $1/2^{(k-h)}$).

Essendo la scelta delle posizioni dei marker e dei loro valori due fenomeni indipendenti, possiamo semplicemente andare a moltiplicare i valori delle precedenti probabilità per ciascun caso, ottenendo così:

$$p_{\underline{x}}(\underline{\alpha}) = \begin{cases} \frac{1}{2^k} \frac{1}{\binom{n}{k}}, & \|\underline{\alpha}\|_H = k; \\ \frac{1}{2^h} \frac{\binom{n-h}{k-h}}{\binom{n}{k}} \frac{1}{2^{k-h}}, & \|\underline{\alpha}\|_H = h < k; \end{cases}$$

Andando a semplificare, possiamo osservare che diventerà:

$$p_{\underline{x}}(\underline{\alpha}) = \frac{\binom{n-h}{k-h}}{2^k \binom{n}{k}} =: q_h$$

dove $\|\underline{\alpha}\|_H = h \leq k$, da cui, ponendo $n_h := \binom{n}{h}$ il numero di vettori $\underline{\alpha}$ in $\mathcal{A}_{\underline{x}}$ con *peso di Hamming* uguale ad h :

- $\mathbb{H}_0(\underline{x}) = \log_2 |\mathcal{A}_{\underline{x}}| = \log_2 \left(\sum_{h=0}^k n_h \right)$;
- $\mathbb{H}_1(\underline{x}) = \mathbb{H}(\underline{x}) = - \sum_{\underline{\alpha} \in \mathcal{A}_{\underline{x}}} p_{\underline{x}}(\underline{\alpha}) \log_2(p_{\underline{x}}(\underline{\alpha})) = \sum_{h=0}^k \sum_{\underline{\alpha}: \|\underline{\alpha}\|_H=h} q_h \log_{\frac{1}{2}}(q_h) =$
 $= \sum_{h=0}^k n_h q_h \log_{\frac{1}{2}}(q_h)$;
- $\mathbb{H}_2(\underline{x}) = \log_{\frac{1}{2}} \left(\sum_{\underline{\alpha} \in \mathcal{A}_{\underline{x}}} p_{\underline{x}}^2(\underline{\alpha}) \right) = \log_{\frac{1}{2}} \left(\sum_{h=0}^k \sum_{\underline{\alpha}: \|\underline{\alpha}\|_H=h} q_h^2 \right) =$
 $= \log_{\frac{1}{2}} \left(\sum_{h=0}^k n_h q_h^2 \right)$;
- $\mathbb{H}_{\infty}(\underline{x}) = \log_{\frac{1}{2}}(q_0) = \log_{\frac{1}{2}} \left(\frac{1}{2^k} \right) = k$;

dove nell'ultimo punto possiamo osservare che il $\max_{\underline{\alpha}} p_{\underline{x}}(\underline{\alpha})$ è raggiunto per $h = 0$, ossia quando $\underline{\alpha}$ non contiene alcun 1.

Quest'ultimo modello è quello concettualmente più simile a Chimera e può essere usato come suo sostituto nel caso di calcoli particolarmente complessi, che vengono semplificati qui dall'assenza della struttura della look-up table.

4.2 Confronto dei modelli

Calcoliamo ora l'*entropia di Rényi* per i vari modelli elencati in precedenza, assegnando loro i parametri di Chimera; siano $L = 33, n = 29, p = 1/10$ e confrontiamoli elencandoli in una tabella.

Indichiamo con:

- "modello 1" il modello a bit indipendenti ed identicamente distribuiti;
- "modello 2" il modello a marker fissati, dati indipendenti ed equiprobabili;
- "modello 3" il modello a marker uniformi in numero k fissato, dati fissati;
- "modello 4" il modello a marker uniformi in numero k fissato, dati indipendenti ed equiprobabili.

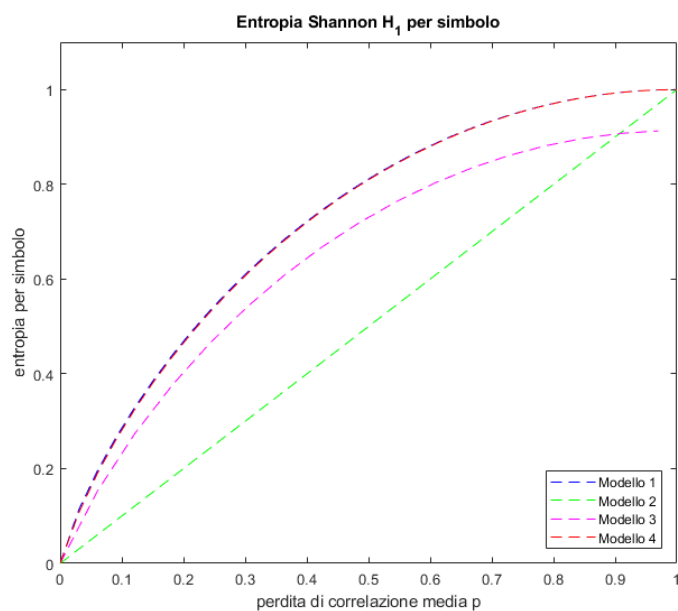
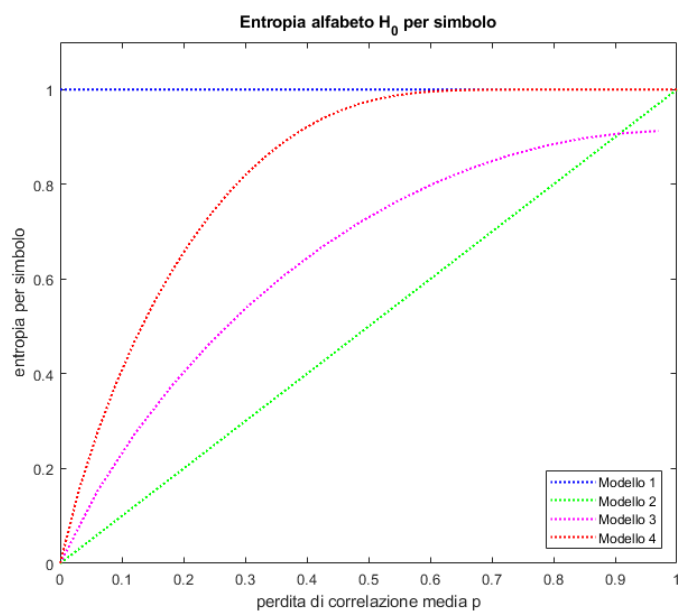
	Modello 1	Modello 2	Modello 3	Modello 4
\mathbb{H}_0	29	3.3	7.42	12
\mathbb{H}_1	4.34	3.3	7.42	8.77
\mathbb{H}_2	4.18	3.3	7.42	6.10
\mathbb{H}_∞	2.15	3.3	7.42	3.3

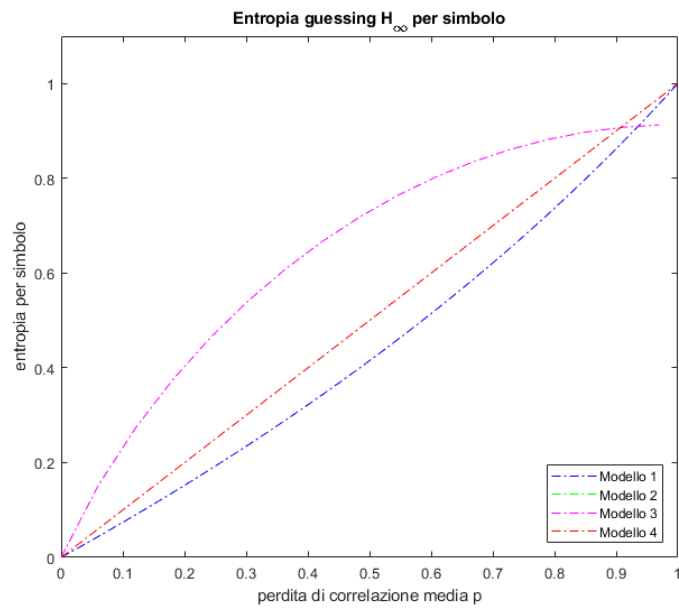
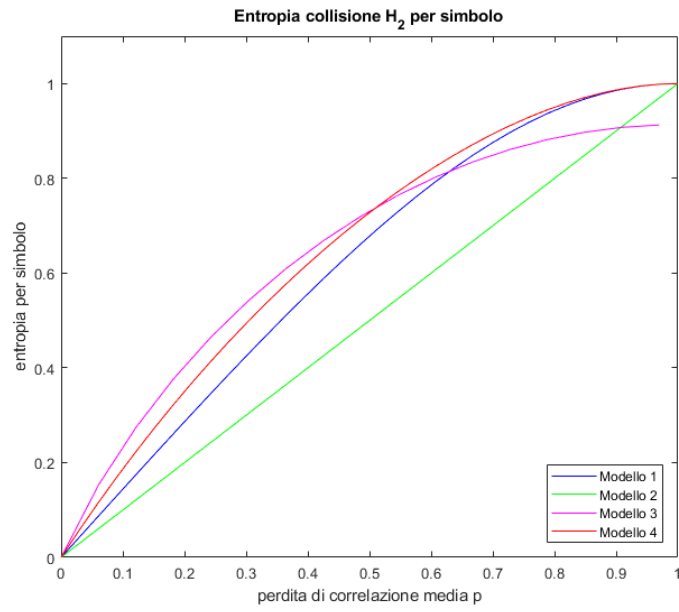
Da un primo confronto tra le entropie, il modello 3 (ossia quello a marker uniformi in numero fissato e dati fissati) risulta essere il migliore fra tutti.

In particolare, le caratteristiche che lo rendono più robusto rispetto al modello 4 (il più simile a Chimera) sono:

- \mathbb{H}_0 e \mathbb{H}_1 minori, ossia fornisce una rappresentazione più efficiente (richiedente meno bit) degli \underline{x} ;
- \mathbb{H}_2 e \mathbb{H}_∞ maggiori, ossia è più resistente a determinati tipi di attacchi.

Riportiamo in seguito i grafici delle quattro entropie prese in considerazione al variare di p e osserviamo che per $p = 1/10$ ritroviamo i risultati ricavati analiticamente:





Capitolo 5

Analisi degli attacchi

In questo capitolo, descriveremo ed analizzeremo tre possibili strategie di attacco a Chimera:

- nelle prime due, lo scopo dell'attaccante sarà quello di creare un frame punturato che sia indistinguibile da quello generato dal sistema nello stesso momento; in altre parole, possiamo riscrivere questo evento successo come

$$S = \{\hat{c} = \underline{c}'\};$$

- nella terza, l'attaccante, stimando i chip del frame inviato dal sistema fino ad una determinata posizione, punterà a ridurre il numero di righe plausibili della look-up table, assegnando a ciascuna di esse una certa probabilità di essere quella utilizzata dal sistema nel frame in esame.

Questi attacchi, oltre ad avere valenza di per sé, possono essere visti anche come un punto di partenza per (o come blocchi costituenti di) attacchi più sofisticati, indirizzati a ridurre la distinguibilità tra il segnale autentico e quello modificato in condizioni di canale rumoroso o disturbato.

Poiché, come annunciato nell'introduzione, da [1] non è ben chiaro se la sequenza di bit sulla base della quale viene effettuata la scelta di $k = 3$ o $k = 4$ per un particolare segmento sia nota o meno all'attaccante, andremo ad analizzare i tre tipi di attacchi in entrambi gli scenari.

5.1 Attacco 1: indovinare la sequenza di marker a partire dal primo intercettato

In questa sezione, consideriamo un attacco in cui l'avversario:

- 1) aspetta finché viene intercettato un marker (ossia viene rivelato un bit alterato nel segnale);
- 2) assume che questo sia il primo marker del frame;
- 3) indovina la possibile sequenza dei marker (sia le posizioni - tra le righe di M - che i valori).

Lo scopo dell'attaccante è quindi quello di indovinare tutte le posizioni e tutti i valori dei marker utilizzati dal sistema, partendo dal primo intercettato (che dovrà quindi modificare il chip dello *spreading code*) e assumendo che sia il primo del frame.

Vediamo innanzitutto che questo evento si verificherà 4 volte su 8 nel caso $k = 3$ e 8 volte su 16 nel caso $k = 4$; infatti, ad esempio, nel caso $k = 3$ i marker potranno trovarsi in 8 configurazioni diverse a seconda del valore che assumono e possiamo osservare che solo $\frac{1}{2} \cdot 8 = 4$ di queste avranno un marker modificato nella prima posizione.

Osserviamo inoltre che, sul totale delle m_k possibili righe contenenti k marker, $h_k^j = \binom{n-j}{k-1}$ di queste avranno il primo marker in una data posizione j ; infatti, essendo j la posizione in cui troviamo il primo marker, i rimanenti $k - 1$ marker potranno distribuirsi nelle $n - j$ posizioni del frame rimaste. Quindi, per descrivere statisticamente la variabile casuale R_k^j che indica quante righe della look-up table contenenti k marker avranno il primo marker nella stessa posizione j , ci basta osservare che questa segue una distribuzione ipergeometrica, poiché conta, per r_k elementi distinti estratti a caso in modo equiprobabile da un insieme L_k di cardinalità m_k , quanti sono nel sottoinsieme di cardinalità h_k^j (quello delle righe da k marker aventi il primo nella stessa posizione j).

Nel nostro caso questi valori saranno quindi:

k	3	4
r_k	256	256
m_k	3654	23751
h_k^j	$\binom{29-j}{2}$	$\binom{29-j}{3}$

L'evento successo per questo attacco rimarrà $S = \{\hat{c} = \underline{c}\}$, ma nel seguito ne andremo a considerare un sottoinsieme S' , la cui probabilità fungerà da *lower bound* per quella di S . Utilizzando la simbologia descritta finora, scriviamo dunque l'evento successo per questo attacco, che sarà

$$S' = \left\{ \hat{x} = \underline{x}, \hat{d} = \underline{d}, d_1 \neq c_{x_1} \right\}$$

Introduciamo un'ulteriore notazione, utile nel resto di questa sezione:

- R_k^j : numero di righe da k marker della look-up table aventi il primo marker nella stessa posizione j .

Numero di marker utilizzati noto all'attaccante

Andiamo qui a calcolare la probabilità dell'evento successo S' per questo attacco, assumendo che l'attaccante conosca il numero k di marker utilizzati dal sistema.

$$\begin{aligned}
P[S'] &= P[\hat{x} = \underline{x}, \hat{d} = \underline{d}, d_1 \neq c_{x_1}] = \\
&= \sum_{k=3}^4 P[\hat{x} = \underline{x}, \hat{d} = \underline{d} \mid w(\underline{x}) = k, d_1 \neq c_{x_1}] \cdot \\
&\quad \cdot P[w(\underline{x}) = k, d_1 \neq c_{x_1}] = \\
&= \sum_{k=3}^4 P[\hat{x} = \underline{x} \mid w(\underline{x}) = k] \cdot P[\hat{d} = \underline{d} \mid w(\underline{x}) = k, d_1 \neq c_{x_1}] \cdot \\
&\quad \cdot P[w(\underline{x}) = k, d_1 \neq c_{x_1}] = \\
&= \sum_{k=3}^4 P[\hat{x} = \underline{x} \mid w(\underline{x}) = k] \cdot P[\hat{d} = \underline{d} \mid w(\underline{x}) = k, d_1 \neq c_{x_1}] \cdot \\
&\quad \cdot P[d_1 \neq c_{x_1} \mid w(\underline{x}) = k] \cdot P[w(\underline{x}) = k]
\end{aligned}$$

dove:

- $P[w(\underline{x}) = k] = \begin{cases} q_3, & k = 3 \\ q_4, & k = 4 \end{cases}$ indica la probabilità di trovarci in una riga della look-up table contenente 3 o 4 marker;
- $P[d_1 \neq c_{x_1} | w(\underline{x}) = k] = \begin{cases} \frac{4}{8} = 0.5, & k = 3 \\ \frac{8}{16} = 0.5, & k = 4 \end{cases}$ indica la probabilità che il primo marker sia modificato, condizionatamente al fatto di trovarsi in una riga contenente 3 o 4 marker;
- $P[\hat{d} = \underline{d} | w(\underline{x}) = k, d_1 \neq c_{x_1}] = \left(\frac{1}{2}\right)^{k-1} = \begin{cases} \frac{1}{4} = 0.25, & k = 3 \\ \frac{1}{8} = 0.125, & k = 4 \end{cases}$ indica la probabilità di indovinare i valori corretti di tutti i marker sapendo di trovarsi in una riga che ne contiene k e che il primo è modificato;
- $P[\hat{x} = \underline{x} | w(\underline{x}) = k]$ indica la probabilità di indovinare le posizioni corrette di tutti i marker, sapendo di trovarsi in una riga che ne contiene k , ed è dato da:

$$\begin{aligned}
P[\hat{x} = \underline{x} | w(\underline{x}) = k] &= \sum_{\ell=1}^n P[\hat{x} = \underline{x} | w(\underline{x}) = k, x_1 = \ell] \cdot \\
&\quad \cdot P[x_1 = \ell | w(\underline{x}) = k] = \\
&= \sum_{\ell=1}^n \sum_N P[\hat{x} = \underline{x} | w(\underline{x}) = k, x_1 = \ell, R_k^\ell = N] \cdot \\
&\quad \cdot P[x_1 = \ell | w(\underline{x}) = k, R_k^\ell = N] \cdot \\
&\quad \cdot P[R_k^\ell = N | w(\underline{x}) = k] = \\
&= \sum_{\ell=1}^n \sum_N \frac{1}{N} \frac{N}{r_k} \frac{\binom{h_k^\ell}{N} \binom{m_k - h_k^\ell}{r_k - N}}{\binom{m_k}{r_k}} = \\
&= \frac{1}{r_k} \sum_{\ell=1}^n \sum_N \frac{\binom{h_k^\ell}{N} \binom{m_k - h_k^\ell}{r_k - N}}{\binom{m_k}{r_k}}
\end{aligned}$$

dove $N = 1, \dots, \min(r_k, \binom{n-\ell}{k-1})$ e ricordando che R_k^ℓ è una variabile che segue una distribuzione ipergeometrica.

Quindi, andando a sommare infine sui valori di k corrispondenti, avremo che:

$$\begin{aligned}
 P[S] \geq P[S'] &= \sum_{k=3}^4 P[S'_k] \cdot q_k = P[S'_3] \cdot q_3 + P[S'_4] \cdot q_4 = \\
 &= 0.09082 \cdot 0.25 \cdot 0.5 \cdot 0.7 + 0.07847 \cdot 0.125 \cdot 0.5 \cdot 0.3 = \\
 &= 9.42 \cdot 10^{-3}
 \end{aligned}$$

Numero di marker utilizzati sconosciuto all'attaccante

Consideriamo ora lo scenario in cui il numero k di marker utilizzati dal sistema non sia noto all'attaccante e calcoliamo la nuova probabilità dell'evento successo S' per questo attacco. Ora il condizionamento sul numero di marker della riga scelta dovrà avvenire, oltre che rispetto a quanto svolto dal sistema, anche rispetto a quanto svolto dall'attaccante; infatti, per avere successo, è fondamentale che il numero di marker scelto dai due sia identico.

$$\begin{aligned}
 P[S'] &= P[\hat{\underline{x}} = \underline{x}, \hat{\underline{d}} = \underline{d}, d_1 \neq c_{x_1}] = \\
 &= \sum_{k=3}^4 P[\hat{\underline{x}} = \underline{x}, \hat{\underline{d}} = \underline{d} \mid w(\underline{x}) = k, w(\hat{\underline{x}}) = k, d_1 \neq c_{x_1}] \cdot \\
 &\quad \cdot P[w(\underline{x}) = k, w(\hat{\underline{x}}) = k, d_1 \neq c_{x_1}] = \\
 &= \sum_{k=3}^4 P[\hat{\underline{x}} = \underline{x} \mid w(\underline{x}) = k, w(\hat{\underline{x}}) = k] \cdot \\
 &\quad \cdot P[\hat{\underline{d}} = \underline{d} \mid w(\underline{x}) = k, w(\hat{\underline{x}}) = k, d_1 \neq c_{x_1}] \cdot \\
 &\quad \cdot P[w(\underline{x}) = k, w(\hat{\underline{x}}) = k, d_1 \neq c_{x_1}] = \\
 &= \sum_{k=3}^4 P[\hat{\underline{x}} = \underline{x} \mid w(\underline{x}) = k, w(\hat{\underline{x}}) = k] \cdot \\
 &\quad \cdot P[\hat{\underline{d}} = \underline{d} \mid w(\underline{x}) = k, w(\hat{\underline{x}}) = k, d_1 \neq c_{x_1}] \cdot \\
 &\quad \cdot P[d_1 \neq c_{x_1} \mid w(\underline{x}) = k] \cdot P[w(\underline{x}) = k] \cdot P[w(\hat{\underline{x}}) = k]
 \end{aligned}$$

dove abbiamo introdotto un nuovo fattore rispetto allo scenario precedente, ossia:

- $P[w(\hat{x}) = k] = \begin{cases} q_3, & k = 3 \\ q_4, & k = 4 \end{cases}$ indica la probabilità che l'attaccante scelga un frame da una riga della look-up table contenente 3 o 4 marker.

In modo analogo al primo caso, i valori delle probabilità coinvolte rimarranno identici, l'unica cosa aggiuntiva da prendere in considerazione sarà la presenza del fattore appena descritto.

Avremo quindi, andando a sommare nuovamente sui valori di k corrispondenti:

$$\begin{aligned}
 P[S] \geq P[S'] &= \sum_{k=3}^4 P[S'_k] \cdot q_k \cdot q_k = \sum_{k=3}^4 P[S'_k] \cdot (q_k)^2 = \\
 &= 0.09082 \cdot 0.25 \cdot 0.5 \cdot (0.7)^2 + 0.07847 \cdot 0.125 \cdot 0.5 \cdot (0.3)^2 = \\
 &= 6 \cdot 10^{-3}
 \end{aligned}$$

5.2 Attacco 2: indovinare solo i marker intercettabili

Consideriamo ora un attacco in cui l'avversario generi casualmente un frame contenente k marker, analogamente a quanto svolto dal sistema, senza osservare alcun simbolo di \underline{c}' . Osserviamo che, se il frame originale ha un marker modificato nella posizione x_ℓ , l'attaccante, per avere successo, deve generarne uno a sua volta nella posizione \hat{x}_ℓ ; al contrario, nel caso in cui il valore del marker nel frame originale non modifichi il corrispondente chip dello *spreading code*, l'attaccante potrà o generarne a sua volta uno dello stesso tipo nella stessa posizione, oppure semplicemente non inserire alcun marker in quella posizione.

In questo caso, come nel precedente, l'evento successo rimarrà $S = \{\hat{c} = \underline{c}'\}$ e ne andremo a considerare due differenti versioni, a seconda del tipo di controllo eseguito dal ricevitore sui frame. Nel caso in cui la vittima controlli solamente i k valori nelle posizioni dei marker inseriti dal sistema, chiameremo l'evento successo S_1'' , mentre, se il controllo avverrà su tutti gli $n = 29$ bit che compongono il frame, l'evento successo sarà S_2'' , dove:

$$S_1'' = \bigcap_{\ell=1}^k \{\hat{c}_{x_\ell} = c'_{x_\ell}\} \quad S_2'' = \bigcap_{\ell=1}^n \{\hat{c}_\ell = c'_\ell\}$$

In particolare, nel caso di controllo da parte del ricevitore su tutti i 29 bit del frame, se l'attaccante posizionerà dei marker in posizioni diverse da quelle selezionate dal sistema, questi, per far sì che l'attacco abbia successo, non dovranno andare ad alterare i corrispondenti bit dello *spreading code*.

Nel seguito della trattazione, questi due eventi successo saranno riscritti in termini degli $x_\ell, d_\ell, \hat{x}_\ell, \hat{d}_\ell$ generati indipendentemente e con esplicita dipendenza da k .

Come nella sezione precedente, andiamo a distinguere i due casi in base al fatto che la sequenza per la scelta del numero di marker sia nota o meno all'attaccante.

Numero di marker utilizzati noto all'attaccante

Dato k il numero di marker utilizzati dal sistema noto anche all'attaccante, saranno:

$$(S_1'')_k = \bigcap_{\ell=1}^k \left[\left(\{d_\ell \neq c_{x_\ell}\} \cap \left(\bigcup_{\ell'=1}^k \left(\{\hat{x}_{\ell'} = x_\ell\} \cap \{\hat{d}_{\ell'} \neq c_{x_\ell}\} \right) \right) \right) \cup \right. \\ \left. \cup \left(\{d_\ell = c_{x_\ell}\} \cap \left(\bigcap_{\ell'=1}^k \left(\{\hat{x}_{\ell'} \neq x_\ell\} \cup \right. \right. \right. \right. \\ \left. \left. \left. \cup \left(\{\hat{x}_{\ell'} = x_\ell\} \cap \{\hat{d}_{\ell'} = c_{x_\ell}\} \right) \right) \right) \right) \right]$$

$$\begin{aligned}
(S_2'')_k = & \left\{ \bigcap_{\ell=1}^k \left[\left(\{d_\ell \neq c_{x_\ell}\} \cap \left(\bigcup_{\ell'=1}^k \left(\{\hat{x}_{\ell'} = x_\ell\} \cap \{\hat{d}_{\ell'} \neq c_{x_\ell}\} \right) \right) \right) \cup \right. \right. \\
& \left. \left. \cup \left(\{d_\ell = c_{x_\ell}\} \cap \left(\bigcap_{\ell'=1}^k \left(\{\hat{x}_{\ell'} \neq x_\ell\} \cup \right. \right. \right. \right. \right. \\
& \left. \left. \left. \left. \cup \left(\{\hat{x}_{\ell'} = x_\ell\} \cap \{\hat{d}_{\ell'} = c_{x_\ell}\} \right) \right) \right) \right] \right\} \cap \\
& \cap \left\{ \bigcap_{\ell'=1}^k \left[\left(\{\hat{d}_{\ell'} \neq c_{\hat{x}_{\ell'}}\} \cap \left(\bigcup_{\ell=1}^k \left(\{\hat{x}_{\ell'} = x_\ell\} \cap \{d_\ell \neq \hat{c}_{x_{\ell'}}\} \right) \right) \right) \cup \right. \right. \\
& \left. \left. \cup \left(\{\hat{d}_{\ell'} = c_{\hat{x}_{\ell'}}\} \cap \left(\bigcap_{\ell=1}^k \left(\{\hat{x}_{\ell'} \neq x_\ell\} \cup \right. \right. \right. \right. \right. \\
& \left. \left. \left. \left. \cup \left(\{\hat{x}_{\ell'} = x_\ell\} \cap \{d_\ell = \hat{c}_{\hat{x}_{\ell'}}\} \right) \right) \right) \right] \right\}
\end{aligned}$$

Andando a calcolare la probabilità di entrambi gli eventi condizionando rispetto al fatto di trovarsi di fronte ad un frame contenente 3 o 4 marker, otteniamo che:

$$P[S_i''] = \sum_{k=3}^4 P[(S_i'')_k \mid w(\underline{x}) = k] \cdot P[w(\underline{x}) = k]$$

dove $i = 1, 2$.

Nel seguito, la trattazione dettagliata sarà svolta solamente per S_1'' , ma vale in modo del tutto analogo per S_2'' .

Tornando alla precedente descrizione degli eventi successo, andiamo a rinominare i diversi fattori di S_1'' , al fine di facilitarne il calcolo:

- $a_\ell := \{d_\ell \neq c_{x_\ell}\};$
- $b_{\ell\ell'} := \{\hat{x}_{\ell'} = x_\ell\};$
- $c_\ell := \{\hat{d}_{\ell'} \neq c_{x_\ell}\};$
- $e_\ell := \{d_\ell = c_{x_\ell}\};$
- $f_{\ell\ell'} := \{\hat{x}_{\ell'} \neq x_\ell\};$
- $g_\ell := \{\hat{d}_{\ell'} = c_{x_\ell}\};$

e osserviamo che i primi tre eventi sono i complementari dei rispettivi ultimi tre, ossia $e_\ell = \bar{a}_\ell$, $f_{\ell\ell'} = \bar{b}_{\ell\ell'}$ e $g_\ell = \bar{c}_\ell$.

Possiamo quindi riscrivere:

$$(S_1'')_k = \bigcap_{\ell=1}^k \left[a_\ell \cap \left(\bigcup_{\ell'=1}^k (b_{\ell\ell'} \cap c_{\ell'}) \right) \cup \bar{a}_\ell \cap \bigcap_{\ell'=1}^k \left(\bar{b}_{\ell\ell'} \cup (b_{\ell\ell'} \cap \bar{c}_{\ell'}) \right) \right]$$

che, ad esempio nel caso $k = 3$, diventerà:

$$(S_1'')_3 = \bigcap_{\ell=1}^3 \left(a_\ell b_{\ell 1} c_1 \cup a_\ell b_{\ell 2} c_2 \cup a_\ell b_{\ell 3} c_3 \cup \bar{a}_\ell (\bar{b}_{\ell 1} \bar{b}_{\ell 2} \bar{b}_{\ell 3}) \cup \bar{a}_\ell b_{\ell 1} \bar{c}_1 \cup \right. \\ \left. \cup \bar{a}_\ell b_{\ell 2} \bar{c}_2 \cup \bar{a}_\ell b_{\ell 3} \bar{c}_3 \right)$$

Ora, andando a svolgere l'intersezione su ℓ , possiamo osservare che si presenteranno eventi successo con probabilità nulla, che dovranno essere rimossi dall'insieme di tutte le possibili combinazioni; inoltre, per ogni valore di t , sarà necessario rimuovere le varie ripetizioni di \bar{c}_t e, dalle combinazioni contenenti un $b_{\ell\ell'}$, andranno tolti anche tutti i $\bar{b}_{t\ell'}$ ¹.

La precedente operazione di rimozione è stata svolta al fine di ottenere tutti termini indipendenti tra loro, per poter così calcolare le probabilità di ogni combinazione svolgendo una semplice moltiplicazione ricordando che:

- $P[a_\ell] = 1/2$;
- $P[\bar{a}_\ell] = 1/2$;
- $P[b_{\ell\ell'}] = 1/29$;
- $P[\bar{b}_{\ell\ell'}] = 28/29$;
- $P[c_\ell] = 1/2$;
- $P[\bar{c}_\ell] = 1/2$.

Svolgendo lo stesso procedimento per il caso $k = 4$, otterremo che:

$$\begin{aligned}
 P[S_1''] &= \sum_{k=3}^4 P[(S_1'')_k] \cdot q_k = P[(S_1'')_3] \cdot q_3 + P[(S_1'')_4] \cdot q_4 = \\
 &= 1.28 \cdot 10^{-1} \cdot 0.7 + 6.57 \cdot 10^{-2} \cdot 0.3 = 1.09 \cdot 10^{-1}
 \end{aligned}$$

$$\begin{aligned}
 P[S_2''] &= \sum_{k=3}^4 P[(S_2'')_k] \cdot q_k = P[(S_2'')_3] \cdot q_3 + P[(S_2'')_4] \cdot q_4 = \\
 &= 2.11 \cdot 10^{-2} \cdot 0.7 + 6.66 \cdot 10^{-3} \cdot 0.3 = 1.68 \cdot 10^{-2}
 \end{aligned}$$

¹Per una lista completa di tutte le combinazioni valide, si veda l'appendice.

Numero di marker utilizzati sconosciuto all'attaccante

Consideriamo ora, come prima, lo scenario in cui il numero k di marker utilizzati dal sistema non sia noto all'attaccante e calcoliamo la probabilità dei nuovi eventi successo \hat{S}_1'' ed \hat{S}_2'' per questo attacco, dove j indica il numero di marker presenti nel frame generato dall'attaccante:

$$(\hat{S}_1'')_{k,j} = \bigcap_{\ell=1}^k \left[\left(\{d_\ell \neq c_{x_\ell}\} \cap \left(\bigcup_{\ell'=1}^j \left(\{\hat{x}_{\ell'} = x_\ell\} \cap \{\hat{d}_{\ell'} \neq c_{x_\ell}\} \right) \right) \right) \cup \right. \\ \left. \cup \left(\{d_{\ell'} = c_{x_\ell}\} \cap \left(\bigcap_{\ell'=1}^j \left(\{\hat{x}_{\ell'} \neq x_\ell\} \cup \right. \right. \right. \right. \\ \left. \left. \left. \cup \left(\{\hat{x}_{\ell'} = x_\ell\} \cap \{\hat{d}_{\ell'} = c_{x_\ell}\} \right) \right) \right) \right) \right]$$

$$(S_2'')_{k,j} = \left\{ \bigcap_{\ell=1}^k \left[\left(\{d_\ell \neq c_{x_\ell}\} \cap \left(\bigcup_{\ell'=1}^j \left(\{\hat{x}_{\ell'} = x_\ell\} \cap \{\hat{d}_{\ell'} \neq c_{x_\ell}\} \right) \right) \right) \cup \right. \right. \\ \left. \left. \cup \left(\{d_\ell = c_{x_\ell}\} \cap \left(\bigcap_{\ell'=1}^j \left(\{\hat{x}_{\ell'} \neq x_\ell\} \cup \right. \right. \right. \right. \right. \right. \\ \left. \left. \left. \left. \left. \cup \left(\{\hat{x}_{\ell'} = x_\ell\} \cap \{\hat{d}_{\ell'} = c_{x_\ell}\} \right) \right) \right) \right) \right) \right] \right\} \cap \\ \cap \left\{ \bigcap_{\ell'=1}^j \left[\left(\{\hat{d}_{\ell'} \neq c_{\hat{x}_{\ell'}}\} \cap \left(\bigcup_{\ell=1}^k \left(\{\hat{x}_{\ell'} = x_\ell\} \cap \{d_\ell \neq \hat{c}_{\hat{x}_{\ell'}}\} \right) \right) \right) \cup \right. \right. \\ \left. \left. \cup \left(\{\hat{d}_{\ell'} = c_{\hat{x}_{\ell'}}\} \cap \left(\bigcap_{\ell=1}^k \left(\{\hat{x}_{\ell'} \neq x_\ell\} \cup \right. \right. \right. \right. \right. \right. \\ \left. \left. \left. \left. \left. \cup \left(\{\hat{x}_{\ell'} = x_\ell\} \cap \{d_\ell = \hat{c}_{\hat{x}_{\ell'}}\} \right) \right) \right) \right) \right) \right] \right\}$$

Osserviamo che, perché questo tipo di attacco abbia successo, non è più necessario che il frame originale e quello generato dall'attaccante abbiano lo stesso numero di marker; la probabilità dei due eventi successo, ponendo gli adeguati condizionamenti, sarà data quindi da:

$$P[\hat{S}_i''] = \sum_{k=3}^4 P[w(\underline{x}) = k] \cdot \sum_{j=3}^4 P[w(\hat{x}) = j] \cdot P[(\hat{S}_i'')_{k,j} \mid w(\underline{x}) = k, w(\hat{x}) = j]$$

dove $i = 1, 2$.

Andiamo a procedere in modo analogo al caso in cui il numero di marker del frame originale era noto ² e otteniamo infine che:

$$\begin{aligned} P[\hat{S}_1''] &= \sum_{k=3}^4 q_k \cdot \sum_{j=3}^4 q_j \cdot P[(\hat{S}_1'')_{k,j}] = \\ &= q_3 \cdot (q_3 \cdot P[(\hat{S}_1'')_{3,3}] + q_4 \cdot P[(\hat{S}_1'')_{3,4}]) + \\ &\quad + q_4 \cdot (q_3 \cdot P[(\hat{S}_1'')_{4,3}] + q_4 \cdot P[(\hat{S}_1'')_{4,4}]) = \\ &= 0.7 \cdot (0.7 \cdot 1.28 \cdot 10^{-1} + 0.3 \cdot 1.29 \cdot 10^{-1}) + \\ &\quad + 0.3 \cdot (0.7 \cdot 6.45 \cdot 10^{-2} + 0.3 \cdot 6.57 \cdot 10^{-2}) = 1.09 \cdot 10^{-1} \end{aligned}$$

$$\begin{aligned} P[\hat{S}_2''] &= \sum_{k=3}^4 q_k \cdot \sum_{j=3}^4 q_j \cdot P[(\hat{S}_2'')_{k,j}] = \\ &= q_3 \cdot (q_3 \cdot P[(\hat{S}_2'')_{3,3}] + q_4 \cdot P[(\hat{S}_2'')_{3,4}]) + \\ &\quad + q_4 \cdot (q_3 \cdot P[(\hat{S}_2'')_{4,3}] + q_4 \cdot P[(\hat{S}_2'')_{4,4}]) = \\ &= 0.7 \cdot (0.7 \cdot 2.11 \cdot 10^{-2} + 0.3 \cdot 1.17 \cdot 10^{-2}) + \\ &\quad + 0.3 \cdot (0.7 \cdot 1.17 \cdot 10^{-2} + 0.3 \cdot 6.66 \cdot 10^{-3}) = 1.59 \cdot 10^{-2} \end{aligned}$$

²Come nel caso precedente, per una lista completa di tutte le combinazioni valide di eventi successo, si veda l'appendice.

5.3 Attacco 3: ridurre il numero di plausibili righe di M

In questa sezione consideriamo un attacco in cui, invece di puntare ad indovinare correttamente l'intera sequenza, l'attaccante, basandosi sull'osservazione del frame corrente, cerca di ridurre il più possibile la cardinalità del sottoinsieme di righe della look-up table contenente quella usata dal sistema, assegnando a ciascuna riga che lo compone la rispettiva probabilità di essere quella esatta.

L'attaccante quindi comincerà l'osservazione del frame del sistema e, sulla base di ogni chip stimato, sfoletterà la lista delle possibili righe della look-up table, che diventeranno mano a mano più o meno probabili; questo permetterebbe potenzialmente all'attaccante di stoppare la stima prima della fine del frame, aumentando la probabilità di successo dell'attacco a priori. Andiamo quindi ad analizzare dopo quanti chip stimati possiamo avere una probabilità significativa di indovinare la riga esatta della look-up table.

In questo caso si è proceduto solo per mezzo dello svolgimento di simulazioni, tralasciando il calcolo analitico in quanto in forma estremamente complessa e poco intuitiva; si sono stimati sia il numero medio di righe rimanenti nella look-up table in seguito allo sfolettamento effettuato dopo l'osservazione del frame fino ad una determinata posizione, sia la probabilità media assegnata alla riga usata dal sistema per ciascuna posizione analizzata.

In seguito è riportato il nucleo centrale in pseudocodice del programma utilizzato per svolgere le suddette simulazioni e, date una realizzazione della look-up table M e una del frame punturato dal sistema T , saranno:

- $M[i, j] = \begin{cases} 1, & \text{se la riga } i \text{ di } M \text{ ha un marker nella posizione } j \\ 0, & \text{altrimenti} \end{cases}$
- $T[j] = \begin{cases} 1, & \text{se il bit nella posizione } j \text{ di } T \text{ risulta modificato} \\ 0, & \text{altrimenti} \end{cases}$
- $p(i, j)$: probabilità che la riga i sia quella usata dal sistema, avendo osservato il frame fino alla posizione j .

Pseudocodice:

```
p(i,0) = 1/m, j = 1,...,m; //righe equiprobabili

for(i=1; i<n+1; i++) //iterazione sulle colonne
{
  for(j=1; j<m+1; j++) //iterazione sulle righe
  {
    if(T[j] == 1) // bit modificato nel frame
    {
      if(M[i,j] == 0) p(i,j) = 0;

      else if(M[i,j] == 1) p(i,j) = p(i,j-1);
    }

    else if(T[j] == 0) // bit non modificato nel frame
    {
      if(M[i,j] == 0) p(i,j) = p(i,j-1);

      else if(M[i,j] == 1) p(i,j) = p(i,j-1)/2;
    }
  }

  p(i,j) = p(i,j)/sum(p(:,j)); //normalizzazione
}
```

dove $n = 29$, $m = 256$ nel caso in cui il numero di marker utilizzato dal sistema sia noto all'attaccante e $m = 512$ nel caso contrario.

Spieghiamo qui brevemente il ragionamento effettuato per il calcolo di $p(i, j)$ prima di passare all'analisi dei risultati ottenuti:

- se nell'osservazione del frame si incontra un bit modificato in posizione j (ossia $T[j] = 1$) si può subito andare ad escludere dalla look-up table le righe non contenenti marker nella posizione j , mentre le rimanenti righe manterranno la stessa probabilità;
- se nell'osservazione del frame si incontra un bit non modificato in posizione j (ossia $T[j] = 0$), le righe della look-up table non contenenti un marker nella posizione j manterranno la stessa probabilità, mentre quella delle righe contenenti un marker in j si dimezzerà, poiché un marker potrebbe essere in seguito sia alterato che non alterato in modo equiprobabile.

Per ciascuna delle n posizioni sono state effettuate 1000 simulazioni (corrispondenti ad altrettante realizzazioni di M e T), delle quali riportiamo i risultati nel capitolo seguente.

Capitolo 6

Risultati

In questo capitolo andiamo ad analizzare e a confrontare i risultati ottenuti in precedenza, riportando anche quanto ottenuto da una serie di simulazioni svolte per ogni caso preso in considerazione.

6.1 Attacco 1

Come abbiamo visto nel capitolo precedente, la probabilità dell'evento successo S' di questo tipo di attacco è pari a:

- $P[S'] = 9.42 \cdot 10^{-3} = 0.94\%$ nel caso in cui la sequenza di bit sulla base della quale viene scelto il numero di marker da utilizzare sia nota all'attaccante;
- $P[S'] = 6 \cdot 10^{-3} = 0.6\%$ nel caso in cui, invece, non lo sia.

Dalle simulazioni svolte di questo tipo di attacco, i risultati ottenuti sono stati:

- 103 successi su 10000 prove per quanto riguarda il primo caso, ossia, in percentuale, 1.03%;
- 57 successi su 10000 prove nel secondo caso, ossia 0.57%.

Possiamo quindi osservare che le simulazioni hanno confermato quanto ottenuto dalla teoria.

6.2 Attacco 2

I risultati ottenuti nel capitolo precedente per questo tipo di attacco (sia nel caso di controllo da parte del ricevitore solo sulle posizioni dei marker del frame originale, sia nel caso di controllo su tutti i 29 bit del frame) sono stati:

- $P[S_1''] = 1.09 \cdot 10^{-1} = 10.9\%$ e $P[S_2''] = 1.68 \cdot 10^{-2} = 1.68\%$ nel caso in cui la sequenza per la scelta del numero di marker sia nota anche all'attaccante;
- $P[\hat{S}_1''] = 1.09 \cdot 10^{-1} = 10.9\%$ e $P[\hat{S}_2''] = 1.59 \cdot 10^{-2} = 1.59\%$ nel caso in cui non lo sia.

Dalle simulazioni si è ottenuto:

- 1087 successi su 10000 prove, ossia 10.87%, e 178 successi sempre su 10000 prove, ovvero 1.78%;
- 1077 successi su 10000 prove, ossia 10.77%, e 169 successi anche qui su 10000 prove, ovvero 1.69%.

Anche in questo caso, possiamo notare come le simulazioni abbiano confermato quanto ottenuto dalla teoria.

6.2.1 Varianti dell'attacco

La probabilità di successo di questo secondo attacco è stata valutata anche apportando delle modifiche al tipo di approccio utilizzato; vediamo quali.

L'attaccante genera un frame con tutti marker alterati

Con questa nuova tipologia di approccio, l'attaccante non va più a generare un frame assegnando casualmente e in modo equiprobabile a ciascuno dei marker il compito di modificare il corrispondente chip dello *spreading code* o meno, bensì li pone tutti in modo tale che vadano a cambiarlo, velocizzando così la generazione del frame; in altre, parole, riferendoci alla notazione della sezione 5.2, avremo che $P[c_\ell] = 1$ e, quindi, $P[\bar{c}_\ell] = 0$.

Le nuove probabilità di successo di questo tipo di attacco diventeranno quindi:

- $P[S_1''] = 1.09 \cdot 10^{-1} = 10.9\%$ e $P[S_2''] = 2.2 \cdot 10^{-5} = 0.0022\%$ nel caso di sequenza per numero di marker nota all'attaccante;
- $P[\hat{S}_1''] = 1.09 \cdot 10^{-1} = 10.9\%$ e $P[\hat{S}_2''] = 4.4 \cdot 10^{-5} = 0.0044\%$ nel caso di sequenza non nota.

Possiamo quindi osservare che, nel caso di controllo solamente sulle posizioni dei marker nel frame del sistema, la probabilità di successo resta invariata rispetto a quella della modalità di attacco originale, mentre, nel caso in cui il controllo avvenga su tutti i 29 bit, la probabilità di successo si abbassa notevolmente. Concludiamo quindi che è preferibile, per l'attaccante, rimanere fedeli alla modalità di attacco originale analizzata nella sezione 5.2.

L'attaccante genera tutti frame contenenti 3 marker

Con quest'altra modifica apportata all'attacco 2, vogliamo sfruttare il fatto che il sistema generi un frame contenente 3 marker nel 70% dei casi, mentre uno che ne contenga 4 solo nel rimanente 30%; andiamo ad applicare questo tipo di approccio al caso in cui non si conosca il numero k di marker utilizzati dal sistema.

Le nuove probabilità di successo diventeranno quindi:

- $P[\hat{S}_1''] = 1.09 \cdot 10^{-1} = 10.9\%$ nel caso di controllo solo sulle posizioni dei marker;
- $P[\hat{S}_2''] = 1.83 \cdot 10^{-2} = 1.83\%$ nel caso di controllo su tutti i 29 bit.

In questo caso possiamo osservare un leggero aumento della probabilità di successo rispetto alla modalità di attacco originale per quanto riguarda \hat{S}_2'' , mentre, nel caso di \hat{S}_1'' , rimane invariata.

6.2.2 Modello semplificato

In questa sezione andiamo a confrontare i risultati ottenuti per quanto riguarda l'attacco 2 nello scenario originale con quelli che andremo ad ottenere considerando il modello semplificato in cui eliminiamo la struttura della look-up table e costruiamo i frame considerandoli composti da $n = 29$ bit indipendenti ed identicamente distribuiti, con una probabilità di essere punteggiati da un marker pari a $p = 1/10$.

Osserviamo che, secondo questo nuovo modello, la variabile che descrive il numero di marker all'interno di un frame seguirà quindi una distribuzione binomiale $B(n, p)$.

Controllo sulle posizioni dei marker del frame originale

Consideriamo il caso in cui il ricevitore effettui il controllo solo sulle posizioni del frame in cui aveva inserito i marker e calcoliamo qual è la probabilità che un frame generato casualmente dall'attaccante coincida, in queste posizioni, con quello generato dal sistema.

Avremo quindi:

$$\begin{aligned} P[S_1''] &= \sum_{k=0}^n \binom{n}{k} p^k (1-p)^{(n-k)} \left[\frac{1}{2} \cdot p \cdot \frac{1}{2} + \frac{1}{2} \left(p \cdot \frac{1}{2} + (1-p) \right) \right]^k = \\ &= \sum_{k=0}^{29} \binom{n}{k} p^k (1-p)^{(n-k)} \left(\frac{1}{2} \right)^k = 2.26 \cdot 10^{-1} = 22.6\% \end{aligned}$$

Osserviamo che, nel caso in cui non vengano inseriti marker da parte del sistema (ossia $k = 0$), il ricevitore non effettuerà il controllo su alcun bit dello *spreading code*, quindi qualunque frame generato dall'attaccante porterà alla riuscita dell'attacco.

Anche in questo caso il risultato viene confermato dalle simulazioni, che restituiscono 2231 successi su un totale di 10000 prove (ossia 22.3%); inoltre, confrontando questo risultato con quello ottenuto in presenza della look-up table, possiamo osservare che quest'ultima consente di abbassare la probabilità di successo dell'attacco fino al 10.9%.

Controllo su tutti i bit del frame

Consideriamo invece ora il caso in cui il ricevitore effettui il controllo su tutti gli $n = 29$ bit del frame e vediamo qual è la probabilità che un frame generato casualmente dall'attaccante coincida perfettamente con quello generato dal sistema.

Ricordando che il numero di marker segue una distribuzione binomiale di parametri (n, p) e che i bit sono indipendenti ed identicamente distribuiti, avremo che:

$$\begin{aligned} P[S_2''] &= \left[\left(p \cdot \frac{1}{2} \right)^2 + \left((1-p) + p \cdot \frac{1}{2} \right)^2 \right]^n = \\ &= \left[\frac{p^2}{4} + \left(1 - \frac{p}{2} \right)^2 \right]^n = \left(\frac{p^2}{2} - p + 1 \right)^n = \\ &= (0.905)^{29} = 5.53 \cdot 10^{-2} = 5.53\% \end{aligned}$$

Questo risultato, confermato dalle simulazioni che ci restituiscono un numero di successi pari a 549 su un totale di 10000 prove (ovvero 5.49%), ci permette di osservare come la presenza della struttura della look-up table permetta di abbassare la probabilità di successo di questo tipo di attacco che, ricordiamo, essere pari ad 1.68% nel caso in cui il numero di marker utilizzati fosse noto all'attaccante e ad 1.59% nel caso contrario.

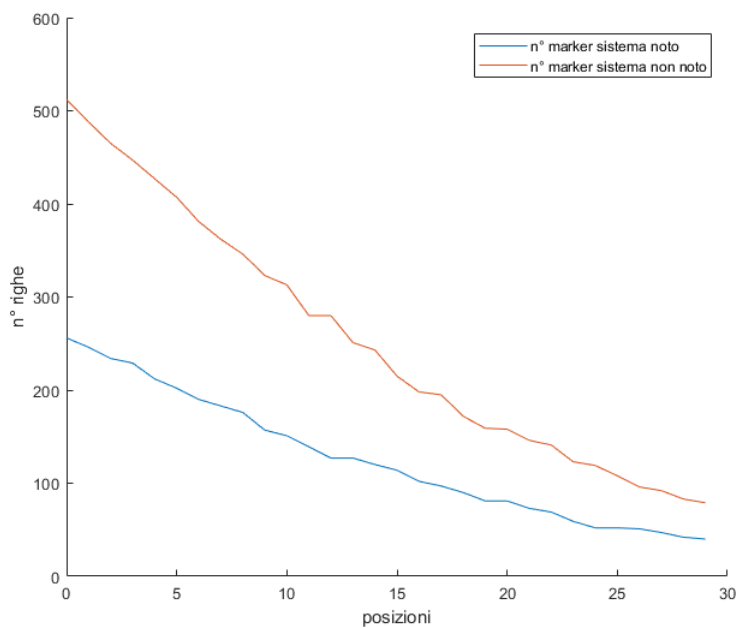
6.3 Attacco 3

In questa sezione riportiamo i dati ottenuti dalle 1000 simulazioni effettuate per questo tipo di attacco, elencandoli in due tabelle ed analizzandoli in altrettanti grafici; le due tabelle avranno la seguente struttura:

- **numero medio di righe plausibili**: indichiamo nella prima e nella quarta colonna la posizione fino alla quale il frame del sistema è stato osservato, nella seconda e nella quinta il numero di righe della look-up table rimanenti dopo l'osservazione nel caso in cui l'attaccante conosca il numero di marker utilizzati dal sistema, infine nella terza e nella sesta elenchiamo lo stesso numero di righe nel caso in cui l'attaccante non conosca però il numero di marker usati;
- **probabilità media riga esatta**: come nel caso del numero di righe, indichiamo nella prima e nella quarta colonna le posizioni, nella seconda e nella quinta i valori relativi al numero di marker noto, mentre nella terza e nella sesta quelli relativi al numero di marker sconosciuto.

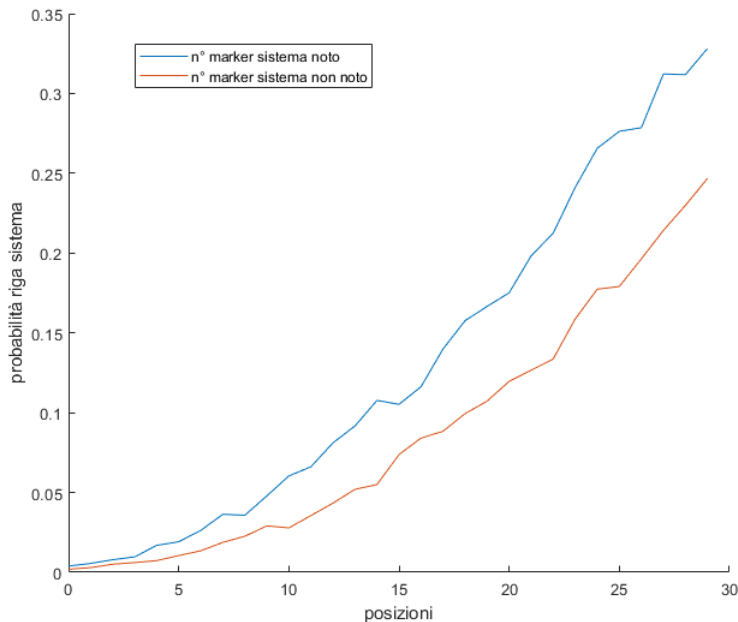
Numero medio di righe plausibili:

Posizione	Noto	Non noto	Posizione	Noto	Non noto
0	256	512	15	114	215
1	246	488	16	102	198
2	234	465	17	97	195
3	229	447	18	90	172
4	212	427	19	81	159
5	202	407	20	81	158
6	190	381	21	73	146
7	183	362	22	69	141
8	176	346	23	59	123
9	157	323	24	52	119
10	151	313	25	52	108
11	139	280	26	51	96
12	127	280	27	47	92
13	127	251	28	42	83
14	120	243	29	40	79



Probabilità media riga esatta:

Posizione	Nota	Non noto	Posizione	Nota	Non noto
0	0.00391	0.001953	15	0.10523	0.073726
1	0.00556	0.002928	16	0.11627	0.084110
2	0.00785	0.005045	17	0.13995	0.088377
3	0.00969	0.006091	18	0.15767	0.099441
4	0.01686	0.007333	19	0.16660	0.107271
5	0.01913	0.010475	20	0.17513	0.119631
6	0.02620	0.013493	21	0.19831	0.126600
7	0.03635	0.018735	22	0.21249	0.133690
8	0.03574	0.022597	23	0.24124	0.158797
9	0.04784	0.029062	24	0.26567	0.177382
10	0.06039	0.027835	25	0.27626	0.179090
11	0.06608	0.035527	26	0.27856	0.196385
12	0.08109	0.043320	27	0.31219	0.214205
13	0.09166	0.051971	28	0.31179	0.229880
14	0.10772	0.054380	29	0.32815	0.246731



Dall'osservazione di questi dati possiamo osservare che, già prima di aver stimato la metà dei bit del frame (in particolare il 41% nel caso di numero di marker noto e il 45% nel caso opposto), possiamo escludere con sicurezza metà delle righe della look-up table; proseguendo con la stima, possiamo arrivare ad escludere i 2/3 delle righe dopo aver stimato il 62% del frame in entrambi i casi e, infine, possiamo escludere i 3/4 delle righe dopo aver stimato il 76% del frame nel primo caso e il 79% nel secondo.

Inoltre, giunti a questo punto della stima, alla riga usata dal sistema saranno state assegnate probabilità piuttosto elevate e rispettivamente pari a 8%, 16% e 21% nel caso di numero di marker noto e a 5%, 10% e 13% nel caso contrario.

Confrontandolo con gli altri attacchi visti finora, l'attacco 3 risulta il più efficace sotto i seguenti vincoli:

- rispetto all'attacco 1, se si attende fino alla stima del 3° chip nel primo caso e fino al 4° nel secondo;

- rispetto all'attacco 2, se si attende fino alla stima del 16° chip nel primo caso e fino al 20° nel secondo se il ricevitore controlla solo le posizioni dei marker, se si attende fino alla stima del 4° chip nel primo caso e fino al 7° nel secondo se il ricevitore controlla tutti i 29 bit del frame;

dove con "primo caso" si intende quello in cui il numero di marker usati dal sistema sia noto e con "secondo caso" quello in cui non lo sia.

Nel contesto di questo attacco sono state svolte simulazioni anche per andare a valutare le probabilità di stimare correttamente le posizioni dei marker all'interno del frame osservandolo fino ad un certo numero di chip, ma hanno prodotto risultati non rilevanti ai fini della costruzione di un possibile attacco al sistema.

Capitolo 7

Conclusioni

Dall'analisi dei dati ottenuti relativamente allo studio di determinati tipi di attacchi a Chimera, e confrontandoli con quelli ottenuti lanciando i medesimi attacchi ad un sistema con lo stesso *duty factor* ma in assenza di *look-up table*, si può osservare che:

- nonostante la struttura della *look-up table* riduca notevolmente il numero di possibili conformazioni di marker frame a disposizione, non fa perdere sicurezza al sistema in modo rilevante;
- il fatto di avere dei marker in numero fissato permette di ridurre la probabilità di collisione e di guessing;
- queste probabilità si abbassano ulteriormente in presenza di un sistema in cui tutti i marker sono alterati.

Questi risultati, permettendoci di capire come questo sistema si comporti in un ambiente ideale, gettano le basi per una valutazione futura della sicurezza di Chimera in presenza di situazioni più verosimili di canali di trasmissione rumorosi e tempo-varianti.

Appendice

In quest'appendice sono elencate tutti i possibili eventi successo validi per l'attacco 2 al variare del numero k di marker del frame di sistema e del numero j di marker del frame generato dall'attaccante.

Per semplicità di notazione, si sono posti $a_i := a_i$, $b_{ii'} := b_{ii'}$, $c_i := c_i$, $A_i := \bar{a}_i$, $B_{ii'} := \bar{b}_{ii'}$ e $C_i := \bar{c}_i$ per ogni i .

Controllo solo sulle posizioni dei marker originali

• $k = 3, j = 3$

a1 b11 c1 a2 b22 c2 a3 b33 c3	a1 b12 c2 a2 b21 c1 a3 b33 c3	a1 b13 c3 a2 b21 c1 a3 b32 c2	A1 B13 a2 b21 c1 a3 b32 c2	A1 B11 B12 A2 B21 B22 a3 b33 c3
a1 b11 c1 a2 b22 c2 A3 B33	a1 b12 c2 a2 b21 c1 A3 B33	a1 b13 c3 a2 b21 c1 A3 B32	A1 B12 a2 b21 c1 a3 b33 c3	A1 B11 B12 B13 A2 B21 B22 B23 A3 B31
a1 b11 c1 a2 b22 c2 A3 b33 C3	a1 b12 c2 a2 b21 c1 A3 b33 C3	a1 b13 c3 a2 b21 c1 A3 b32 C2	A1 B12 B13 a2 b21 c1 A3 B32 B33	B32 B33 A1 B12 B13 A2 B22
a1 b11 c1 a2 b23 c3 a3 b32 c2	a1 b12 c2 a2 b23 c3 a3 b31 c1	a1 b13 c3 a2 b22 c2 a3 b31 c1	A1 B13 a2 b21 c1 A3 b32 C2	B23 A3 b31 C1 A1 B11 B13 A2 B21
a1 b11 c1 a2 b23 c3 A3 B32	a1 b12 c2 a2 b23 c3 A3 B31	a1 b13 c3 a2 b22 c2 A3 B31	A1 B12 a2 b21 c1 A3 b33 C3	B23 A3 b32 C2 A1 B11 B12 A2 B21
a1 b11 c1 a2 b23 c3 A3 b32 C2	a1 b12 c2 a2 b23 c3 A3 b31 C1	a1 b13 c3 a2 b22 c2 A3 b31 C1	A1 B13 a2 b22 c2 a3 b31 c1	A1 B12 A2 b21 C1 a3 b32 c2
a1 b11 c1 A2 B23 a3 b32 c2	a1 b12 c2 A2 B23 a3 b31 c1	a1 b13 c3 A2 B22 a3 b31 c1	A1 B11 a2 b22 c2 a3 b33 c3	A1 B12 A2 b21 C1 a3 b33 c3
a1 b11 c1 A2 B22 a3 b33 c3	a1 b12 c2 A2 B21 a3 b33 c3	a1 b13 c3 A2 B21 a3 b32 c2	A1 B11 B13 a2 b22 c2 A3 B31 B33	A1 B12 B13 A2 b21 C1 A3 B32 B33
a1 b11 c1 A2 B22 B23 A3 B32 B33	a1 b12 c2 A2 B23 A3 B31 B33	a1 b13 c3 A2 B21 B22 A3 B31 B32	A1 B13 a2 b22 c2 A3 b31 C1	A1 B13 A2 b21 C1 A3 b32 C2
a1 b11 c1 A2 B23 A3 b32 C2	a1 b12 c2 A2 B23 A3 b31 C1	a1 b13 c3 A2 B22 A3 b31 C1	A1 B11 a2 b22 c2 A3 b33 C3	A1 B12 A2 b21 C1 A3 b33 C3
a1 b11 c1 A2 B22 A3 b33 C3	a1 b12 c2 A2 B21 A3 b33 C3	a1 b13 c3 A2 B21 A3 b32 C2	A1 B12 a2 b23 c3 a3 b31 c1	A1 B13 A2 b22 C2 a3 b31 c1
a1 b11 c1 A2 b22 C2 a3 b33 c3	a1 b12 c2 A2 b21 C1 a3 b33 c3	a1 b13 c3 A2 b21 C1 a3 b32 c2	A1 B11 a2 b23 c3 a3 b32 c2	A1 B11 A2 b22 C2 a3 b33 c3
a1 b11 c1 A2 b22 C2 A3 B33	a1 b12 c2 A2 b21 C1 A3 B33	a1 b13 c3 A2 b21 C1 A3 B32	A1 B11 B12 a2 b23 c3 A3 B31 B32	A1 B11 B13 A2 b22 C2 A3 B31 B33
a1 b11 c1 A2 b22 C2 A3 b33 C3	a1 b12 c2 A2 b21 C1 A3 b33 C3	a1 b13 c3 A2 b21 C1 A3 b32 C2	A1 B12 a2 b23 c3 A3 b31 C1	A1 B13 A2 b22 C2 A3 b31 C1
a1 b11 c1 A2 b23 C3 a3 b32 c2	a1 b12 c2 A2 b23 C3 a3 b31 c1	a1 b13 c3 A2 b22 C2 a3 b31 c1	A1 B11 a2 b23 c3 A3 b32 C2	A1 B12 A2 b22 C2 A3 b33 C3
a1 b11 c1 A2 b23 C3 A3 B32	a1 b12 c2 A2 b23 C3 A3 B31	a1 b13 c3 A2 b22 C2 A3 B31	A1 B12 B13 A2 B22 B23 a3 b31 c1	A1 B12 A2 b23 C3 a3 b31 c1
a1 b11 c1 A2 b23 C3 A3 b32 C2	a1 b12 c2 A2 b23 C3 A3 b31 C1	a1 b13 c3 A2 b22 C2 A3 b31 C1	A1 B11 B13 A2 B21 B23 a3 b32 c2	A1 B11 A2 b23 C3 a3

b32 c2	b33 c3	A3 B33	A3 B33	b31 c1
A1 B11 B12 A2 b23	A1 b11 C1 A2 B22	A1 b12 C2 a2 b21 c1	A1 b12 C2 A2 b21 C1	A1 b13 C3 A2 B21 a3
C3 A3 B31 B32	B23 A3 B32 B33	A3 b33 C3	A3 b33 C3	b32 c2
A1 B12 A2 b23 C3 A3	A1 b11 C1 A2 B23 A3	A1 b12 C2 a2 b23 c3	A1 b12 C2 A2 b23 C3	A1 b13 C3 A2 B21 B22
b31 C1	b32 C2	a3 b31 c1	a3 b31 c1	A3 B31 B32
A1 B11 A2 b23 C3 A3	A1 b11 C1 A2 B22 A3	A1 b12 C2 a2 b23 c3	A1 b12 C2 A2 b23 C3	A1 b13 C3 A2 B22 A3
b32 C2	b33 C3	A3 B31	A3 B31	b31 C1
A1 b11 C1 a2 b22 c2	A1 b11 C1 A2 b22 C2	A1 b12 C2 a2 b23 c3	A1 b12 C2 A2 b23 C3	A1 b13 C3 A2 B21 A3
a3 b33 c3	a3 b33 c3	A3 b31 C1	A3 b31 C1	b32 C2
A1 b11 C1 a2 b22 c2	A1 b11 C1 A2 b22 C2	A1 b12 C2 A2 B23 a3	A1 b13 C3 a2 b21 c1	A1 b13 C3 A2 b21 C1
A3 B33	A3 B33	b31 c1	a3 b32 c2	a3 b32 c2
A1 b11 C1 a2 b22 c2	A1 b11 C1 A2 b22 C2	A1 b12 C2 A2 B21 a3	A1 b13 C3 a2 b21 c1	A1 b13 C3 A2 b21 C1
A3 b33 C3	A3 b33 C3	b33 c3	A3 B32	A3 B32
A1 b11 C1 a2 b23 c3	A1 b11 C1 A2 b23 C3	A1 b12 C2 A2 B21	A1 b13 C3 a2 b21 c1	A1 b13 C3 A2 b21 C1
a3 b32 c2	a3 b32 c2	B23 A3 B33	A3 b32 C2	A3 b32 C2
A1 b11 C1 a2 b23 c3	A1 b11 C1 A2 b23 C3	A1 b12 C2 A2 B23 A3	A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 b22 C2
A3 B32	A3 B32	b31 C1	a3 b31 c1	a3 b31 c1
A1 b11 C1 a2 b23 c3	A1 b11 C1 A2 b23 C3	A1 b12 C2 A2 B21 A3	A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 b22 C2
A3 b32 C2	A3 b32 C2	b33 C3	A3 B31	A3 B31
A1 b11 C1 A2 B23 a3	A1 b12 C2 a2 b21 c1	A1 b12 C2 A2 b21 C1	A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 b22 C2
b32 c2	a3 b33 c3	a3 b33 c3	A3 b31 C1	A3 b31 C1
A1 b11 C1 A2 B22 a3	A1 b12 C2 a2 b21 c1	A1 b12 C2 A2 b21 C1	A1 b13 C3 A2 B22 a3	

• $k = 3, j = 4$

a1 b11 c1 a2 b22 c2 a3	a3 b34 c4	a1 b12 c2 a2 b24 c4 a3	a3 b33 c3	a1 b13 c3 A2 B21 B24
b33 c3 C4	a1 b11 c1 A2 b22 C2	b31 c1	a1 b12 c2 A2 b24 C4	A3 b32 C2
a1 b11 c1 a2 b22 c2 a3	A3 B33 B34	a1 b12 c2 a2 b24 c4 a3	A3 B31 B33	a1 b13 c3 A2 B21 B22
b34 c4 c3	a1 b11 c1 A2 b22 C2	b33 c3	a1 b12 c2 A2 b24 C4	A3 b34 C4
a1 b11 c1 a2 b22 c2	A3 b33 C3	a1 b12 c2 a2 b24 c4	A3 b31 C1	a1 b13 c3 A2 b21 C1
A3 B33 B34	a1 b11 c1 A2 b22 C2	A3 B31 B33	a1 b12 c2 A2 b24 C4	a3 b32 c2
a1 b11 c1 a2 b22 c2	A3 b34 C4	a1 b12 c2 a2 b24 c4	A3 b33 C3	a1 b13 c3 A2 b21 C1
A3 b33 C3 C4	a1 b11 c1 A2 b23 C3	A3 b31 C1	a1 b12 c2 a2 b24 c4	a3 b34 c4
a1 b11 c1 a2 b22 c2	a3 b32 c2	a1 b12 c2 A2 B23 B24	b32 c2	a1 b13 c3 A2 b21 C1
A3 b34 C4 C3	a1 b11 c1 A2 b23 C3	A3 b33 C3	a1 b13 c3 a2 b21 c1 a3	A3 B32 B34
a1 b11 c1 a2 b23 c3 a3	a3 b34 c4	a1 b12 c2 A2 B23 B24	b34 c4	a1 b13 c3 A2 b21 C1
b32 c2 C4	a1 b11 c1 A2 b23 C3	a3 b31 c1	a1 b13 c3 a2 b21 c1	A3 b32 C2
a1 b11 c1 a2 b23 c3 a3	A3 B32 B34	a1 b12 c2 A2 B21 B24	A3 B32 B34	a1 b13 c3 A2 b21 C1
b34 c4 C2	a1 b11 c1 A2 b23 C3	a3 b33 c3	a1 b13 c3 a2 b21 c1	A3 b34 C4
a1 b11 c1 a2 b23 c3	A3 b32 C2	a1 b12 c2 A2 B21 B23	A3 b32 C2	a1 b13 c3 A2 b22 C2
A3 B32 B34	a1 b11 c1 A2 b23 C3	a3 b34 c4	a1 b13 c3 a2 b21 c1	a3 b31 c1
a1 b11 c1 a2 b23 c3	A3 b34 C4	a1 b12 c2 A2 B21 B23	A3 b34 C4	a1 b13 c3 A2 b22 C2
A3 b32 C2	a1 b11 c1 A2 b24 C4	B24 A3 B31 B33 B34	a1 b13 c3 a2 b22 c2 a3	a3 b34 c4
a1 b11 c1 a2 b23 c3	a3 b32 c2	a1 b12 c2 A2 B23 B24	b31 c1	a1 b13 c3 A2 b22 C2
A3 b34 C4	a1 b11 c1 A2 b24 C4	A3 b31 C1	a1 b13 c3 a2 b22 c2 a3	A3 B31 B34
a1 b11 c1 a2 b24 c4 a3	a3 b33 c3	a1 b12 c2 A2 B21 B24	b34 c4	a1 b13 c3 A2 b22 C2
b32 c2	a1 b11 c1 A2 b24 C4	A3 b33 C3	a1 b13 c3 a2 b22 c2	A3 b31 C1
a1 b11 c1 a2 b24 c4 a3	A3 B32 B33	a1 b12 c2 A2 B21 B23	A3 B31 B34	a1 b13 c3 A2 b22 C2
b33 c3	a1 b11 c1 A2 b24 C4	A3 b34 C4	a1 b13 c3 a2 b22 c2	A3 b34 C4
a1 b11 c1 a2 b24 c4	A3 b32 C2	a1 b12 c2 A2 b21 C1	A3 b31 C1	a1 b13 c3 A2 b24 C4
A3 B32 B33	a1 b11 c1 A2 b24 C4	a3 b33 c3	a1 b13 c3 a2 b22 c2	a3 b31 c1
a1 b11 c1 a2 b24 c4	A3 b33 C3	a1 b12 c2 A2 b21 C1	A3 b34 C4	a1 b13 c3 A2 b24 C4
A3 b32 C2	a1 b12 c2 a2 b21 c1 a3	a3 b34 c4	a1 b13 c3 a2 b24 c4 a3	a3 b32 c2
a1 b11 c1 a2 b24 c4	b33 c3	a1 b12 c2 A2 b21 C1	b31 c1	a1 b13 c3 A2 b24 C4
A3 b33 C3	a1 b12 c2 a2 b21 c1 a3	A3 B33 B34	a1 b13 c3 a2 b24 c4 a3	A3 B31 B32
a1 b11 c1 A2 B23 B24	b34 c4	a1 b12 c2 A2 b21 C1	b32 c2	a1 b13 c3 A2 b24 C4
a3 b32 c2	a1 b12 c2 a2 b21 c1	A3 b33 C3	a1 b13 c3 a2 b24 c4	A3 b31 C1
a1 b11 c1 A2 B22 B24	A3 B33 B34	a1 b12 c2 A2 b21 C1	A3 B31 B32	a1 b13 c3 A2 b24 C4
a3 b33 c3	a1 b12 c2 a2 b21 c1	A3 b34 C4	a1 b13 c3 a2 b24 c4	A3 b32 C2
a1 b11 c1 A2 B22 B23	A3 b33 C3	a1 b12 c2 A2 b23 C3	A3 b31 C1	a1 b14 c4 a2 b21 c1 a3
a3 b34 c4	a1 b12 c2 a2 b21 c1	a3 b31 c1	a1 b13 c3 a2 b24 c4	b32 c2
a1 b11 c1 A2 B22 B23	A3 b34 C4	a1 b12 c2 A2 b23 C3	A3 b32 C2	a1 b14 c4 a2 b21 c1 a3
B24 A3 B32 B33 B34	a1 b12 c2 a2 b23 c3 a3	a3 b34 c4	a1 b13 c3 A2 B22 B24	b33 c3
a1 b11 c1 A2 B23 B24	b31 c1	a1 b12 c2 A2 b23 C3	a3 b31 c1	a1 b14 c4 a2 b21 c1
A3 b32 C2	a1 b12 c2 a2 b23 c3 a3	A3 B31 B34	a1 b13 c3 A2 B21 B24	A3 B32 B33
a1 b11 c1 A2 B22 B24	b34 c4	a1 b12 c2 A2 b23 C3	a3 b32 c2	a1 b14 c4 a2 b21 c1
A3 b33 C3	a1 b12 c2 a2 b23 c3	A3 b31 C1	a1 b13 c3 A2 B21 B22	A3 b32 C2
a1 b11 c1 A2 B22 B23	A3 B31 B34	a1 b12 c2 A2 b23 C3	a3 b34 c4	a1 b14 c4 a2 b21 c1
A3 b34 C4	a1 b12 c2 a2 b23 c3	A3 b34 C4	a1 b13 c3 A2 B21 B22	A3 b33 C3
a1 b11 c1 A2 b22 C2	A3 b31 C1	B24 A3 B31 B32 B34	a1 b13 c3 A2 B22 B24	a1 b14 c4 a2 b22 c2 a3
a3 b33 c3	a1 b12 c2 a2 b23 c3	a3 b31 c1	a1 b13 c3 A2 B22 B24	b31 c1
a1 b11 c1 A2 b22 C2	A3 b34 C4	a1 b12 c2 A2 b24 C4	A3 b31 C1	a1 b14 c4 a2 b22 c2 a3

b33 c3	a3 b31 c1	A1 B12 B13 B14 A2	a3 b33 c3	A3 B31 B33
a1 b14 c4 a2 b22 c2	A1 B11 B14 a2 b22 c2	b21 C1 A3 B32 B33	A1 b11 C1 a2 b24 c4	A1 b12 C2 a2 b24 c4
A3 B31 B33	a3 b33 c3	B34	A3 B32 B33	A3 b31 C1
a1 b14 c4 a2 b22 c2	A1 B11 B13 a2 b22 c2	A1 B13 B14 A2 b21	A1 b11 C1 a2 b24 c4	A1 b12 C2 a2 b24 c4
A3 b31 C1	a3 b34 c4	C1 A3 b32 C2	A3 b32 C2	A3 b33 C3
a1 b14 c4 a2 b22 c2	A1 B11 B13 B14 a2	A1 B12 B14 A2 b21	A1 b11 C1 a2 b24 c4	A1 b12 C2 A2 B23
A3 B33 C3	b22 c2 A3 B31 B33	C1 A3 b33 C3	A3 b33 C3	B24 a3 b31 c1
a1 b14 c4 a2 b23 c3 a3	B34	A1 B12 B13 A2 b21	A1 b11 C1 A2 B23	A1 b12 C2 A2 B21
b31 c1	A1 B13 B14 a2 b22 c2	C1 A3 b34 C4	B24 a3 b32 c2	B24 a3 b33 c3
a1 b14 c4 a2 b23 c3 a3	A3 b31 C1	A1 B13 B14 A2 b22	A1 b11 C1 A2 B22	A1 b12 C2 A2 B21
b32 c2	A1 B11 B14 a2 b22 c2	C2 a3 b31 c1	B24 a3 b33 c3	B23 a3 b34 c4
a1 b14 c4 a2 b23 c3	A3 b33 C3	A1 B11 B14 A2 b22	A1 b11 C1 A2 B22	A1 b12 C2 A2 B21
A3 B31 B32	A1 B11 B13 a2 b22 c2	C2 a3 b33 c3	B23 a3 b34 c4	B23 B24 A3 B31 B33
a1 b14 c4 a2 b23 c3	A3 b34 C4	A1 B11 B13 A2 b22	A1 b11 C1 A2 B22	B34
A3 b31 C1	A1 B12 B14 a2 b23 c3	C2 a3 b34 c4	B23 B24 A3 B32 B33	A1 b12 C2 A2 B23
a1 b14 c4 a2 b23 c3	a3 b31 c1	A1 B11 B13 B14 A2	B34	B24 A3 b31 C1
A3 b32 C2	A1 B11 B14 a2 b23 c3	b22 C2 A3 B31 B33	A1 b11 C1 A2 B23	A1 b12 C2 A2 B21
a1 b14 c4 A2 B22 B23	a3 b32 c2	B34	B24 A3 b32 C2	B24 A3 b33 C3
a3 b31 c1	A1 B11 B12 a2 b23 c3	A1 B13 B14 A2 b22	A1 b11 C1 A2 B22	A1 b12 C2 A2 B21
a1 b14 c4 A2 B21 B23	a3 b34 c4	C2 A3 b31 C1	B24 A3 b33 C3	B23 A3 b34 C4
a3 b32 c2	A1 B11 B12 B14 a2	A1 B11 B14 A2 b22	A1 b11 C1 A2 B22	A1 b12 C2 A2 b21 C1
a1 b14 c4 A2 B21 B22	b23 c3 A3 B31 B32	C2 A3 b33 C3	B23 A3 b34 C4	a3 b33 c3
a3 b33 c3	B34	A1 B11 B13 A2 b22	A1 b11 C1 A2 b22 C2	A1 b12 C2 A2 b21 C1
a1 b14 c4 A2 B21 B22	A1 B12 B14 a2 b23 c3	C2 A3 b34 C4	a3 b33 c3	A1 b12 C2 A2 b21 C1
B23 A3 B31 B32 B33	A3 b31 C1	A1 B12 B14 A2 b23	A1 b11 C1 A2 b22 C2	A1 b12 C2 A2 b21 C1
a1 b14 c4 A2 B22 B23	A1 B11 B14 a2 b23 c3	C3 a3 b31 c1	a3 b34 c4	A3 B33 B34
A3 b31 C1	A3 b32 C2	A1 B11 B14 A2 b23	A1 b11 C1 A2 b22 C2	A1 b12 C2 A2 b21 C1
a1 b14 c4 A2 B21 B23	A1 B11 B12 a2 b23 c3	C3 a3 b32 c2	A3 B33 B34	A3 b33 C3
A3 b32 C2	A3 b34 C4	A1 B11 B12 A2 b23	A1 b11 C1 A2 b22 C2	A1 b12 C2 A2 b21 C1
a1 b14 c4 A2 B21 B22	A1 B12 B13 a2 b24 c4	C3 a3 b34 c4	A3 b33 C3	A3 b34 C4
A3 b33 C3	a3 b31 c1	A1 B11 B12 B14 A2	A1 b11 C1 A2 b22 C2	A1 b12 C2 A2 b23 C3
a1 b14 c4 A2 b21 C1	A1 B11 B13 a2 b24 c4	b23 C3 A3 B31 B32	A3 b34 C4	a3 b31 c1
a3 b32 c2	a3 b32 c2	B34	A1 b11 C1 A2 b23 C3	A1 b12 C2 A2 b23 C3
a1 b14 c4 A2 b21 C1	A1 B11 B12 a2 b24 c4	A1 B12 B14 A2 b23	a3 b32 c2	a3 b34 c4
a3 b33 c3	a3 b33 c3	C3 A3 b31 C1	A1 b11 C1 A2 b23 C3	A1 b12 C2 A2 b23 C3
a1 b14 c4 A2 b21 C1	A1 B11 B12 B13 a2	A1 B11 B14 A2 b23	a3 b34 c4	A3 B31 B34
A3 B32 B33	b24 c4 A3 B31 B32	C3 A3 b32 C2	A1 b11 C1 A2 b23 C3	A1 b12 C2 A2 b23 C3
a1 b14 c4 A2 b21 C1	B33	A1 B11 B12 A2 b23	A3 B32 B34	A3 b31 C1
A3 b32 C2	A1 B12 B13 a2 b24 c4	C3 A3 b34 C4	A1 b11 C1 A2 b23 C3	A1 b12 C2 A2 b23 C3
a1 b14 c4 A2 b21 C1	A3 b31 C1	A1 B12 B13 A2 b24	A3 b32 C2	A3 b34 C4
A3 b33 C3	A1 B11 B13 a2 b24 c4	C4 a3 b31 c1	A1 b11 C1 A2 b23 C3	A1 b12 C2 A2 b24 C4
a1 b14 c4 A2 b22 C2	A3 b32 C2	A1 B11 B13 A2 b24	A3 b34 C4	a3 b31 c1
a3 b31 c1	A1 B11 B12 a2 b24 c4	C4 a3 b32 c2	A1 b11 C1 A2 b24 C4	A1 b12 C2 A2 b24 C4
a1 b14 c4 A2 b22 C2	A3 b33 C3	A1 B11 B12 A2 b24	a3 b32 c2	a3 b33 c3
a3 b33 c3	A1 B12 B13 B14 A2	C4 a3 b33 c3	A1 b11 C1 A2 b24 C4	A1 b12 C2 A2 b24 C4
a1 b14 c4 A2 b22 C2	B22 B23 B24 a3 b31	A1 B11 B12 B13 A2	a3 b33 c3	A3 B31 B33
A3 B31 B33	c1	b24 C4 A3 B31 B32	A1 b11 C1 A2 b24 C4	A1 b12 C2 A2 b24 C4
a1 b14 c4 A2 b22 C2	A1 B11 B13 B14 A2	B33	A3 B32 B33	A3 b31 C1
A3 b31 C1	B21 B23 B24 a3 b32	A1 B12 B13 A2 b24	A1 b11 C1 A2 b24 C4	A1 b12 C2 A2 b24 C4
a1 b14 c4 A2 b22 C2	c2	C4 A3 b31 C1	A3 b32 C2	A3 b33 C3
A3 b33 C3	A1 B11 B12 B14 A2	A1 B11 B13 A2 b24	A1 b11 C1 A2 b24 C4	A1 b13 C3 a2 b21 c1
a1 b14 c4 A2 b23 C3	B21 B22 B24 a3 b33	C4 A3 b32 C2	A3 b33 C3	a3 b32 c2
a3 b31 c1	c3	A1 B11 B12 A2 b24	A1 b12 C2 a2 b21 c1	A1 b13 C3 a2 b21 c1
a1 b14 c4 A2 b23 C3	A1 B11 B12 B13 A2	C4 A3 b33 C3	a3 b33 c3	a3 b34 c4
a3 b32 c2	B21 B22 B23 a3 b34	A1 b11 C1 a2 b22 c2	A1 b12 C2 a2 b21 c1	A1 b13 C3 a2 b21 c1
a1 b14 c4 A2 b23 C3	c4	a3 b33 c3	a3 b34 c4	A3 B32 B34
A3 B31 B32	A1 B11 B12 B13 B14	A1 b11 C1 a2 b22 c2	A1 b12 C2 a2 b21 c1	A1 b13 C3 a2 b21 c1
a1 b14 c4 A2 b23 C3	A2 B21 B22 B23 B24	a3 b34 c4	A3 B33 B34	A3 b32 C2
A3 b31 C1	A3 B31 B32 B33 B34	A1 b11 C1 a2 b22 c2	A1 b12 C2 a2 b21 c1	A1 b13 C3 a2 b21 c1
a1 b14 c4 A2 b23 C3	A1 B12 B13 B14 A2	A3 B33 B34	A3 b33 C3	A3 b34 C4
A3 b32 C2	B22 B23 B24 A3 b31	A1 b11 C1 a2 b22 c2	A1 b12 C2 a2 b21 c1	A1 b13 C3 a2 b22 c2
A1 B13 B14 a2 b21 c1	C1	A3 b33 C3	A3 b34 C4	a3 b31 c1
a3 b32 c2	A1 B11 B13 B14 A2	A1 b11 C1 a2 b22 c2	A1 b12 C2 a2 b23 c3	A1 b13 C3 a2 b22 c2
A1 B12 B14 a2 b21 c1	B21 B23 B24 A3 b32	A3 b34 C4	a3 b31 c1	a3 b34 c4
a3 b33 c3	C2	A1 b11 C1 a2 b23 c3	A1 b12 C2 a2 b23 c3	A3 B31 B34
A1 B12 B13 a2 b21 c1	A1 B11 B12 B14 A2	a3 b32 c2	a3 b34 c4	A1 b13 C3 a2 b22 c2
a3 b34 c4	B21 B22 B24 A3 b33	A1 b11 C1 a2 b23 c3	A1 b12 C2 a2 b23 c3	A3 b31 C1
A1 B12 B13 B14 a2	C3	a3 b34 c4	A3 B31 B34	A1 b12 C2 a2 b23 c3
b21 c1 A3 B32 B33	A1 B11 B12 B13 A2	A1 b11 C1 a2 b23 c3	A1 b12 C2 a2 b23 c3	A3 b31 C1
B34	B21 B22 B23 A3 b34	A3 B32 B34	A3 b31 C1	A1 b12 C2 a2 b23 c3
A1 B13 B14 a2 b21 c1	C4	A1 b11 C1 a2 b23 c3	A1 b12 C2 a2 b23 c3	A3 b34 C4
A3 b32 C2	A1 B13 B14 A2 b21	A3 b32 C2	A3 b34 C4	A1 b12 C2 a2 b24 c4
A1 B12 B14 a2 b21 c1	C1 a3 b32 c2	A1 b11 C1 a2 b23 c3	A1 b12 C2 a2 b24 c4	a3 b31 c1
A3 b33 C3	A1 B12 B14 A2 b21	A3 b34 C4	A1 b12 C2 a2 b24 c4	A3 B31 B32
A1 B12 B13 a2 b21 c1	C1 a3 b33 c3	A1 b11 C1 a2 b24 c4	A1 b12 C2 a2 b24 c4	A1 b13 C3 a2 b24 c4
A3 b34 C4	A1 B12 B13 A2 b21	a3 b32 c2	a3 b33 c3	A3 B31 B32
A1 B13 B14 a2 b22 c2	C1 a3 b34 c4	A1 b11 C1 a2 b24 c4	A1 b12 C2 a2 b24 c4	A1 b13 C3 a2 b24 c4

A3 b31 C1	A3 b32 C2	A1 b14 C4 a2 b21 c1	A3 b31 C1	A3 b32 C2
A1 b13 C3 a2 b24 c4	A1 b13 C3 A2 b21 C1	a3 b33 c3	A1 b14 C4 a2 b23 c3	A1 b14 C4 A2 b21 C1
A3 b32 C2	A3 b34 C4	A1 b14 C4 a2 b21 c1	A3 b32 C2	A3 b33 C3
A1 b13 C3 A2 B22	A1 b13 C3 A2 b22 C2	A3 B32 B33	A1 b14 C4 A2 B22	A1 b14 C4 A2 b22 C2
B24 a3 b31 c1	a3 b31 c1	A1 b14 C4 a2 b21 c1	B23 a3 b31 c1	a3 b31 c1
A1 b13 C3 A2 B21	A1 b13 C3 A2 b22 C2	A3 b32 C2	A1 b14 C4 A2 B21	A1 b14 C4 A2 b22 C2
B24 a3 b32 c2	a3 b34 c4	A1 b14 C4 a2 b21 c1	B23 a3 b32 c2	a3 b33 c3
A1 b13 C3 A2 B21	A1 b13 C3 A2 b22 C2	A3 b33 C3	A1 b14 C4 A2 B21	A1 b14 C4 A2 b22 C2
B22 a3 b34 c4	A3 B31 B34	A1 b14 C4 a2 b22 c2	B22 a3 b33 c3	A3 B31 B33
A1 b13 C3 A2 B21	A1 b13 C3 A2 b22 C2	a3 b31 c1	A1 b14 C4 A2 B21	A1 b14 C4 A2 b22 C2
B22 B24 A3 B31 B32	A3 b31 C1	A1 b14 C4 a2 b22 c2	B22 B23 A3 B31 B32	A3 b31 C1
B34	A1 b13 C3 A2 b22 C2	a3 b33 c3	B33	A1 b14 C4 A2 b22 C2
A1 b13 C3 A2 B22	A3 b34 C4	A1 b14 C4 a2 b22 c2	A1 b14 C4 A2 B22	A3 b33 C3
B24 A3 b31 C1	A1 b13 C3 A2 b24 C4	A3 B31 B33	B23 A3 b31 C1	A1 b14 C4 A2 b23 C3
A1 b13 C3 A2 B21	a3 b31 c1	A1 b14 C4 a2 b22 c2	A1 b14 C4 A2 B21	a3 b31 c1
B24 A3 b32 C2	A1 b13 C3 A2 b24 C4	A3 b31 C1	B23 A3 b32 C2	A1 b14 C4 A2 b23 C3
A1 b13 C3 A2 B21	a3 b32 c2	A1 b14 C4 a2 b22 c2	A1 b14 C4 A2 B21	A1 b32 c2
B22 A3 b34 C4	A1 b13 C3 A2 b24 C4	A3 b33 C3	B22 A3 b33 C3	A1 b14 C4 A2 b23 C3
A1 b13 C3 A2 b21 C1	A3 B31 B32	A1 b14 C4 a2 b23 c3	A1 b14 C4 A2 b21 C1	A3 B31 B32
a3 b32 c2	A1 b13 C3 A2 b24 C4	a3 b31 c1	a3 b32 c2	A1 b14 C4 A2 b23 C3
A1 b13 C3 A2 b21 C1	A3 b31 C1	A1 b14 C4 a2 b23 c3	A1 b14 C4 A2 b21 C1	A3 b31 C1
a3 b34 c4	A1 b13 C3 A2 b24 C4	a3 b32 c2	a3 b33 c3	A1 b14 C4 A2 b23 C3
A1 b13 C3 A2 b21 C1	A3 b32 C2	A1 b14 C4 a2 b23 c3	A1 b14 C4 A2 b21 C1	A3 b32 C2
A3 B32 B34	A1 b14 C4 a2 b21 c1	A3 B31 B32	A3 B32 B33	
A1 b13 C3 A2 b21 C1	a3 b32 c2	A1 b14 C4 a2 b23 c3	A1 b14 C4 A2 b21 C1	

• $k = 4, j = 3$

a1 b11 c1 a2 b22 c2 a3	C2 a4 b43 c3	A3 a4 b41 c1	a1 b12 c2 A2 b21 C1	a1 b13 c3 A2 a3 b32
b33 c3 A4	a1 b11 c1 A2 B23 A3	a1 b12 c2 a2 b23 c3	A3 a4 b43 c3	c2 a4 b41 c1
a1 b11 c1 a2 b22 c2	b32 C2 A4 B43	A3 B31 A4 B41	a1 b12 c2 A2 b21 C1	a1 b13 c3 A2 B21 a3
A3 a4 b43 c3	a1 b11 c1 A2 A3 b32	a1 b12 c2 a2 b23 c3	A3 B33 A4 B43	b32 c2 A4 B41
a1 b11 c1 a2 b22 c2	C2 A4 b43 C3	A3 A4 b41 C1	a1 b12 c2 A2 b21 C1	a1 b13 c3 A2 a3 b32
A3 B33 A4 B43	a1 b11 c1 A2 A3 b33	a1 b12 c2 a2 b23 c3	A3 A4 b43 C3	c2 A4 b41 C1
a1 b11 c1 a2 b22 c2	C3 a4 b42 c2	A3 b31 C1 A4	a1 b12 c2 A2 b21 C1	a1 b13 c3 A2 B22 A3
A3 A4 b43 C3	a1 b11 c1 A2 B22 A3	a1 b12 c2 A2 a3 b31	A3 b33 C3 A4	B32 a4 b41 c1
a1 b11 c1 a2 b22 c2	b33 C3 A4 B42	c1 a4 b43 c3	a1 b12 c2 A2 b23 C3	a1 b13 c3 A2 B21 A3
A3 b33 C3 A4	a1 b11 c1 A2 A3 b33	a1 b12 c2 A2 B23 a3	a3 b31 c1 A4	B31 a4 b42 c2
a1 b11 c1 a2 b23 c3 a3	C3 A4 b42 C2	b31 c1 A4 B43	a1 b12 c2 A2 b23 C3	A1 b13 c3 A2 B21 B22
b32 c2 A4	a1 b11 c1 A2 b22 C2	a1 b12 c2 A2 a3 b31	A3 a4 b41 c1	A3 B31 B32 A4 B41
a1 b11 c1 a2 b23 c3	a3 b33 c3 A4	c1 A4 b43 C3	a1 b12 c2 A2 b23 C3	B42
A3 a4 b42 c2	a1 b11 c1 A2 b22 C2	a1 b12 c2 A2 a3 b33	A3 B31 A4 B41	a1 b13 c3 A2 B22 A3
a1 b11 c1 a2 b23 c3	A3 a4 b43 c3	c3 a4 b41 c1	a1 b12 c2 A2 b23 C3	B32 A4 b41 C1
A3 B32 A4 B42	a1 b11 c1 A2 b22 C2	a1 b12 c2 A2 B21 a3	A3 A4 b41 C1	a1 b13 c3 A2 B21 A3
A3 B33 A4 B43	A3 B33 A4 B43	b33 c3 A4 B41	a1 b12 c2 A2 b23 C3	B31 A4 b42 C2
a1 b11 c1 a2 b23 c3	a1 b11 c1 A2 b22 C2	a1 b12 c2 A2 a3 b33	A3 b31 C1 A4	a1 b13 c3 A2 A3 b31
A3 A4 b42 C2	A3 A4 b43 C3	c3 A4 b41 C1	a1 b13 c3 a2 b21 c1 a3	C1 a4 b42 c2
a1 b11 c1 a2 b23 c3	a1 b11 c1 A2 b22 C2	a1 b12 c2 A2 B23 A3	b32 c2 A4	a1 b13 c3 A2 B22 A3
A3 b32 C2 A4	A3 b33 C3 A4	B33 a4 b41 c1	a1 b13 c3 a2 b21 c1	b31 C1 A4 B42
a1 b11 c1 A2 a3 b32	a1 b11 c1 A2 b23 C3	a1 b12 c2 A2 B21 A3	A3 a4 b42 c2	a1 b13 c3 A2 A3 b31
c2 A4 b43 C3	a3 b32 c2 A4	B31 a4 b43 c3	a1 b13 c3 a2 b21 c1	C1 A4 b42 C2
a1 b11 c1 A2 a3 b33	A3 a4 b42 c2	a1 b12 c2 A2 B21 B23	A3 B32 A4 B42	a1 b13 c3 A2 A3 b32
c3 a4 b42 c2	a1 b11 c1 A2 b23 C3	A3 B31 B33 A4 B41	a1 b13 c3 a2 b21 c1	C2 a4 b41 c1
a1 b11 c1 A2 B22 a3	A3 B32 A4 B42	B43	A3 A4 b42 C2	a1 b13 c3 A2 B21 A3
b33 c3 A4 B42	a1 b11 c1 A2 b23 C3	a1 b12 c2 A2 B23 A3	a1 b13 c3 a2 b21 c1	b32 C2 A4 B41
a1 b11 c1 A2 a3 b33	A3 A4 b42 C2	B33 A4 b41 C1	A3 b32 C2 A4	a1 b13 c3 A2 A3 b32
c3 A4 b42 C2	a1 b11 c1 A2 b23 C3	a1 b12 c2 A2 B21 A3	a1 b13 c3 a2 b21 c1	C2 A4 b41 c1
a1 b11 c1 A2 B23 A3	A3 b32 C2 A4	B31 A4 b43 C3	a1 b13 c3 a2 b22 c2	a1 b13 c3 A2 B21 A3
B33 a4 b42 c2	a1 b12 c2 a2 b21 c1 a3	a1 b12 c2 A2 A3 b31	A3 a4 b41 c1	b32 C2 A4 B41
a1 b11 c1 A2 B22 A3	b33 c3 A4	a1 b12 c2 A2 B23 A3	a1 b13 c3 a2 b22 c2	a1 b13 c3 A2 A3 b32
B32 a4 b43 c3	a1 b12 c2 a2 b21 c1	b31 C1 A4 B43	A3 B31 A4 B41	C2 a4 b41 c1
a1 b11 c1 A2 B22 B23	A3 a4 b43 c3	a1 b12 c2 A2 A3 b31	a1 b13 c3 a2 b22 c2	a1 b13 c3 A2 b21 C1
A3 B32 B33 A4 B42	a1 b12 c2 a2 b21 c1	C1 a4 b43 c3	A3 a4 b41 c1	a3 b32 c2 A4
B43	A3 A4 b43 C3	a1 b12 c2 A2 B23 A3	a1 b13 c3 a2 b22 c2	A3 a4 b42 c2
a1 b11 c1 A2 B23 A3	a1 b12 c2 a2 b21 c1	b31 C1 A4 B41	A3 B31 A4 B41	a1 b13 c3 A2 b21 C1
B33 A4 b42 C2	A3 b33 C3 A4	a1 b12 c2 A2 A3 b31	a1 b13 c3 a2 b22 c2	A3 B32 A4 B42
a1 b11 c1 A2 B23 A3	a1 b12 c2 a2 b21 c1	C1 A4 b43 C3	A3 A4 b41 C1	a1 b13 c3 A2 b21 C1
B32 A4 b43 C3	A3 B33 A4 B43	a1 b12 c2 A2 A3 b33	a1 b13 c3 a2 b22 c2	A3 A4 b42 C2
a1 b11 c1 A2 B22 B23	a1 b12 c2 a2 b21 c1	C3 a4 b41 c1	A3 b31 C1 A4	a1 b13 c3 A2 b21 C1
A3 B32 B33 A4 B42	A3 A4 b43 C3	a1 b12 c2 A2 B21 A3	a1 b13 c3 A2 a3 b31	A3 b32 C2 A4
B43	a1 b12 c2 a2 b21 c1	b33 C3 A4 B41	c1 a4 b42 c2	a1 b13 c3 A2 b22 C2
a1 b11 c1 A2 B23 A3	A3 b33 C3 A4	a1 b12 c2 A2 A3 b33	a1 b13 c3 A2 B22 a3	a3 b31 c1 A4
B33 A4 b42 C2	a1 b12 c2 a2 b23 c3 a3	C3 A4 b41 C1	b31 c1 A4 B42	a1 b13 c3 A2 b22 C2
a1 b11 c1 A2 B23 A3	b31 c1 A4	a1 b12 c2 A2 b21 C1	a1 b13 c3 A2 a3 b31	A3 a4 b41 c1
B32 A4 b43 C3	a1 b12 c2 a2 b23 c3	a3 b33 c3 A4	c1 A4 b42 C2	a1 b13 c3 A2 b22 C2
a1 b11 c1 A2 A3 b32				

A3 B31 A4 B41
a1 b13 c3 A2 b22 C2
A3 A4 b41 C1
a1 b13 c3 A2 b22 C2
A3 b31 C1 A4
A1 a2 b21 c1 a3 b32
c2 a4 b43 c3
A1 B13 a2 b21 c1 a3
b32 c2 A4 B43
A1 a2 b21 c1 a3 b32
c2 A4 b43 C3
A1 a2 b21 c1 a3 b33
c3 a4 b42 c2
A1 B12 a2 b21 c1 a3
b33 c3 A4 B42
A1 a2 b21 c1 a3 b33
c3 A4 b42 C2
A1 B13 a2 b21 c1 A3
B33 A4 b42 C2
A1 B12 a2 b21 c1 A3
B32 a4 b43 c3
A1 B12 B13 a2 b21 c1
A3 B32 B33 A4 B42
B43
A1 B13 a2 b21 c1 A3
B33 A4 b42 C2
A1 B12 a2 b21 c1 A3
B32 A4 b43 C3
A1 a2 b21 c1 A3 b32
C2 a4 b43 c3
A1 B13 a2 b21 c1 A3
b32 C2 A4 B43
A1 a2 b21 c1 A3 b32
C2 A4 b41 C1
A1 a2 b21 c1 A3 b33
C3 a4 b42 c2
A1 B12 a2 b21 c1 A3
b33 C3 A4 B42
A1 a2 b21 c1 A3 b33
C3 A4 b42 C2
A1 a2 b22 c2 a3 b31
c1 a4 b43 c3
A1 B13 a2 b22 c2 a3
b31 c1 A4 B43
A1 a2 b22 c2 a3 b31
c1 A4 b43 C3
A1 a2 b22 c2 a3 b33
c3 a4 b41 c1
A1 B13 a2 b22 c2 A3
B33 a4 b41 C1
A1 B11 a2 b22 c2 A3
B31 A4 b43 C3
A1 a2 b22 c2 A3 b33
c1 a4 b43 c3
A1 B13 a2 b22 c2 A3
b31 C1 A4 B43
A1 a2 b22 c2 A3 b33
c1 A4 b43 C3
A1 a2 b22 c2 A3 b33
C3 a4 b41 c1
A1 B11 a2 b22 c2 A3
B32 A4 b43 C3
A1 a2 b22 c2 A3 b33
c3 a4 b41 c1
A1 B11 a2 b22 c2 A3
B33 A4 b43 C3
A1 a2 b22 c2 A3 b33
c3 a4 b43 c3
A1 B11 C1 a2 b22 c2
a3 b32 c2 A4
A1 b11 C1 a2 b23 c3
A3 a4 b42 c2
A1 b11 C1 a2 b23 c3
A3 B32 A4 B42
A1 b11 C1 a2 b23 c3
A3 A4 b42 C2
A1 b11 C1 a2 b23 c3
A3 b32 C2 A4
A1 b11 C1 a2 a3 b32
c2 a4 b43 C3
A1 b11 C1 A2 a3 b33
c3 a4 b42 c2
A1 b11 C1 A2 B22 a3
b32 c2 A4 B43
A1 b11 C1 A2 a3 b33
c3 A4 b42 C2
A1 b11 C1 A2 B23 A3
B33 a4 b42 c2
A1 b11 C1 A2 B22 A3
B32 a4 b43 c3
A1 b11 C1 A2 A3 b32
C2 a4 b43 c3
A1 b11 C1 A2 B23 A3
b32 C2 A4 B43
A1 b11 C1 A2 A3 b32
C2 A4 b43 C3
A1 b11 C1 A2 A3 b33
C3 a4 b42 c2
A1 b11 C1 A2 B22 A3
b33 C3 A4 B42
A1 b11 C1 A2 A3 b33
C3 A4 b42 C2
A1 b11 C1 A2 b22 C2
a3 b33 c3 A4
A1 b11 C1 A2 b22 C2
A3 a4 b43 c3
A1 b11 C1 A2 b22 C2
A3 a4 b43 c3
A1 b11 C1 A2 b22 C2
A3 B33 A4 B43
A1 b12 C2 a2 b21 c1
a3 b33 c3 A4
A1 b12 C2 a2 b21 c1
A3 a4 b43 c3
A1 b12 C2 a2 b21 c1
A3 B33 A4 B43
A1 b12 C2 a2 b21 c1

A3 A4 b43 C3	A1 b12 C2 A2 B21	A1 b12 C2 A2 b23 C3	A3 b31 C1 A4	C1 A4 b42 C2
A1 b12 C2 a2 b21 c1	B23 A3 B31 B33 A4	a3 b31 c1 A4	A1 b13 C3 A2 a3 b31	A1 b13 C3 A2 A3 b32
A3 b33 C3 A4	B41 B43	A1 b12 C2 A2 b23 C3	c1 a4 b42 c2	C2 a4 b41 c1
A1 b12 C2 a2 b23 c3	A1 b12 C2 A2 B23 A3	A3 a4 b41 c1	A1 b13 C3 A2 B22 a3	A1 b13 C3 A2 B21 A3
a3 b31 c1 A4	B33 A4 b41 C1	A1 b12 C2 A2 b23 C3	b31 c1 A4 B42	b32 C2 A4 B41
A1 b12 C2 a2 b23 c3	A1 b12 C2 A2 B21 A3	A3 B31 A4 B41	A1 b13 C3 A2 a3 b31	A1 b13 C3 A2 A3 b32
A3 a4 b41 c1	B31 A4 b43 C3	A1 b12 C2 A2 b23 C3	c1 A4 b42 C2	C2 A4 b41 C1
A1 b12 C2 a2 b23 c3	A1 b12 C2 A2 A3 b31	A3 A4 b41 C1	A1 b13 C3 A2 a3 b32	A1 b13 C3 A2 b21 C1
A3 B31 A4 B41	C1 a4 b43 c3	A1 b12 C2 A2 b23 C3	c2 a4 b41 c1	a3 b32 c2 A4
A1 b12 C2 a2 b23 c3	A1 b12 C2 A2 B23 A3	A3 b31 C1 A4	A1 b13 C3 A2 B21 a3	A1 b13 C3 A2 b21 C1
A3 A4 b41 C1	b31 C1 A4 B43	A1 b13 C3 a2 b21 c1	b32 c2 A4 B41	A3 a4 b42 c2
A1 b12 C2 a2 b23 c3	A1 b12 C2 A2 A3 b31	a3 b32 c2 A4	A1 b13 C3 A2 a3 b32	A1 b13 C3 A2 b21 C1
A3 b31 C1 A4	C1 A4 b43 C3	A1 b13 C3 a2 b21 c1	c2 A4 b41 C1	A3 B32 A4 B42
A1 b12 C2 A2 a3 b31	A1 b12 C2 A2 A3 b33	A3 a4 b42 c2	A1 b13 C3 A2 B22 A3	A1 b13 C3 A2 b21 C1
c1 a4 b43 c3	C3 a4 b41 c1	A1 b13 C3 a2 b21 c1	B32 a4 b41 c1	A3 A4 b42 C2
A1 b12 C2 A2 B23 a3	A1 b12 C2 A2 B21 A3	A3 B32 A4 B42	A1 b13 C3 A2 B21 A3	A1 b13 C3 A2 b21 C1
b31 c1 A4 B43	b33 C3 A4 B41	A1 b13 C3 a2 b21 c1	B31 a4 b42 c2	A3 b32 C2 A4
A1 b12 C2 A2 a3 b31	A1 b12 C2 A2 A3 b33	A3 A4 b42 C2	A1 b13 C3 A2 B21	A1 b13 C3 A2 b22 C2
c1 A4 b43 C3	C3 A4 b41 C1	A1 b13 C3 a2 b21 c1	B22 A3 B31 B32 A4	a3 b31 c1 A4
A1 b12 C2 A2 a3 b33	A1 b12 C2 A2 b21 C1	A3 b32 C2 A4	B41 B42	A1 b13 C3 A2 b22 C2
c3 a4 b41 c1	a3 b33 c3 A4	A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 B22 A3	A3 a4 b41 c1
A1 b12 C2 A2 B21 a3	A1 b12 C2 A2 b21 C1	a3 b31 c1 A4	B32 A4 b41 C1	A1 b13 C3 A2 b22 C2
b33 c3 A4 B41	A3 a4 b43 c3	A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 B21 A3	A3 B31 A4 B41
A1 b12 C2 A2 a3 b33	A1 b12 C2 A2 b21 C1	A3 a4 b41 c1	B31 A4 b42 C2	A1 b13 C3 A2 b22 C2
c3 A4 b41 C1	A3 B33 A4 B43	A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 A3 b31	A3 A4 b41 C1
A1 b12 C2 A2 B23 A3	A1 b12 C2 A2 b21 C1	A3 B31 A4 B41	C1 a4 b42 c2	A1 b13 C3 A2 b22 C2
B33 a4 b41 c1	A3 A4 b43 C3	A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 B22 A3	A3 b31 C1 A4
A1 b12 C2 A2 B21 A3	A1 b12 C2 A2 b21 C1	A3 A4 b41 C1	b31 C1 A4 B42	
B31 a4 b43 c3	A3 b33 C3 A4	A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 A3 b31	

• $k = 4, j = 4$

a1 b11 c1 a2 b22 c2 a3	b32 c2 A4 b44 C4	a1 b11 c1 a2 b24 c4 a3	a3 b33 c3 A4 B42 B44	a1 b11 c1 A2 B24 A3
b33 c3 a4 b44 c4	a1 b11 c1 a2 b23 c3 a3	b33 c3 A4 b42 C2	a1 b11 c1 A2 B24 a3	b32 C2 A4 b43 C3
a1 b11 c1 a2 b22 c2 a3	b34 c4 a4 b42 c2	a1 b11 c1 a2 b24 c4	b33 c3 A4 b42 C2	a1 b11 c1 A2 B23 A3
b33 c3 A4 B44	a1 b11 c1 a2 b23 c3 a3	A3 B33 a4 b42 c2	a1 b11 c1 A2 B22 a3	b32 C2 A4 b44 C4
a1 b11 c1 a2 b22 c2 a3	b34 c4 A4 B42	a1 b11 c1 a2 b24 c4	b33 c3 A4 b44 C4	a1 b11 c1 A2 B24 A3
b33 c3 A4 b44 C4	a1 b11 c1 a2 b23 c3 a3	A3 B32 a4 b43 c3	a1 b11 c1 A2 B23 a3	b33 C3 a4 b42 c2
a1 b11 c1 a2 b22 c2 a3	b34 c4 A4 b42 C2	a1 b11 c1 a2 b24 c4	b34 c4 a4 b42 c2	a1 b11 c1 A2 B22 A3
b34 c4 a4 b43 c3	a1 b11 c1 a2 b23 c3	A3 B32 B33 A4 B42	a1 b11 c1 A2 B22 a3	b33 C3 a4 b44 c4
a1 b11 c1 a2 b22 c2 a3	A3 B34 a4 b42 c2	B43	b34 c4 a4 b43 c3	a1 b11 c1 A2 B22 B24
b34 c4 A4 B43	a1 b11 c1 a2 b23 c3	a1 b11 c1 a2 b24 c4	a1 b11 c1 A2 B22 B23	A3 b33 C3 A4 B42
a1 b11 c1 a2 b22 c2 a3	A3 B32 a4 b44 c4	A3 B33 A4 b42 C2	a3 b34 c4 A4 B42 B43	B44
b34 c4 A4 b43 C3	a1 b11 c1 a2 b23 c3	a1 b11 c1 a2 b24 c4	a1 b11 c1 A2 B23 a3	a1 b11 c1 A2 B24 A3
a1 b11 c1 a2 b22 c2	A3 B32 B34 A4 B42	A3 B32 A4 b43 C3	b34 c4 A4 b42 C2	b33 C3 A4 b42 C2
A3 B34 a4 b43 c3	B44	a1 b11 c1 a2 b24 c4	a1 b11 c1 A2 B22 a3	a1 b11 c1 A2 B22 A3
a1 b11 c1 a2 b22 c2	a1 b11 c1 a2 b23 c3	A3 b32 C2 a4 b43 c3	b34 c4 A4 b43 C3	b33 C3 A4 b44 C4
A3 B33 a4 b44 c4	A3 B34 A4 b42 C2	a1 b11 c1 a2 b24 c4	a1 b11 c1 A2 B23 B24	a1 b11 c1 A2 B22 B24
a1 b11 c1 a2 b22 c2	a1 b11 c1 a2 b23 c3	A3 b32 C2 A4 B43	A3 B33 B34 a4 b42 c2	A3 b33 C3 A4 B42
A3 B33 B34 A4 B43	A3 B32 A4 b44 C4	a1 b11 c1 a2 b24 c4	a1 b11 c1 A2 B22 B24	B44
B44	a1 b11 c1 a2 b23 c3	A3 b32 C2 A4 b43 C3	A3 B32 B34 a4 b43 c3	a1 b11 c1 A2 B24 A3
a1 b11 c1 a2 b22 c2	A3 B34 A4 b42 C2	a1 b11 c1 a2 b24 c4	a1 b11 c1 A2 B22 B23	b34 C4 a4 b43 C3
A3 B33 a4 b44 c4	A3 B34 A4 B42	A3 b33 C3 a4 b42 c2	A3 B32 B33 a4 b44 c4	a1 b11 c1 A2 B22 B23
a1 b11 c1 a2 b22 c2	a1 b11 c1 a2 b23 c3	a1 b11 c1 a2 b24 c4	a1 b11 c1 A2 B22 B23	A3 b34 C4 A4 B42
A3 B34 A4 b43 c3	A3 b32 C2 A4 B44	A3 b33 C3 A4 B42	B24 A3 B32 B33 B34	B43
a1 b11 c1 a2 b22 c2	a1 b11 c1 a2 b23 c3	a1 b11 c1 a2 b24 c4	A4 B42 B43 B44	a1 b11 c1 A2 B23 A3
A3 b33 C3 a4 b44 c4	A3 b32 C2 A4 b44 C4	A3 b33 C3 A4 b42 C2	a1 b11 c1 A2 B23 B24	b34 C4 A4 b42 C2
a1 b11 c1 a2 b22 c2	A3 b34 C4 a4 b42 c2	a1 b11 c1 A2 B24 a3	A3 B33 B34 A4 b42	a1 b11 c1 A2 B22 A3
A3 B33 C3 A4 B44	a1 b11 c1 a2 b23 c3	b32 c2 a4 b43 c3	C2	b33 C3 A4 b44 C4
a1 b11 c1 a2 b22 c2	A3 b34 C4 A4 B42	a1 b11 c1 A2 B23 a3	a1 b11 c1 A2 B22 B24	a1 b11 c1 A2 b22 C2
A3 b33 C3 A4 b44 C4	a1 b11 c1 a2 b23 c3	b32 c2 a4 b44 c4	A3 B32 B34 A4 b43	a1 b11 c1 A2 b22 C2
a1 b11 c1 a2 b22 c2	A3 b34 C4 A4 b42 C2	a1 b11 c1 A2 B23 B24	C3	a3 b33 c3 A4 B44
A3 b33 C3 a4 b44 c4	a1 b11 c1 a2 b23 c3	a3 b32 c2 A4 B43 B44	a1 b11 c1 A2 B22 B23	a1 b11 c1 A2 b22 C2
a1 b11 c1 a2 b22 c2	b32 c2 a4 b43 c3	a1 b11 c1 A2 B24 a3	A3 B32 B33 A4 b44	a3 b33 c3 A4 b44 C4
A3 b34 C4 A4 B43	a1 b11 c1 a2 b24 c4 a3	b32 c2 A4 b43 C3	C4	a1 b11 c1 A2 b22 C2
a1 b11 c1 a2 b22 c2	b32 c2 A4 B43	a1 b11 c1 A2 B23 a3	a1 b11 c1 A2 B24 A3	a3 b34 c4 a4 b43 c3
A3 b34 C4 A4 b43 C3	a1 b11 c1 a2 b24 c4 a3	b32 c2 A4 b44 C4	b32 C2 a4 b43 c3	a1 b11 c1 A2 b22 C2
a1 b11 c1 a2 b23 c3 a3	b32 c2 A4 b43 C3	a1 b11 c1 A2 B24 a3	a1 b11 c1 A2 B23 A3	a3 b34 c4 A4 B42
b32 c2 a4 b44 c4	a1 b11 c1 a2 b24 c4 a3	b33 c3 a4 b42 c2	b32 C2 a4 b44 c4	a1 b11 c1 A2 b22 C2
a1 b11 c1 a2 b23 c3 a3	b33 c3 a4 b42 c2	a1 b11 c1 A2 B22 a3	a1 b11 c1 A2 B23 B24	a3 b34 c4 A4 b43 C3
b32 c2 A4 B44	a1 b11 c1 a2 b24 c4 a3	b33 c3 a4 b44 c4	A3 b32 C2 A4 B43	a1 b11 c1 A2 b22 C2
a1 b11 c1 a2 b23 c3 a3	b33 c3 A4 B42	a1 b11 c1 A2 B22 B24	B44	A3 B34 a4 b43 c3

A1 B12 B14 a2 b23 c3
A3 B32 B34 a4 b41 c1
A1 B11 B14 a2 b23 c3
A3 B31 B34 a4 b42 c2
A1 B11 B12 a2 b23 c3
A3 B31 B32 a4 b44 c4
A1 B11 B12 B14 a2
b23 c3 A3 B31 B32
B34 A4 B41 B42 B44
A1 B12 B14 a2 b23 c3
A3 B32 B34 A4 b41
C1
A1 B11 B14 a2 b23 c3
A3 B31 B34 A4 b42
C2
A1 B11 B12 a2 b23 c3
A3 B31 B32 A4 b44
C4
A1 B14 a2 b23 c3 A3
b31 C1 a4 b42 c2
A1 B12 a2 b23 c3 A3
b31 C1 a4 b44 c4
A1 B12 B14 a2 b23
c3 A3 b31 C1 A4 B42
B44
A1 B14 a2 b23 c3 A3
b31 C1 A4 b42 C2
A1 B12 a2 b23 c3 A3
b31 C1 A4 b44 C4
A1 B14 a2 b23 c3 A3
b32 C2 a4 b41 c1
A1 B11 a2 b23 c3 A3
b32 C2 a4 b44 c4
A1 B11 B14 a2 b23
c3 A3 b32 C2 A4 B41
B44
A1 B14 a2 b23 c3 A3
b32 C2 A4 b41 C1
A1 B11 a2 b23 c3 A3
b32 C2 A4 b44 C4
A1 B12 a2 b23 c3 A3
b34 C4 a4 b41 c1
A1 B11 a2 b23 c3 A3
b34 C4 a4 b42 c2
A1 B11 B12 a2 b23
c3 A3 b34 C4 A4 B41
B42
A1 B12 a2 b23 c3 A3
b34 C4 A4 b41 C1
A1 B11 a2 b23 c3 A3
b34 C4 A4 b42 C2
A1 B13 a2 b24 c4 a3
b31 c1 a4 b42 c2
A1 B12 a2 b24 c4 a3
b31 c1 a4 b43 c3
A1 B12 B13 a2 b24 c4
a3 b31 c1 A4 B42 B43
A1 B13 a2 b24 c4 a3
b31 c1 A4 b42 C2
A1 B11 a2 b24 c4 a3
b31 c1 A4 b43
A1 B13 a2 b24 c4 a3
b32 c2 a4 b41 c1
A1 B11 a2 b24 c4 a3
b32 c2 a4 b43 c3
A1 B11 B13 a2 b24 c4
a3 b32 c2 A4 B41 B43
A1 B13 a2 b24 c4 a3
b32 c2 A4 b41 C1
A1 B11 a2 b24 c4 a3
b32 c2 A4 b43 C3
A1 B12 a2 b24 c4 a3
b33 c3 a4 b41 c1
A1 B11 a2 b24 c4 a3
b33 c3 a4 b42 c2
A1 B11 B12 a2 b24 c4
a3 b33 c3 A4 B41 B42

A1 B12 a2 b24 c4 a3
b33 c3 A4 b41 C1
A1 B11 a2 b24 c4 a3
b33 c3 A4 b42 C2
A1 B12 B13 a2 b24 c4
A3 B32 B33 a4 b41 c1
A1 B11 B13 a2 b24 c4
A3 B31 B33 a4 b42 c2
A1 B11 B12 a2 b24 c4
A3 B31 B32 a4 b43 c3
A1 B11 B12 B13 a2
b24 c4 A3 B31 B32
B33 A4 B41 B42 B43
A1 B12 B13 a2 b24 c4
A3 B32 B33 A4 b41
C1
A1 B11 B13 a2 b24 c4
A3 B31 B33 A4 b42
C2
A1 B11 B12 a2 b24 c4
A3 B31 B32 A4 b43
C3
A1 B13 a2 b24 c4 A3
b31 C1 a4 b42 c2
A1 B12 a2 b24 c4 A3
b31 C1 a4 b43 c3
A1 B12 B13 a2 b24
c4 A3 b31 C1 A4 B42
B43
A1 B13 a2 b24 c4 A3
b31 C1 A4 b42 C2
A1 B12 a2 b24 c4 A3
b31 C1 A4 b43 C3
A1 B13 a2 b24 c4 A3
b32 C2 a4 b41 c1
A1 B11 a2 b24 c4 A3
b32 C2 a4 b43 c3
A1 B11 B13 a2 b24
c4 A3 b32 C2 A4 B41
B43
A1 B13 a2 b24 c4 A3
b32 C2 A4 b41 C1
A1 B11 a2 b24 c4 A3
b32 C2 A4 b43 C3
A1 B12 a2 b24 c4 A3
b33 C3 a4 b41 c1
A1 B11 a2 b24 c4 A3
b33 C3 a4 b42 c2
A1 B11 B12 a2 b24
c4 A3 b33 C3 A4 B41
B42
A1 B12 a2 b24 c4 A3
b33 C3 A4 b41 C1
A1 B11 a2 b24 c4 A3
b33 C3 A4 b42 C2
A1 B13 B14 A2 B23
B24 a3 b31 c1 a4 b42
c2
A1 B12 B14 A2 B22
B24 a3 b31 c1 a4 b43
c3
A1 B12 B13 A2 B22
B23 a3 b31 c1 a4 b44
c4
A1 B12 B13 B14 A2
B22 B23 B24 a3 b31
c1 A4 B42 B43 B44
A1 B13 B14 A2 B23
B24 a3 b31 c1 A4 b42
C2
A1 B12 B13 A2 B22
B24 a3 b31 c1 A4 b43
C3
A1 B12 B13 A2 B22
B23 a3 b31 c1 A4 b44
C4

B24 a3 b32 c2 a4 b41
c1
A1 B11 B14 A2 B21
B24 a3 b32 c2 a4 b43
c3
A1 B11 B13 A2 B21
B23 a3 b32 c2 a4 b44
c4
A1 B11 B13 B14 A2
B21 B23 B24 a3 b32
c2 A4 B41 B43 B44
A1 B13 B14 A2 B23
B24 a3 b32 c2 A4 b41
C1
A1 B11 B14 A2 B21
B24 a3 b32 c2 A4 b43
C3
A1 B11 B13 A2 B21
B23 a3 b32 c2 A4 b44
C4
A1 B12 B14 A2 B22
B24 a3 b33 c3 a4 b41
c1
A1 B11 B14 A2 B21
B24 a3 b33 c3 a4 b42
c2
A1 B11 B12 A2 B21
B22 a3 b33 c3 a4 b44
c4
A1 B11 B12 B14 A2
B21 B22 B24 a3 b33
c3 A4 B41 B42 B44
A1 B12 B14 A2 B22
B24 a3 b33 c3 A4 b41
C1
A1 B11 B14 A2 B21
B24 a3 b33 c3 A4 b42
C2
A1 B11 B12 A2 B21
B22 a3 b33 c3 A4 b44
C4
A1 B12 B13 A2 B22
B23 a3 b34 c4 a4 b41
c1
A1 B11 B13 A2 B21
B23 a3 b34 c4 a4 b42
c2
A1 B11 B12 A2 B21
B22 a3 b34 c4 a4 b43
c3
A1 B11 B12 B13 A2
B21 B22 B23 a3 b34
c4 A4 B41 B42 B43
A1 B12 B13 A2 B22
B23 a3 b34 c4 A4 b41
C1
A1 B11 B13 A2 B21
B23 a3 b34 c4 A4 b42
C2
A1 B11 B12 A2 B21
B22 a3 b34 c4 A4 b43
C3
A1 B12 B13 B14 A2
B22 B23 B24 A3 B32
B33 B34 a4 b41 c1
A1 B11 B13 B14 A2
B21 B23 B24 A3 B31
B33 B34 a4 b42 c2
A1 B11 B12 B14 A2
B21 B22 B24 A3 B31
B32 B34 a4 b43 c3
A1 B11 B12 B13 A2
B21 B22 B23 A3 B31
B32 B33 a4 b44 c4
A1 B11 B12 B13 B14
A2 B21 B22 B23 B24
A3 B31 B32 B33 B34

A4 B41 B42 B43 B44
A1 B12 B13 B14 A2
B22 B23 B24 A3 B32
B33 B34 A4 b41 C1
A1 B11 B13 B14 A2
B21 B23 B24 A3 B31
B33 B34 A4 b42 C2
A1 B11 B12 B14 A2
B21 B22 B24 A3 B31
B32 B34 A4 b43 C3
A1 B11 B12 B13 A2
B21 B22 B23 A3 B31
B32 B33 A4 b44 C4
A1 B13 B14 A2 B23
B24 A3 b31 C1 a4 b42
c2
A1 B12 B14 A2 B22
B24 A3 b31 C1 a4 b43
c3
A1 B12 B13 A2 B22
B23 A3 b31 C1 a4 b44
c4
A1 B12 B13 B14 A2
B22 B23 B24 A3 b31
C1 A4 B42 B43 B44
A1 B13 B14 A2 B23
B24 A3 b31 C1 A4
b42 C2
A1 B12 B14 A2 B22
B24 A3 b31 C1 A4
b43 C3
A1 B12 B13 A2 B22
B23 A3 b31 C1 A4
b44 C4
A1 B13 B14 A2 B23
B24 A3 b32 C2 a4 b41
c1
A1 B11 B14 A2 B21
B24 A3 b32 C2 a4 b43
c3
A1 B11 B13 A2 B21
B23 A3 b32 C2 a4 b44
c4
A1 B11 B13 B14 A2
B21 B23 B24 A3 b31
C1 A4 B42 B43 B44
A1 B13 B14 A2 B23
B24 A3 b31 C1 A4
b44 C4
A1 B13 B14 A2 B23
B24 A3 b32 C2 a4 b41
c1
A1 B11 B14 A2 B21
B24 A3 b32 C2 a4 b43
c3
A1 B11 B13 A2 B21
B23 A3 b32 C2 a4 b44
c4
A1 B11 B13 B14 A2
B21 B23 B24 A3 b32
C2 A4 B41 B43 B44
A1 B13 B14 A2 B23
B24 A3 b32 C2 A4
b41 C1
A1 B11 B14 A2 B21
B24 A3 b32 C2 A4
b43 C3
A1 B11 B14 A2 B21
B24 A3 b32 C2 A4
b44 C4
A1 B12 B14 A2 B22
B24 A3 b33 C3 a4 b41
c1
A1 B11 B14 A2 B21
B24 A3 b33 C3 a4 b42
c2
A1 B11 B12 A2 B21
B22 A3 b33 C3 a4 b44
c4
A1 B11 B13 A2 B21
B23 A3 b32 C2 A4
b43 C3
A1 B11 B13 A2 B21
B23 A3 b32 C2 A4
b44 C4
A1 B12 B14 A2 B22
B24 A3 b33 C3 a4 b41
c1
A1 B11 B14 A2 B21
B24 A3 b33 C3 a4 b42
c2
A1 B11 B12 A2 B21
B22 A3 b33 C3 a4 b44
c4
A1 B11 B12 B14 A2
B21 B22 B24 A3 b33
C3 A4 B41 B42 B44
A1 B12 B14 A2 B22
B24 A3 b33 C3 A4
b41 C1
A1 B11 B14 A2 B21
B24 A3 b33 C3 A4
b42 C2
A1 B11 B14 A2 B21
B24 A3 b33 C3 A4
b43 C3
A1 B11 B14 A2 B21
B24 A3 b33 C3 A4
b44 C4
A1 B11 B12 A2 B21
B22 A3 b33 C3 A4
b44 C4
A1 B11 B12 A2 B21
B22 A3 b33 C3 A4
b44 C4
A1 B12 B13 A2 B21
B23 A3 b33 C3 A4
b44 C4
A1 B12 B13 A2 B21
B23 A3 b33 C3 A4
b44 C4

B23 A3 b34 C4 a4 b41
c1
A1 B11 B13 A2 B21
B23 A3 b34 C4 a4 b42
c2
A1 B11 B12 A2 B21
B22 A3 b34 C4 a4 b43
c3
A1 B11 B12 B13 A2
B21 B22 B23 A3 b34
C4 A4 B41 B42 B43
A1 B12 B13 A2 B22
B23 A3 b34 C4 A4
b41 C1
A1 B11 B13 A2 B21
B23 A3 b34 C4 A4
b42 C2
A1 B11 B13 A2 B21
B23 A3 b34 C4 A4
b43 C3
A1 B14 A2 b21 C1 a3
b32 c2 a4 b43 c3
A1 B13 A2 b21 C1 a3
b32 c2 a4 b44 c4
A1 B13 B14 A2 b21
C1 a3 b32 c2 A4 B43
B44
A1 B14 A2 b21 C1 a3
b32 c2 A4 b43 C3
A1 B13 A2 b21 C1 a3
b32 c2 A4 b44 C4
A1 B14 A2 b21 C1 a3
b33 c3 a4 b42 c2
A1 B12 A2 b21 C1 a3
b33 c3 a4 b44 c4
A1 B12 B14 A2 b21
C1 a3 b33 c3 A4 B42
B44
A1 B14 A2 b21 C1 a3
b33 c3 A4 b42 C2
A1 B12 A2 b21 C1 a3
b33 c3 A4 b44 C4
A1 B13 A2 b21 C1 a3
b34 c4 a4 b42 c2
A1 B12 A2 b21 C1 a3
b34 c4 a4 b43 c3
A1 B12 B13 A2 b21
C1 a3 b34 c4 A4 B42
B43
A1 B13 A2 b21 C1 a3
b34 c4 A4 b42 C2
A1 B12 A2 b21 C1 a3
b34 c4 A4 b43 C3
A1 B13 B14 A2 b21
C1 A3 B33 B34 a4
b42 c2
A1 B12 B14 A2 b21
C1 A3 B32 B34 a4
b43 c3
A1 B12 B13 A2 b21
C1 A3 B32 B33 a4
b44 c4
A1 B12 B13 B14 A2
b21 C1 A3 B32 B33
B34 A4 B42 B43 B44
A1 B13 B14 A2 b21
C1 A3 B33 B34 A4
b42 C2
A1 B12 B14 A2 b21
C1 A3 B32 B34 A4
b43 C3
A1 B12 B13 A2 b21
C1 A3 B32 B33 A4
b44 C4
A1 B14 A2 b21 C1 A3
b32 C2 a4 b43 c3
A1 B13 A2 b21 C1 A3

b32 C2 a4 b44 c4
A1 B13 B14 A2 b21
C1 A3 b32 C2 A4 B43
B44
A1 B14 A2 b21 C1 A3
b32 C2 A4 b43 C3
A1 B13 A2 b21 C1 A3
b32 C2 A4 b44 C4
A1 B14 A2 b21 C1 A3
b33 C3 a4 b42 c2
A1 B12 A2 b21 C1 A3
b33 C3 a4 b44 c4
A1 B12 B14 A2 b21
C1 A3 b33 C3 A4 B42
B44
A1 B14 A2 b21 C1 A3
b33 C3 A4 b42 C2
A1 B12 A2 b21 C1 A3
b33 C3 A4 b44 C4
A1 B13 A2 b22 C2 a3
b31 c1 a4 b43 c3
A1 B13 A2 b22 C2 a3
b31 c1 a4 b44 c4
A1 B13 B14 A2 b22
C2 a3 b31 c1 A4 B43
B44
A1 B14 A2 b22 C2 a3
b33 C3 A4 b41 C1
A1 B11 A2 b22 C2 A3
b33 C3 A4 b44 C4
A1 B13 A2 b22 C2 A3
b34 C4 a4 b41 c1
A1 B11 A2 b22 C2 A3
b33 C3 a4 b44 c4
A1 B11 B14 A2 b22
C2 A3 b33 C3 A4 B41
B44
A1 B13 A2 b22 C2 a3
b31 c1 A4 b43 C3
A1 B13 A2 b22 C2 a3
b31 c1 A4 b44 C4
A1 B14 A2 b22 C2 a3
b33 c3 A4 b43 C3
A1 B11 A2 b22 C2 a3
b33 c3 A4 b44 C4
A1 B13 A2 b22 C2 a3
b31 c1 A4 b43 C3
A1 B11 A2 b22 C2 a3
b33 c3 A4 b44 c4
A1 B11 B14 A2 b22
C2 a3 b33 c3 A4 B41
B44
A1 B14 A2 b22 C2 a3
b33 c3 A4 b41 C1
A1 B11 A2 b22 C2 a3
b34 c4 A4 b43 C3
A1 B13 B14 A2 b22
C2 A3 B33 B34 a4
b41 c1
A1 B11 B14 A2 b22
C2 A3 B31 B34 a4
b43 c3
A1 B11 B13 A2 b22
C2 A3 B31 B33 a4
b44 c4
A1 B11 B13 B14 A2
b22 C2 A3 B31 B33
B34 A4 B41 B43 B44
A1 B13 B14 A2 b22
C2 A3 B33 B34 A4

b41 C1
A1 B11 B14 A2 b22
C2 A3 B31 B34 A4
b43 C3
A1 B11 B13 A2 b22
C2 A3 B31 B33 A4
b44 C4
A1 B14 A2 b22 C2 A3
b31 C1 a4 b43 c3
A1 B13 A2 b22 C2 A3
b31 C1 a4 b44 c4
A1 B13 B14 A2 b22
C2 A3 b31 C1 A4 B43
B44
A1 B14 A2 b22 C2 A3
b31 C1 A4 b43 C3
A1 B13 A2 b22 C2 A3
b31 C1 A4 b44 C4
A1 B14 A2 b22 C2 A3
b33 C3 a4 b41 c1
A1 B11 A2 b22 C2 A3
b33 C3 a4 b44 c4
A1 B11 B14 A2 b22
C2 A3 b33 C3 A4 B41
B44
A1 B14 A2 b22 C2 A3
b33 C3 A4 b41 C1
A1 B11 A2 b22 C2 A3
b33 C3 A4 b44 C4
A1 B13 A2 b22 C2 A3
b34 C4 a4 b41 c1
A1 B11 A2 b22 C2 A3
b34 C4 a4 b43 c3
A1 B11 B13 A2 b22
C2 A3 b34 C4 A4 B41
B44
A1 B13 A2 b22 C2 A3
b34 C4 A4 b41 C1
A1 B11 A2 b22 C2 A3
b33 C3 A4 b44 C4
A1 B12 A2 b23 C3 a3
b31 c1 A4 b44 C4
A1 B14 A2 b23 C3 a3
b32 c2 a4 b41 c1
A1 B11 A2 b23 C3 a3
b32 c2 a4 b44 c4
A1 B12 B14 A2 b23
C3 a3 b31 c1 A4 B42
B44
A1 B14 A2 b23 C3 a3
b31 c1 A4 b42 C2
A1 B12 A2 b23 C3 a3
b31 c1 A4 b44 C4
A1 B12 A2 b23 C3 a3
b34 c4 a4 b41 c1
A1 B11 A2 b23 C3 a3
b32 c2 a4 b43 c3
A1 B11 B14 A2 b23
C3 a3 b31 c1 A4 B42
B44
A1 B14 A2 b23 C3 a3
b32 c2 A4 b41 C1
A1 B11 A2 b23 C3 a3
b32 c2 A4 b44 C4
A1 B12 A2 b23 C3 a3
b34 c4 a4 b41 c1
A1 B11 A2 b23 C3 a3
b34 c4 a4 b44 c4
A1 B11 B14 A2 b23
C3 a3 b31 c1 A4 B41
B44
A1 B14 A2 b23 C3 a3
b32 c2 A4 b41 C1
A1 B11 A2 b23 C3 a3
b32 c2 A4 b44 C4
A1 B12 A2 b23 C3 a3
b34 c4 a4 b41 c1
A1 B11 A2 b23 C3 a3
b32 c2 a4 b43 c3
A1 B11 B13 A2 b23
C3 a3 b32 c2 A4 B41
B44
A1 B14 A2 b23 C3 a3
b32 c2 A4 b41 C1
A1 B11 A2 b23 C3 a3
b32 c2 A4 b44 C4
A1 B12 A2 b23 C3 a3
b34 c4 a4 b41 c1
A1 B11 A2 b23 C3 a3
b34 c4 a4 b44 c4
A1 B11 B12 A2 b23
C3 a3 b31 c1 A4 B41
B44
A1 B14 A2 b23 C3 a3
b32 c2 A4 b41 C1
A1 B11 A2 b23 C3 a3
b32 c2 A4 b44 C4
A1 B12 A2 b23 C3 a3
b34 c4 A4 b42 C2
A1 B13 A2 b24 C4 a3
b31 c1 a4 b42 c2
A1 B12 A2 b24 C4 a3
b31 c1 a4 b43 c3
A1 B12 B13 A2 b24
C4 a3 b31 c1 A4 B42
B43
A1 B13 A2 b24 C4 a3
b31 c1 A4 b42 C2
A1 B12 A2 b24 C4 a3
b31 c1 A4 b43 C3
A1 B13 A2 b24 C4 a3
b32 c2 a4 b41 c1
A1 B11 A2 b24 C4 a3
b32 c2 a4 b43 c3
A1 B11 B13 A2 b24
C4 a3 b32 c2 A4 B41
B43
A1 B13 A2 b24 C4 a3
b31 c1 A4 b42 C2
A1 B12 A2 b24 C4 a3
b31 c1 A4 b43 C3
A1 B13 A2 b24 C4 a3
b32 c2 a4 b41 c1
A1 B11 A2 b24 C4 a3
b32 c2 a4 b43 c3
A1 B11 B12 A2 b24
C4 a3 b32 c2 A4 B41
B43
A1 B13 A2 b24 C4 a3
b31 c1 A4 b42 C2
A1 B12 A2 b24 C4 a3
b31 c1 A4 b43 C3
A1 B13 A2 b24 C4 a3
b32 c2 A4 b41 C1
A1 B11 A2 b24 C4 a3
b32 c2 A4 b43 C3
A1 B12 A2 b24 C4 a3
b33 c3 a4 b41 c1
A1 B11 A2 b24 C4 a3
b33 c3 a4 b42 c2
A1 B11 B12 A2 b24

C3 A3 B31 B34 a4
b42 c2
A1 B11 B12 A2 b23
C3 A3 B31 B32 a4
b44 c4
A1 B11 B12 B14 A2
b23 C3 A3 B31 B32
B34 A4 B41 B42 B44
A1 B12 B14 A2 b23
C3 A3 B32 B34 A4
b41 C1
A1 B11 B14 A2 b23
C3 A3 B31 B34 A4
b42 C2
A1 B11 B12 A2 b23
C3 A3 B31 B32 A4
b44 C4
A1 B14 A2 b23 C3 A3
b31 C1 a4 b42 c2
A1 B12 A2 b23 C3 A3
b31 C1 a4 b44 c4
A1 B12 B14 A2 b23
C3 A3 b31 C1 A4 B42
B44
A1 B14 A2 b23 C3 A3
b31 C1 A4 b42 C2
A1 B12 A2 b23 C3 A3
b31 C1 A4 b44 C4
A1 B14 A2 b23 C3 A3
b32 C2 a4 b41 c1
A1 B11 A2 b23 C3 A3
b32 C2 a4 b44 c4
A1 B11 B14 A2 b23
C3 A3 b32 C2 A4 B41
B44
A1 B14 A2 b23 C3 A3
b32 C2 A4 b41 C1
A1 B11 A2 b23 C3 A3
b32 C2 A4 b42 C2
A1 B13 A2 b24 C4 a3
b31 c1 a4 b42 c2
A1 B12 A2 b24 C4 a3
b31 c1 a4 b43 c3
A1 B12 B13 A2 b24
C4 a3 b31 c1 A4 B42
B43
A1 B13 A2 b24 C4 a3
b31 c1 A4 b42 C2
A1 B12 A2 b24 C4 a3
b31 c1 A4 b43 C3
A1 B13 A2 b24 C4 a3
b32 c2 a4 b41 c1
A1 B11 A2 b24 C4 a3
b32 c2 a4 b43 c3
A1 B11 B13 A2 b24
C4 a3 b32 c2 A4 B41
B43
A1 B13 A2 b24 C4 a3
b31 c1 A4 b42 C2
A1 B12 A2 b24 C4 a3
b31 c1 A4 b43 C3
A1 B13 A2 b24 C4 a3
b32 c2 A4 b41 C1
A1 B11 A2 b24 C4 a3
b32 c2 A4 b43 C3
A1 B12 A2 b24 C4 a3
b33 c3 a4 b41 c1
A1 B11 A2 b24 C4 a3
b33 c3 a4 b42 c2
A1 B11 B12 A2 b24

C4 a3 b33 c3 A4 B41
B42
A1 B12 A2 b24 C4 a3
b33 c3 A4 b41 C1
A1 B11 A2 b24 C4 a3
b33 c3 A4 b42 C2
A1 B12 B13 A2 b24
C4 A3 B32 B33 a4
b41 c1
A1 B11 B13 A2 b24
C4 A3 B31 B33 a4
b42 c2
A1 B11 B12 A2 b24
C4 A3 B31 B32 a4
b43 c3
A1 B11 B12 B13 A2
b24 C4 A3 B31 B32
B33 A4 B41 B42 B43
A1 B12 B13 A2 b24
C4 A3 B32 B33 A4
b41 C1
A1 B11 B13 A2 b24
C4 A3 B31 B33 A4
b42 C2
A1 B11 B12 A2 b24
C4 A3 B31 B32 A4
b43 C3
A1 B13 A2 b24 C4 A3
b31 C1 a4 b42 c2
A1 B12 A2 b24 C4 A3
b31 C1 a4 b43 c3
A1 B12 B13 A2 b24
C4 A3 b31 C1 A4 B42
B43
A1 B13 A2 b24 C4 A3
b31 C1 A4 b42 C2
A1 B12 A2 b24 C4 A3
b31 C1 A4 b43 C3
A1 B13 A2 b24 C4 A3
b32 C2 a4 b41 c1
A1 B11 A2 b24 C4 A3
b32 C2 a4 b43 c3
A1 B11 B13 A2 b24
C4 A3 B32 C2 A4 B41
B43
A1 B13 A2 b24 C4 A3
b32 C2 A4 b41 C1
A1 B11 A2 b24 C4 A3
b32 C2 A4 b43 C3
A1 B12 A2 b24 C4 A3
b33 C3 a4 b41 c1
A1 B11 A2 b24 C4 A3
b33 C3 a4 b42 c2
A1 B11 B12 A2 b24
C4 A3 b33 C3 A4 B41
B42
A1 B12 A2 b24 C4 A3
b33 C3 A4 b41 C1
A1 B11 A2 b24 C4 A3
b33 C3 A4 b42 C2
A1 b11 C1 a2 b22 c2
a3 b33 c3 a4 b44 c4
A1 b11 C1 a2 b22 c2
a3 b33 c3 A4 B44
A1 b11 C1 a2 b22 c2
a3 b33 c3 A4 b44 C4
A1 b11 C1 a2 b22 c2
a3 b34 c4 a4 b43 c3
A1 b11 C1 a2 b22 c2
a3 B32 a4 B43
A1 b11 C1 a2 b24 c4
a3 b32 c2 A4 b43 C3
A1 b11 C1 a2 b24 c4
a3 b33 c3 A4 b42 C2
A3 B33 a4 b42 c2
A1 b11 C1 a2 b24 c4
a3 B32 a4 b43 c3
A1 b11 C1 a2 b24 c4
A3 B32 B33 A4 B42
B43
A1 b11 C1 a2 b24 c4
A3 B33 A4 b42 C2
A1 b11 C1 a2 b24 c4
A3 B32 A4 b43 c3

A3 b32 C2 a4 b43 c3 b33 C3 a4 b42 c2 A1 b11 C1 A2 b23 C3 A3 b33 C3 A4 b44 C4 A1 b12 C2 A2 B24 a3
 A1 b11 C1 a2 b24 c4 A1 b11 C1 A2 B22 A3 A3 B32 A4 b44 C4 A1 b12 C2 a2 b21 c1 b31 c1 a4 b43 c3
 A3 b32 C2 A4 B43 b33 C3 a4 b44 c4 A1 b11 C1 A2 b23 C3 A3 b34 C4 a4 b43 c3 A1 b12 C2 A2 B23 a3
 A1 b11 C1 a2 b24 c4 A1 b11 C1 A2 B22 A3 b32 C2 a4 b44 c4 A1 b12 C2 a2 b21 c1 b31 c1 a4 b44 c4
 A3 b32 C2 A4 b43 C3 B24 A3 b33 C3 A4 A1 b11 C1 A2 b23 C3 A3 b34 C4 A4 B43 A1 b12 C2 A2 B23
 A1 b11 C1 a2 b24 c4 B42 B44 A3 b32 C2 A4 B44 A1 b12 C2 a2 b21 c1 B24 a3 b31 c1 A4 B43
 A3 b33 C3 a4 b42 c2 A1 b11 C1 A2 B24 A3 A1 b11 C1 A2 b23 C3 A3 b34 C4 A4 b43 C3 B44
 A1 b11 C1 a2 b24 c4 b33 C3 A4 b42 C2 A3 b32 C2 A4 b44 C4 A1 b12 C2 a2 b23 c3 A1 b12 C2 A2 B24 a3
 A3 b33 C3 A4 B42 A1 b11 C1 A2 B22 A3 A1 b11 C1 A2 b23 C3 a3 b31 c1 A4 b44 c4 b31 c1 A4 b43 C3
 A1 b11 C1 a2 b24 c4 b33 C3 A4 b44 C4 A3 b34 C4 a4 b42 c2 A1 b12 C2 a2 b23 c3 A1 b12 C2 A2 B23 a3
 A3 b33 C3 A4 b42 C2 A1 b11 C1 A2 B23 A3 A1 b11 C1 A2 b23 C3 a3 b31 c1 A4 B44 b31 c1 A4 b44 C4
 A1 b11 C1 A2 B24 a3 b34 C4 a4 b42 c2 A3 b34 C4 A4 B42 A1 b12 C2 a2 b23 c3 A1 b12 C2 A2 B24 a3
 b32 c2 a4 b43 c3 A1 b11 C1 A2 B22 A3 A1 b11 C1 A2 b23 C3 a3 b31 c1 A4 b44 C4 b33 c3 a4 b41 c1
 A1 b11 C1 A2 B23 a3 b34 C4 a4 b43 c3 A3 b34 C4 A4 b42 C2 A1 b12 C2 a2 b23 c3 A1 b12 C2 A2 B21 a3
 b32 c2 a4 b44 c4 A1 b11 C1 A2 B22 A1 b11 C1 A2 b24 C4 a3 b34 c4 a4 b41 c1 b33 c3 a4 b44 c4
 A1 b11 C1 A2 B23 B23 A3 b34 C4 A4 a3 b32 c2 a4 b43 c3 A1 b12 C2 a2 b23 c3 A1 b12 C2 A2 B21
 B24 a3 b32 c2 A4 B43 B42 B43 A1 b11 C1 A2 b24 C4 a3 b34 c4 A4 B41 B24 a3 b33 c3 A4 B41
 B44 A1 b11 C1 A2 B23 A3 a3 b32 c2 A4 B43 A1 b12 C2 a2 b23 c3 A1 b12 C2 A2 B24 a3
 A1 b11 C1 A2 B24 a3 b34 C4 A4 b42 C2 a3 b32 c2 A4 B43 A1 b12 C2 a2 b23 c3 b33 c3 A4 b41 C1
 b32 c2 A4 b43 C3 A1 b11 C1 A2 B22 A3 a3 b32 c2 A4 B43 A3 b34 c4 A4 b41 C1 A1 b12 C2 A2 B24 a3
 A1 b11 C1 A2 B23 a3 b34 C4 A4 b43 C3 A1 b11 C1 A2 b24 C4 A3 B34 a4 b41 c1 A1 b12 C2 A2 B21 a3
 b32 c2 A4 b44 C4 A1 b11 C1 A2 b22 C2 a3 b33 c3 a4 b42 c2 A1 b12 C2 a2 b23 c3 b33 c3 A4 b44 C4
 A1 b11 C1 A2 B24 a3 a3 b33 c3 a4 b44 c4 A1 b11 C1 A2 b24 C4 A3 B31 a4 b44 c4 A1 b12 C2 A2 B23 a3
 b33 c3 a4 b42 c2 A1 b11 C1 A2 b22 C2 a3 b33 c3 A4 B42 A1 b12 C2 a2 b23 c3 b34 c4 a4 b41 c1
 A1 b11 C1 A2 B22 a3 A1 b11 C1 A2 b22 C2 A1 b11 C1 A2 b24 C4 A3 B31 B34 A4 B41 A1 b12 C2 A2 B21 a3
 b33 c3 a4 b44 c4 A1 b11 C1 A2 b22 C2 a3 b33 c3 A4 b42 C2 B44 b34 c4 a4 b43 c3
 A1 b11 C1 A2 B22 a3 b33 c3 A4 b44 C4 A1 b11 C1 A2 b24 C4 A1 b12 C2 a2 b23 c3 A1 b12 C2 A2 B21
 B24 a3 b33 c3 A4 B42 A1 b11 C1 A2 b22 C2 A3 B33 a4 b42 c2 A3 B34 A4 b41 C1 B23 a3 b34 c4 A4 B41
 B44 a3 b34 c4 a4 b43 c3 A1 b11 C1 A2 b24 C4 A1 b12 C2 a2 b23 c3 B43
 A1 b11 C1 A2 B24 a3 A1 b11 C1 A2 b22 C2 A3 B32 a4 b43 c3 A3 B31 A4 b44 C4 A1 b12 C2 A2 B23 a3
 b33 c3 a4 b42 C2 a3 b34 c4 A4 B43 A1 b11 C1 A2 b24 C4 A1 b12 C2 a2 b23 c3 b34 c4 A4 b41 C1
 A1 b11 C1 A2 B22 a3 A1 b11 C1 A2 b22 C2 A3 B32 B33 A4 B42 A3 b31 C1 a4 b44 c4 A1 b12 C2 A2 B21 a3
 b33 c3 A4 b44 C4 a3 b34 c4 A4 b43 C3 B43 A1 b12 C2 a2 b23 c3 b34 c4 A4 b43 C3
 A1 b11 C1 A2 B23 a3 A1 b11 C1 A2 b22 C2 A1 b11 C1 A2 b24 C4 A3 b31 C1 A4 B44 A1 b12 C2 A2 B23
 b34 c4 a4 b42 c2 A3 B34 a4 b43 c3 A3 B33 A4 b42 C2 A1 b12 C2 a2 b23 c3 B24 A3 B33 B34 a4
 A1 b11 C1 A2 B22 a3 A1 b11 C1 A2 b22 C2 A1 b11 C1 A2 b24 C4 A3 b31 C1 A4 b44 C4 b41 c1
 b34 c4 a4 b43 c3 A3 B33 a4 b44 c4 A3 B32 A4 b43 C3 A1 b12 C2 a2 b23 c3 A1 b12 C2 A2 B21
 A1 b11 C1 A2 B22 A1 b11 C1 A2 b22 C2 A1 b11 C1 A2 b24 C4 A3 b34 C4 a4 b41 c1 B24 A3 B31 B34 a4
 B23 a3 b34 c4 A4 B42 A3 B33 B34 A4 B43 A3 b32 C2 a4 b43 c3 A1 b12 C2 a2 b23 c3 b43 c3
 B43 B44 A1 b11 C1 A2 b24 C4 A3 b34 C4 A4 B41 A1 b12 C2 a2 b23 c3 A1 b12 C2 A2 B21
 A1 b11 C1 A2 B23 a3 b34 C4 A4 b43 c3 A3 b32 C2 A4 B43 A1 b12 C2 a2 b23 c3 B23 A3 B31 B33 a4
 b34 c4 A4 b42 C2 A3 B34 A4 b43 C3 A3 b32 C2 A4 B43 A3 b34 C4 A4 b41 C1 b44 c4
 A1 b11 C1 A2 B22 a3 A1 b11 C1 A2 b22 C2 A3 b32 C2 A4 b43 C3 A1 b12 C2 a2 b24 c4 A1 b12 C2 A2 B21
 b34 c4 A4 b43 C3 A3 B33 A4 b44 C4 A3 b33 C3 A4 b42 C2 a3 b31 c1 a4 b43 c3 B23 B24 A3 B31 B33
 A1 b11 C1 A2 B23 A1 b11 C1 A2 b22 C2 A3 b33 C3 a4 b42 c2 A1 b12 C2 a2 b24 c4 B34 A4 B41 B43 B44
 B24 A3 B33 B34 a4 A3 b33 C3 a4 b44 c4 A1 b11 C1 A2 b24 C4 a3 b31 c1 A4 B43 A1 b12 C2 A2 B23
 b42 c2 A1 b11 C1 A2 b22 C2 A3 b33 C3 A4 B42 A1 b12 C2 a2 b24 c4 A1 b12 C2 A2 B23
 A1 b11 C1 A2 B22 A3 b33 C3 A4 B44 A1 b11 C1 A2 b24 C4 A1 b12 C2 a2 b24 c4 B24 A3 B33 B34 A4
 B24 A3 B32 B34 a4 A1 b11 C1 A2 b22 C2 A3 b33 C3 A4 b44 C2 A1 b12 C2 a2 b24 c4 b41 C1
 b43 c3 A3 b33 C3 A4 b44 C4 A1 b12 C2 a2 b21 c1 a3 b33 c3 a4 b41 c1 A1 b12 C2 A2 B21
 A1 b11 C1 A2 B22 A1 b11 C1 A2 b22 C2 a3 b33 c3 a4 b44 c4 A1 b12 C2 a2 b24 c4 B24 A3 B31 B34 A4
 B23 A3 B32 B33 a4 A3 b34 C4 a4 b43 c3 A1 b12 C2 a2 b21 c1 a3 b33 c3 A4 B41 b43 C3
 b44 c4 A1 b11 C1 A2 b22 C2 a3 b33 c3 A4 B44 A1 b12 C2 a2 b24 c4 A1 b12 C2 A2 B21
 A1 b11 C1 A2 B22 A3 b34 C4 A4 B43 A1 b12 C2 a2 b21 c1 a3 b33 c3 A4 b41 C1 B23 A3 B31 B33 A4
 B23 B24 A3 B32 B33 A1 b11 C1 A2 b22 C2 a3 b33 c3 A4 b44 C4 A1 b12 C2 a2 b24 c4 b44 C4
 B34 A4 B42 B43 B44 A3 b34 C4 A4 b43 C3 A1 b12 C2 a2 b21 c1 A3 B33 a4 b41 c1 A1 b12 C2 A2 B24 A3
 A1 b11 C1 A2 B23 A1 b11 C1 A2 b23 C3 a3 b34 c4 a4 b43 c3 A1 b12 C2 a2 b24 c4 b31 C1 a4 b43 c3
 B24 A3 B33 B34 A4 a3 b32 c2 a4 b44 c4 A1 b12 C2 a2 b21 c1 A3 B31 a4 b43 c3 A1 b12 C2 A2 B23 A3
 b42 C2 A1 b11 C1 A2 b23 C3 a3 b34 c4 A4 B43 A1 b12 C2 a2 b24 c4 A3 B31 a4 b43 c3 b31 C1 a4 b44 c4
 A1 b11 C1 A2 B22 a3 b32 c2 A4 B44 A1 b12 C2 a2 b21 c1 A1 b12 C2 a2 b24 c4 A1 b12 C2 A2 B23
 B24 A3 B32 B34 A4 A1 b11 C1 A2 b23 C3 a3 b34 c4 A4 b43 C3 A3 B31 B33 A4 B41 B24 A3 B31 C1 A4
 b43 C3 A3 b32 c2 A4 b44 C4 A1 b12 C2 a2 b21 c1 B43 B43 B44
 B23 A3 B32 B33 A4 A1 b11 C1 A2 b23 C3 A1 b12 C2 a2 b21 c1 A1 b12 C2 a2 b24 c4 A1 b12 C2 A2 B24 A3
 b44 C4 a3 b34 c4 a4 b42 c2 A3 B33 A4 b41 C1 A1 b12 C2 a2 b24 c4 b31 C1 A4 b43 C3
 A1 b11 C1 A2 B24 A3 A1 b11 C1 A2 b23 C3 A3 B31 A4 b43 C3 A3 b31 C1 a4 b43 c3 A1 b12 C2 A2 B23 A3
 b32 C2 a4 b43 c3 A1 b11 C1 A2 b23 C3 A1 b12 C2 a2 b24 c4 A3 b31 C1 a4 b43 c3 A1 b12 C2 A2 B21 a3
 A1 b11 C1 A2 B23 A3 A1 b11 C1 A2 b23 C3 A3 B34 A4 b43 C3 A1 b12 C2 a2 b24 c4 b33 c3 a4 b44 c4
 b32 C2 a4 b44 c4 A3 B34 a4 b42 c2 A3 B33 A4 b43 C3 A1 b12 C2 a2 b24 c4 A1 b12 C2 A2 B21
 A1 b11 C1 A2 B23 A1 b11 C1 A2 b23 C3 A3 B34 A4 b43 C3 A3 b31 C1 A4 b43 C3 B24 A3 b33 C3 A4
 B24 A3 b32 C2 A4 A3 B32 a4 b44 c4 A3 B33 A4 b44 C4 A1 b12 C2 a2 b24 c4 B41 B44
 B43 B44 A1 b11 C1 A2 b23 C3 A1 b12 C2 a2 b21 c1 A3 b33 C3 a4 b41 c1 A1 b12 C2 A2 B24 A3
 A1 b11 C1 A2 B24 A3 A1 b11 C1 A2 b23 C3 A3 b33 C3 a4 b44 c4 A1 b12 C2 a2 b24 c4 b33 C3 A4 b41 C1
 b32 C2 A4 b43 C3 A3 B32 B34 A4 B42 A1 b12 C2 a2 b21 c1 A3 b33 C3 A4 B41 A1 b12 C2 A2 B21 a3
 A1 b11 C1 A2 B23 A3 B44 A3 b33 C3 A4 B44 A3 b33 C3 A4 b41 c1 b33 C3 A4 b44 c4
 b32 C2 A4 b44 C4 A1 b11 C1 A2 b23 C3 A3 b33 C3 A4 B44 A1 b12 C2 a2 b24 c4 A1 b12 C2 A2 B24 A3
 A1 b11 C1 A2 B24 A3 A3 B34 A4 b42 C2 A1 b12 C2 a2 b21 c1 A3 b33 C3 A4 b41 C1 B23 A3 B31 B33 A4

Controllo su tutti i 29 bit del frame

• $k = 3, j = 3$

a1 b11 c1 a2 b22 c2 a3 b33 c3	a3 b33 c3	A1 B11 a2 b22 c2 a3 b33 c3 C1	A1 B11 B12 A2 b23 C3 A3 B31 B32 C1 C2	A1 b12 C2 A2 B21 B23 A3 B31 B33 C1 C3
a1 b11 c1 a2 b22 c2 A3 B33 C3	A3 B33 C3	A1 B11 B13 a2 b22 c2 A3 B31 B33 C1 C3	A1 B12 A2 b23 C3 A3 b31 C1 C2	A1 b12 C2 A2 B23 A3 b31 C1 C3
a1 b11 c1 a2 b22 c2 A3 B33 C3	a1 b12 c2 A2 b21 C1 A3 b33 C3	A1 B13 a2 b22 c2 A3 b31 C1 C3	A1 B11 A2 b23 C3 A3 b32 C2 C1	A1 b12 C2 A2 B21 A3 b33 C3 C1
a1 b11 c1 a2 b23 c3 a3 b32 c2	a1 b12 c2 A2 b23 C3 a3 b31 c1	A1 B11 a2 b22 c2 A3 b33 C3 C1	A1 b11 C1 a2 b22 c2 a3 b33 c3	A1 b12 C2 A2 b21 C1 a3 b33 c3
a1 b11 c1 a2 b23 c3 A3 B32 C2	a1 b12 c2 A2 b23 C3 A3 B31 C1	A1 B12 a2 b23 c3 a3 b31 c1 C2	A1 b11 C1 a2 b22 c2 A3 B33 C3	A1 b12 C2 A2 b21 C1 A3 B33 C3
a1 b11 c1 a2 b23 c3 A3 b32 C2	a1 b12 c2 A2 b23 C3 A3 b31 C1	A1 B11 a2 b23 c3 a3 b32 c2 C1	A1 b11 C1 a2 b22 c2 A3 b33 C3	A1 b12 C2 A2 b21 C1 A3 b33 C3
a1 b11 c1 A2 B23 a3 b32 c2 C3	a1 b13 c3 a2 b21 c1 a3 b32 c2	A1 B11 B12 a2 b23 c3 A3 B31 B32 C1 C2	A1 b11 C1 a2 b23 c3 a3 b32 c2	A1 b12 C2 A2 b23 C3 a3 b31 c1
a1 b11 c1 A2 B22 a3 b33 c3 C2	A3 B32 C2	A1 B12 a2 b23 c3 A3 b31 C1 C2	A1 b11 C1 a2 b23 c3 A3 B32 C2	A1 b12 C2 A2 b23 C3 a3 b31 c1
a1 b11 c1 A2 B22 B23 A3 B32 B33 C2 C3	a1 b13 c3 a2 b21 c1 A3 b32 C2	A1 B11 a2 b23 c3 A3 b32 C2 C1	A1 b11 C1 a2 b23 c3 A3 B32 C2	A1 b12 C2 A2 b23 C3 A3 B31 C1
a1 b11 c1 A2 B23 A3 b32 C2 C3	a1 b13 c3 a2 b22 c2 A3 B32 C2	A1 B12 B13 A2 B22 B23 a3 b31 c1 C2 C3	A1 b11 C1 A2 B23 a3 b32 c2 C3	A1 b12 C2 A2 b23 C3 A3 b31 C1
a1 b11 c1 A2 B22 A3 b33 C3 C2	A3 B31 C1	A1 B11 B13 A2 B21 B23 a3 b32 c2 C1 C3	A1 b11 C1 A2 B22 a3 b33 c3 C2	A1 b13 C2 a2 b21 c1 A3 B32 C2
a1 b11 c1 A2 B22 B23 A3 B32 B33 C2 C3	A3 b31 C1	A1 B11 B12 A2 B21 B22 a3 b33 c3 C1 C2	A1 b11 C1 A2 B22 A3 b32 C2 C3	A1 b13 C3 a2 b21 c1 A3 B32 C2
a1 b11 c1 A2 B23 A3 b32 C2 C3	a1 b13 c3 a2 b22 c2 A3 B31 C1	A1 B11 B12 B13 A2 B21 B22 B23 A3 B31 B32 B33 C1 C2 C3	A1 b11 C1 A2 B23 A3 b32 C2 C3	A1 b13 C3 a2 b21 c1 a3 b32 c2
a1 b11 c1 A2 B22 A3 b33 C3 C2	a1 b13 c3 a2 b22 c2 A3 b31 C1	A1 B12 B13 A2 B22 B23 a3 b31 C1 C2 C3	A1 b11 C1 A2 B22 A3 b32 C2 C3	A1 b13 C3 a2 b21 c1 A3 B32 C2
a1 b11 c1 A2 b23 C3 a3 b32 c2	a1 b13 c3 A2 B22 a3 b31 c1 C2	A1 B11 B13 A2 B21 B23 A3 b32 C2 C1 C3	A1 b11 C1 A2 B22 A3 b32 C2 C3	A1 b13 C3 a2 b22 c2 a3 b31 c1
a1 b11 c1 A2 b23 C3 A3 B32 C2	a1 b13 c3 A2 B21 a3 b32 c2 C1	A1 B11 B12 A2 B21 B22 A3 b33 C3 C1 C2	A1 b11 C1 A2 B22 A3 b32 C2 C3	A1 b13 C3 a2 b22 c2 a3 b31 c1
a1 b11 c1 A2 b23 C3 A3 b33 C3	a1 b13 c3 A2 B21 B22 A3 B31 B32 C1 C2	A1 B12 B13 A2 B22 B23 a3 b32 c2 C1 C3	A1 b11 C1 A2 B22 A3 b32 C2 C3	A1 b13 C3 a2 b22 c2 a3 b31 c1
a1 b11 c1 A2 b23 C3 A3 b32 C2	a1 b13 c3 A2 B22 A3 b31 C1 C2	A1 B11 B13 A2 B21 B23 A3 b32 C2 C1 C3	A1 b11 C1 A2 B22 A3 b32 C2 C3	A1 b13 C3 a2 b22 c2 a3 b31 c1
a1 b11 c1 A2 b23 C3 A3 b32 C2	a1 b13 c3 A2 B21 A3 b32 C2 C1	A1 B11 B12 A2 B21 B22 A3 b33 C3 C1 C2	A1 b11 C1 A2 B22 C2 A3 B33 C3	A1 b13 C3 A2 B22 a3 b31 c1 C2
a1 b12 c2 a2 b21 c1 a3 b33 c3	a1 b13 c3 A2 b21 C1 a3 b32 c2	A1 B13 A2 b21 C1 a3 b32 c2 C3	A1 b11 C1 A2 b22 C2 A3 b33 C3	A1 b13 C3 A2 B21 a3 b32 c2 C1
a1 b12 c2 a2 b21 c1 A3 B33 C3	a1 b13 c3 A2 b21 C1 A3 B32 C2	A1 B12 A2 b21 C1 a3 b33 c3 C2	A1 b11 C1 A2 b23 C3 a3 b32 c2	A1 b13 C3 A2 B21 B22 A3 B31 B32 C1 C2
a1 b12 c2 a2 b21 c1 A3 B33 C3	a1 b13 c3 A2 b21 C1 A3 b32 C2	A1 B12 B13 A2 b21 C1 A3 B32 B33 C2 C3	A1 b11 C1 A2 b23 C3 A3 B32 C2	A1 b13 C3 A2 B22 A3 b31 C1 C2
a1 b12 c2 a2 b23 c3 a3 b31 c1	a1 b13 c3 A2 b22 C2 a3 b31 c1	A1 B13 A2 b21 C1 A3 b32 C2 C3	A1 b11 C1 A2 b23 C3 A3 b32 C2	A1 b13 C3 A2 B21 A3 b32 C2 C1
a1 b12 c2 a2 b23 c3 A3 B31 C1	a1 b13 c3 A2 b22 C2 A3 B31 C1	A1 B12 A2 b21 C1 A3 b33 C3 C2	A1 b12 C2 a2 b21 c1 a3 b33 c3	A1 b13 C3 A2 b21 C1 a3 b32 c2
a1 b12 c2 a2 b23 c3 A3 b31 C1	A1 B13 a2 b21 c1 a3 b32 c2 C3	A1 B11 A2 b22 C2 a3 b31 c1 C3	A1 b12 C2 a2 b21 c1 A3 B33 C3	A1 b13 C3 A2 b21 C1 A3 B32 C2
a1 b12 c2 A2 B23 a3 b31 c1 C3	A1 B12 a2 b21 c1 a3 b33 c3 C2	A1 B11 A2 b22 C2 a3 b33 c3 C1	A1 b12 C2 a2 b23 c3 a3 b31 c1	A1 b13 C3 A2 B22 a3 b31 c1 C2
a1 b12 c2 A2 B21 a3 b33 C3 C1	A1 B12 B13 a2 b21 c1 A3 B32 B33 C2 C3	A1 B11 B13 A2 b22 C2 A3 B31 B33 C1 C3	A1 b12 C2 a2 b23 c3 a3 b31 c1	A1 b13 C3 A2 b22 C2 a3 b31 c1
a1 b12 c2 A2 B23 A3 b31 C1 C3	A1 B13 a2 b21 c1 A3 b32 C2 C3	A1 B13 A2 b22 C2 A3 b31 C1 C3	A1 b12 C2 a2 b23 c3 A3 B31 C1	A1 b13 C3 A2 b22 C2 A3 B31 C1
a1 b12 c2 A2 B21 A3 b33 C3 C1	A1 B12 a2 b21 c1 A3 b33 C3 C2	A1 B12 A2 b23 C3 a3 b31 c1 C2	A1 b12 C2 A2 B23 a3 b31 c1 C3	A1 b13 C3 A2 b22 C2 A3 b31 C1
a1 b12 c2 A2 b21 C1 b33 c3	A1 B13 a2 b22 c2 a3 b31 c1 C3	A1 B11 A2 b23 C3 a3 b32 c2 C1	A1 b12 C2 A2 B21 a3 b33 c3 C1	A1 b13 C3 A2 b22 C2 A3 b31 C1

• $k = 3, j = 4$

a1 b11 c1 a2 b22 c2 a3 b33 c3 C4	a1 b11 c1 a2 b22 c2 A3 B33 B34 C3 C4	a1 b11 c1 a2 b22 c2 A3 b34 C4 C3	a1 b11 c1 a2 b23 c3 a3 b34 c4 C2	a1 b11 c1 a2 b23 c3 A3 b32 C2 C4
a1 b11 c1 a2 b22 c2 a3 b34 c4 c3	a1 b11 c1 a2 b22 c2 A3 b33 C3 C4	a1 b11 c1 a2 b23 c3 a3 b32 c2 C4	a1 b11 c1 a2 b23 c3 A3 B32 B34 C2 C4	a1 b11 c1 a2 b23 c3 A3 b34 C4 C2

A1 B11 B14 A2 b22
C2 a3 b33 c3 C1 C4
A1 B11 B13 A2 b22
C2 a3 b34 c4 C1 C3
A1 B11 B13 B14 A2
b22 C2 A3 B31 B33
B34 C1 C3 C4
A1 B13 B14 A2 b22
C2 A3 b31 C1 C3 C4
A1 B11 B14 A2 b22
C2 A3 b33 C3 C1 C4
A1 B11 B13 A2 b22
C2 A3 b34 C4 C1 C3
A1 B12 B14 A2 b23
C3 a3 b31 c1 C2 C4
A1 B11 B14 A2 b23
C3 a3 b32 c2 C1 C4
A1 B11 B12 A2 b23
C3 a3 b34 c4 C1 C2
A1 B11 B12 B14 A2
b23 C3 A3 B31 B32
B34 C1 C2 C4
A1 B12 B14 A2 b23
C3 A3 b31 C1 C2 C4
A1 B11 B13 A2 b23
C3 A3 b32 C2 C1 C4
A1 B11 B12 A2 b23
C3 A3 b34 C4 C1 C2
A1 B12 B13 A2 b24
C4 a3 b31 c1 C2 C3
A1 B11 B13 A2 b24
C4 a3 b32 c2 C1 C3
A1 B11 B12 A2 b24
C4 a3 b33 c3 C1 C2
A1 B11 B12 B13 A2
b24 C4 A3 B31 B32
B33 C1 C2 C3
A1 B12 B13 A2 b24
C4 A3 b31 C1 C2 C3
A1 B11 B13 A2 b24
C4 A3 b32 C2 C1
a3 b33 c3 C4
A1 b11 C1 a2 b22 c2
a3 b34 c4 C3
A1 b11 C1 a2 b22 c2
A3 B33 B34 C3 C4
A1 b11 C1 a2 b22 c2
A3 b33 C3 C4
A1 b11 C1 a2 b22 c2
A3 b34 C4 C3
A1 b11 C1 a2 b23 c3
a3 b32 c2 C4
A1 b11 C1 a2 b23 c3
a3 b34 c4 C2
A1 b11 C1 a2 b23 c3
A3 B32 B34 C2 C4
A1 B11 C1 a2 b23 c3
A3 b32 C2 C4
A1 b11 C1 a2 b23 c3
A3 b34 C4 C2
A1 b11 C1 a2 b24 c4
a3 b32 c2 C3
A1 b11 C1 a2 b24 c4
a3 b33 c3 C2
A1 b11 C1 a2 b24 c4
A3 B32 B33 C2 C3
A1 b11 C1 a2 b24 c4
A3 b32 C2 C3
A1 b11 C1 a2 b24 c4
A3 b33 C3 C2
A1 b11 C1 a2 B23
B24 a3 b32 c2 C3 C4
A1 b11 C1 A2 B22
B24 a3 b33 c3 C2 C4
A1 b11 C1 A2 B22
B23 a3 b34 c4 C2 C3
A1 b11 C1 A2 B22
B23 A3 b34 C4 C2 C3
A1 b11 C1 A2 b22 C2
a3 b33 c3 C4
A1 b11 C1 A2 b22 C2
a3 b34 c4 C3
A1 b11 C1 A2 b22 C2
A3 B33 B34 C3 C4
A1 b11 C1 A2 b22 C2
A3 b33 C3 C4
A1 b11 C1 A2 b22 C2
A3 b34 C4 C3
A1 b11 C1 A2 b23 C3
a3 b32 c2 C4
A1 b11 C1 A2 b23 C3
a3 b34 c4 C2
A1 b11 C1 A2 b23 C3
A3 B32 B34 C2 C4
A1 b11 C1 A2 b23 C3
a3 b31 c1 C4
A1 b12 C2 a2 b23 c3
a3 b34 c4 C1
A1 b12 C2 a2 b23 c3
A3 B31 B34 C1 C4
A1 b12 C2 a2 b23 c3
A3 b31 C1 C4
A1 b12 C2 a2 b23 c3
A3 b34 C4 C1
A1 b12 C2 a2 b24 c4
a3 b32 c2 C3
A1 b11 C1 a2 b24 c4
a3 b33 c3 C2
A1 b11 C1 a2 b24 c4
A3 B32 B33 C2 C3
A1 b11 C1 a2 b24 c4
A3 B32 B33 C2 C3
A1 b11 C1 a2 b24 c4
A3 b33 C3 C2
A1 b11 C1 A2 B23
B23 a3 b32 c2 C3 C4
A1 b11 C1 A2 B22
B24 a3 b33 c3 C2 C4
A1 b11 C1 A2 B22
B23 a3 b34 c4 C2 C3
A1 b11 C1 A2 B22
B23 A3 b34 C4 C2 C3
A1 b11 C1 A2 b22 C2
a3 b33 c3 C4
A1 b11 C1 A2 b22 C2
a3 b34 c4 C3
A1 b11 C1 A2 b22 C2
A3 B33 B34 C3 C4
A1 b11 C1 A2 b23 C3
A3 b34 C4 C2
A1 b11 C1 A2 b24 C4
a3 b32 c2 C3
A1 b11 C1 A2 b24 C4
a3 b33 c3 C2
A1 b11 C1 A2 b24 C4
A3 B32 B33 C2 C4
A1 b11 C1 A2 b24 C4
A3 b32 C2 C3
A1 b11 C1 A2 b24 C4
A3 b33 C3 C2
A1 b12 C2 a2 b21 c1
a3 b33 c3 C4
A1 b12 C2 a2 b21 c1
a3 b34 c4 C3
A1 b12 C2 a2 b21 c1
A3 B33 B34 C3 C4
A1 b12 C2 a2 b21 c1
a3 b33 C3 C4
A1 b12 C2 a2 b21 c1
A3 b34 C4 C3
A1 b12 C2 a2 b23 c3
a3 b31 c1 C4
A1 b12 C2 a2 b23 c3
a3 b34 c4 C1
A1 b12 C2 a2 b23 c3
A3 B31 B34 C1 C4
A1 b12 C2 a2 b23 c3
A3 b31 C1 C4
A1 b12 C2 a2 b23 c3
A3 B32 B34 C2 C4
A1 b13 C3 a2 b21 c1
a3 b32 c2 C4
A1 b13 C3 a2 b21 c1
a3 b34 c4 C2
A1 b13 C3 a2 b21 c1
A3 B32 B34 C2 C4
A1 b13 C3 a2 b21 c1
a3 b32 C2 C4
A1 b13 C3 a2 b21 c1
A3 b34 C4 C2
A1 b13 C3 a2 b22 c2
a3 b31 c1 C4
A1 b13 C3 a2 b22 c2
a3 b34 c4 C1
A1 b13 C3 a2 b22 c2
A3 B31 B34 C1 C4
A1 b13 C3 A2 b22 C2
A3 b31 C1 C4
A1 b13 C3 A2 b22 C2
A3 b34 C4 C1
A1 b13 C3 A2 b24 C4
a3 b31 c1 C2
A1 b13 C3 A2 b24 C4
a3 b32 c2 C1
A1 b13 C3 A2 b24 C4
A3 B31 B32 C1 C2
A1 b13 C3 A2 b24 C4
A3 b31 C1 C2
A1 b13 C3 A2 b24 C4
A3 b32 C2 C1
A1 b14 C4 a2 b21 c1
a3 b32 c2 C3
A1 b14 C4 a2 b21 c1
a3 b33 c3 C2
A1 b14 C4 a2 b23 C3
A3 B31 B32 C1 C2
A1 b14 C4 a2 b23 C3
A3 b31 C1 C2
A1 b14 C4 A2 b23 C3
A3 b32 C2 C1

• $k = 4, j = 3$

a1 b11 c1 a2 b22 c2 a3
 b33 c3 A4
 a1 b11 c1 a2 b22 c2
 A3 a4 b43 c3
 a1 b11 c1 a2 b22 c2
 A3 B33 A4 B43 C3
 a1 b11 c1 a2 b22 c2
 A3 A4 b43 C3
 a1 b11 c1 a2 b22 c2
 A3 B33 C3 A4
 a1 b11 c1 a2 b23 c3 a3
 b32 c2 A4
 a1 b11 c1 a2 b23 c3
 A3 a4 b42 c2
 a1 b11 c1 a2 b23 c3
 A3 B32 A4 B42 C2
 a1 b11 c1 a2 b23 c3
 A3 A4 b42 C2
 a1 b11 c1 a2 b23 c3
 A3 b32 C2 A4
 a1 b11 c1 A2 a3 b32
 c2 a4 b43 c3
 a1 b11 c1 A2 B23 a3
 b32 c2 A4 B43 C3
 a1 b11 c1 A2 a3 b32
 c2 A4 b43 C3
 a1 b12 c2 A2 a3 b33
 c3 a4 b42 c2
 a1 b11 c1 A2 B22 a3
 b33 c3 A4 B42 C2
 a1 b11 c1 A2 a3 b33
 c3 A4 b42 C2
 a1 b11 c1 A2 B23 A3
 B33 a4 b42 c2 C3
 a1 b11 c1 A2 B22 A3
 B32 a4 b43 c3 C2
 a1 b11 c1 A2 B22 B23
 A3 B32 B33 A4 B42
 B43 C2 C3
 a1 b11 c1 A2 B23 A3
 B33 A4 b42 C2 C3
 a1 b11 c1 A2 B22 A3
 B32 A4 b43 C3 C2
 a1 b11 c1 A2 A3 b32
 C2 a4 b43 c3
 a1 b11 c1 A2 B23 A3
 b32 C2 A4 B43 C3
 a1 b11 c1 A2 A3 b32
 C2 A4 b43 C3
 a1 b11 c1 A2 A3 b33
 C3 a4 b42 c2
 a1 b11 c1 A2 B22 A3
 b33 C3 A4 B42 C2
 a1 b11 c1 A2 A3 b33
 C3 A4 b42 C2
 a1 b11 c1 A2 b22 C2
 a3 b33 c3 A4
 a1 b11 c1 A2 b22 C2
 A3 a4 b43 c3
 a1 b11 c1 A2 b22 C2
 A3 B33 A4 B43 C3
 a1 b11 c1 A2 b22 C2
 A3 A4 b43 C3
 a1 b11 c1 A2 b23 C3
 a3 b32 c2 A4
 a1 b11 c1 A2 b23 C3
 A3 a4 b42 c2
 a1 b11 c1 A2 b23 C3
 A3 B32 A4 B42 C2
 a1 b12 c2 A2 a3 b31
 c1 A4 b43 C3
 a1 b12 c2 A2 a3 b33
 c3 a4 b41 c1
 a1 b12 c2 A2 B21 a3
 b33 c3 A4 B41 C1
 a1 b12 c2 A2 a3 b33
 c3 A4 b41 C1
 a1 b12 c2 A2 B23 A3
 B33 a4 b41 c1 C3
 a1 b12 c2 A2 B21 A3
 B31 a4 b43 c3 C1
 a1 b12 c2 A2 B21 B23
 A3 B31 B33 A4 B41
 B43 C1 C3
 a1 b12 c2 A2 B23 A3
 B33 A4 b41 C1 C3
 a1 b12 c2 A2 B21 A3
 B31 A4 b43 C3 C1
 a1 b12 c2 A2 A3 b31
 C1 a4 b43 c3
 a1 b12 c2 A2 B23 A3
 b31 C1 A4 B43 C3
 a1 b12 c2 A2 A3 b31
 C1 A4 b43 C3
 a1 b12 c2 A2 A3 b33
 C3 a4 b41 c1
 a1 b12 c2 A2 B21 A3
 b33 C3 A4 B41 C1
 a1 b12 c2 A2 A3 b33
 C3 A4 b41 c1
 a1 b12 c2 A2 B21 A3
 b33 C3 A4 B41 C1
 a1 b12 c2 A2 b21 C1
 a3 b33 c3 A4
 a1 b12 c2 A2 b21 C1
 A3 a4 b43 c3
 a1 b12 c2 A2 b21 C1
 A3 B33 A4 B43 C3
 a1 b12 c2 A2 b21 C1
 A3 A4 b43 C3
 a1 b12 c2 A2 b21 C1
 A3 b33 C3 A4
 a1 b12 c2 A2 b23 C3
 a3 b31 c1 A4
 a1 b12 c2 A2 b23 C3
 A3 a4 b41 c1
 a1 b12 c2 A2 b23 C3
 A3 B31 A4 B41 C1

a1 b12 c2 A2 b23 C3
 A3 A4 b41 C1
 a1 b12 c2 A2 b23 C3
 A3 b31 C1 A4
 a1 b13 c3 a2 b21 c1 a3
 b32 c2 A4
 a1 b13 c3 a2 b21 c1
 A3 a4 b42 c2
 a1 b13 c3 a2 b21 c1
 A3 B32 A4 B42 C2
 a1 b13 c3 a2 b21 c1
 A3 A4 b42 C2
 a1 b13 c3 a2 b21 c1
 A3 b32 C2 A4
 a1 b13 c3 a2 b22 c2 a3
 b31 c1 A4
 a1 b13 c3 a2 b22 c2
 A3 a4 b41 c1
 a1 b13 c3 a2 b22 c2
 A3 B31 A4 B41 C1
 a1 b13 c3 a2 b22 c2
 A3 A4 b41 C1
 a1 b13 c3 a2 b22 c2
 A3 b31 C1 A4
 a1 b13 c3 A2 a3 b31
 c1 a4 b42 c2
 a1 b13 c3 A2 B22 a3
 b31 c1 A4 B42 C2
 a1 b13 c3 A2 a3 b31
 c1 A4 b42 C2
 a1 b13 c3 A2 a3 b32
 c2 a4 b41 c1
 a1 b13 c3 A2 B21 a3
 b32 c2 A4 B41 C1
 a1 b13 c3 A2 a3 b32
 c2 A4 b41 C1
 a1 b13 c3 A2 B22 A3
 B32 a4 b41 c1 C2
 a1 b13 c3 A2 B21 A3
 B31 a4 b42 c2 C1
 a1 b13 c3 A2 B21 B22
 A3 B31 B32 A4 B41
 B42 C1 C2
 a1 b13 c3 A2 B22 A3
 B32 A4 b41 C1 C2
 a1 b13 c3 A2 B21 A3
 B31 A4 b42 C2 C1
 a1 b13 c3 A2 A3 b31
 C1 a4 b42 c2
 a1 b13 c3 A2 B22 A3
 b31 C1 A4 B42 C2
 a1 b13 c3 A2 A3 b31
 C1 a4 b42 c2
 a1 b13 c3 A2 B21 A3
 b32 C2 A4 B41 C1
 a1 b13 c3 A2 A3 b32
 C2 A4 b41 C1
 a1 b13 c3 A2 B21 A3
 b32 C2 A4 B41 C1
 a1 b13 c3 A2 A3 b32
 C2 A4 b41 C1
 a1 b13 c3 A2 b21 C1
 a3 b32 c2 A4
 a1 b13 c3 A2 b21 C1
 A3 a4 b42 c2
 a1 b13 c3 A2 b21 C1
 A3 B32 A4 B42 C2
 a1 b13 c3 A2 b21 C1
 A3 A4 b42 C2
 a1 b13 c3 A2 b21 C1
 A3 b32 C2 A4
 a1 b13 c3 A2 b22 C2
 a3 b31 c1 A4
 a1 b13 c3 A2 b22 C2
 A3 a4 b41 c1

a1 b13 c3 A2 b22 C2
 A3 B31 A4 B41 C1
 a1 b13 c3 A2 b22 C2
 A3 A4 b41 C1
 a1 b13 c3 A2 b22 C2
 A3 b31 C1 A4
 A1 a2 b21 c1 a3 b32
 c2 a4 b43 c3
 A1 B13 a2 b21 c1 a3
 b32 c2 A4 B43 C3
 A1 a2 b21 c1 a3 b32
 c2 A4 b43 C3
 A1 a2 b21 c1 a3 b33
 c3 a4 b42 c2
 A1 B12 a2 b21 c1 a3
 B32 a4 b43 c3 C2
 A1 a2 b21 c1 A3 b32
 C2 a4 b43 c3
 A1 B13 a2 b21 c1 A3
 b32 C2 A4 B43 C3
 A1 a2 b21 c1 A3 b32
 C2 A4 b43 C3
 C3 a4 b42 c2
 A1 B12 a2 b21 c1 A3
 b33 C3 A4 B42 C2
 A1 a2 b21 c1 A3 b33
 C3 A4 b42 C2
 A1 a2 b22 c2 a3 b31
 c1 a4 b43 c3
 A1 B13 a2 b22 c2 a3
 b31 c1 A4 B43
 A1 a2 b22 c2 a3 b31
 c1 A4 b43 C3
 A1 a2 b22 c2 a3 b33
 c3 a4 b41 c1
 A1 B11 a2 b22 c2 a3
 b33 c3 A4 B41 C1
 A1 a2 b22 c2 a3 b33
 c3 A4 b41 C1
 A1 B13 a2 b22 c2 A3
 B33 a4 b41 c1 C3
 A1 B11 a2 b22 c2 A3
 B31 A4 b43 C3 C1
 A1 B11 B13 a2 b22 c2
 A3 B31 B33 A4 B41
 B43 C1 C3
 A1 B13 a2 b22 c2 A3
 B33 A4 b41 C1 C3
 A1 B11 a2 b22 c2 A3
 B31 A4 b43 C3 C1
 A1 a2 b22 c2 A3 b31
 C1 a4 b43 c3
 A1 B13 a2 b22 c2 A3
 b31 C1 A4 B43 C3
 A1 a2 b22 c2 A3 b31
 C1 a4 b43 c3
 A1 B11 a2 b22 c2 A3
 B33 c3 A4 B41 C1 C3
 A1 B12 B13 a2 B22
 B23 a3 b31 c1 A4 B42
 B43 C2 C3
 A1 B13 A2 B23 a3
 b31 c1 A4 b42 c2 C3
 A1 B12 A2 B22 a3
 b31 c1 a4 b43 c3 C2
 A1 B12 B13 A2 B22
 B23 a3 b31 c1 A4 B42
 B43 C2 C3
 A1 B13 A2 B23 a3
 b31 c1 A4 b42 C2 C3
 A1 B12 A2 B22 a3
 b31 c1 A4 b43 C3 C2
 A1 B13 A2 B23 a3
 b32 c2 a4 b41 c1 C3
 A1 B11 A2 B21 a3
 b32 c2 a4 b43 c3 C1
 A1 B11 B13 A2 B21
 B23 a3 b32 c2 A4 B41
 B43 C1 C3
 A1 B13 A2 B23 a3
 b32 c2 A4 b41 C1 C3
 A1 B11 A2 B21 a3
 b32 c2 A4 b43 C3 C1
 A1 B12 A2 B22 a3
 b33 c3 A4 b41 c1 C2
 A1 B11 A2 B21 a3
 b33 c3 a4 b42 c2 C1
 A1 B11 B12 A2 B21
 B22 a3 b33 c3 A4 B41
 B42 C1 C2
 A1 B12 A2 B22 a3
 b33 c3 A4 b41 C1 C2
 A1 B11 A2 B21 a3
 b33 c3 A4 b42 C2 C1
 A1 B12 B13 A2 B22
 B23 A3 B32 B33 a4

b41 c1 C2 C3
A1 B11 B13 A2 B21
B23 A3 B31 B33 a4
b42 c2 C1 C3
A1 B11 B12 A2 B21
B22 A3 B31 B32 a4
b43 c3 C1 C2
A1 B11 B12 B13 A2
B21 B22 B23 A3 B31
B32 B33 A4 B41 B42
B43 C1 C2 C3
A1 B12 B13 A2 B22
B23 A3 B32 B33 A4
b41 C1 C2 C3
A1 B11 B13 A2 B21
B23 A3 B31 B33 A4
b42 C2 C1 C3
A1 B11 B12 A2 B21
B22 A3 B31 B32 A4
b43 C3 C1 C2
A1 B13 A2 B23 A3
b31 C1 a4 b42 c2 C3
A1 B12 A2 B22 A3
b31 C1 a4 b43 c3 C2
A1 B12 B13 A2 B22
B23 A3 b31 C1 A4
B42 B43 C2 C3
A1 B13 A2 B23 A3
b31 C1 A4 b42 C2 C3
A1 B12 A2 B22 A3
b31 C1 A4 b43 C3 C2
A1 B13 A2 B23 A3
b32 C2 a4 b41 c1 C3
A1 B11 A2 B21 A3
b32 C2 a4 b43 c3 C1
A1 B11 B13 A2 B21
B23 A3 b32 C2 A4
B41 B43 C1 C3
A1 B13 A2 B23 A3
b32 C2 A4 b41 C1 C3
A1 B11 A2 B21 A3
b32 C2 A4 b43 c3
A1 B12 A2 B22 A3
b33 C3 a4 b41 c1 C2
A1 A2 B21 A3
b33 C3 A4 b42 C2 C1
A1 A2 b21 C1 a3 b32
c2 a4 b43 c3
A1 B13 A2 b21 C1 a3
b32 c2 A4 B43 C3
A1 A2 b21 C1 a3 b32
c2 A4 b43 C3
A1 A2 b21 C1 a3 b33
c3 a4 b42 c2
A1 B12 A2 b21 C1 a3
b33 c3 A4 B42 C2
A1 A2 b21 C1 a3 b33
c3 A4 b42 C2
A1 B13 A2 b21 C1 A3
B33 a4 b42 c2 C3
A1 B12 A2 b21 C1 A3
B32 a4 b43 c3 C2
A1 B12 B13 A2 b21
C1 A3 B32 B33 A4
B42 B43 C2 C3
A1 B13 A2 b21 C1 A3
B32 a4 b43 c3 C2
A1 B12 B13 A2 b21
C1 A3 B32 B33 A4
B42 B43 C2 C3
A1 B13 A2 b22 C2 A3
b43 C3 C1 C2
A1 B13 A2 B23 A3
b31 C1 a4 b42 c2 C3
A1 B12 A2 B22 A3
b31 C1 a4 b43 c3 C2
A1 B12 B13 A2 B22
B23 A3 b31 C1 A4
B42 B43 C2 C3
A1 B13 A2 B23 A3
b31 C1 A4 b42 C2 C3
A1 B12 A2 B22 A3
b31 C1 A4 b43 C3
A1 B12 C2 A2 B21 A3
b33 c3 A4 B41 C1
A1 b12 C2 A2 a3 b33
c3 A4 b41 C1
A1 b12 C2 A2 B23 A3
B33 a4 b41 c1 C3
A1 b12 C2 A2 B21 A3
B31 a4 b43 c3 C1
A1 b12 C2 A2 B21
B23 A3 B31 B33 A4
B41 B43 C1 C3
A1 b12 C2 A2 B23 A3
B33 A4 b41 C1 C3
A1 b12 C2 A2 B21 A3
B31 A4 b43 C3 C1
A1 b12 C2 A2 A3 b31
C1 a4 b43 c3
A1 b12 C2 A2 B23 A3
b31 C1 A4 B43 C3
A1 b12 C2 A2 A3 b31
C3 a4 b41 c1
A1 b12 C2 A2 B21 A3
b33 C3 A4 B41 C1
A1 b12 C2 A2 A3 b33
C3 A4 b41 C1
A1 b12 C2 A2 b21 C1
a3 b33 c3 A4
A1 b12 C2 A2 b21 C1
A3 a4 b43 c3
A1 b12 C2 A2 b21 C1
A3 B33 A4 B43 C3
A1 b12 C2 A2 b21 C1
A3 A4 b43 C3
A1 b12 C2 A2 b21 C1
A3 b33 C3 A4
A1 b12 C2 A2 b23 C3
a3 b31 c1 A4
A1 b12 C2 A2 b23 C3
A3 a4 b41 c1
A1 b12 C2 A2 b23 C3
A3 B31 A4 B41 C1
A1 b12 C2 A2 b23 C3
A3 A4 b41 C1
A1 b12 C2 A2 b23 C3
A3 b31 C1 A4

A3 b34 C4 A4 B41 C1	a1 b12 c2 A2 B21 B23	A3 b33 C3 A4 b44 C4	a1 b13 c3 a2 b21 c1 a3	b32 c2 a4 b41 c1
A3 B31 B33 a4 b44 c4	A3 B31 B33 a4 b44 c4	a1 b12 c2 A2 B21 C1	b32 c2 a4 b44 c4	a1 b13 c3 a2 b24 c4 a3
A3 b34 C4 A4 b41 C1	C1 C3	A3 b34 C4 a4 b43 c3	a1 b13 c3 a2 b21 c1 a3	b32 c2 A4 B41 C1
a1 b12 c2 a2 b24 c4 a3	a1 b12 c2 A2 B21 B23	a1 b12 c2 A2 B21 C1	b32 c2 A4 B44 C4	a1 b13 c3 a2 b24 c4 a3
b31 c1 a4 b43 c3	B24 A3 B31 B33 B34	A3 b34 C4 A4 B43 C3	a1 b13 c3 a2 b21 c1 a3	A3 B32 a4 b41 c1 C2
a1 b12 c2 a2 b24 c4 a3	A4 B41 B43 B44 C1	a1 b12 c2 A2 b21 C1	b34 c4 a4 b42 c2	a1 b13 c3 a2 b24 c4
b31 c1 A4 B43 C3	C3 C4	A3 b34 C4 A4 b43 C3	a1 b13 c3 a2 b21 c1 a3	A3 B31 a4 b42 c2 C1
a1 b12 c2 a2 b24 c4 a3	a1 b12 c2 A2 B23 B24	a3 b31 c1 a4 b44 c4	b34 c4 A4 B42 C2	a1 b13 c3 a2 b24 c4
b33 c3 a4 b41 c1	A3 B33 B34 A4 b41	a1 b12 c2 A2 b23 C3	a1 b13 c3 a2 b21 c1 a3	A3 B31 B32 A4 B41
a1 b12 c2 a2 b24 c4 a3	C1 C3 C4	a3 b31 c1 A4 B44 C4	b34 c4 A4 B42 C2	B42 C1 C2
b33 c3 A4 B41 C1	a1 b12 c2 A2 B21 B24	a1 b12 c2 A2 b23 C3	a1 b13 c3 a2 b21 c1	a1 b13 c3 a2 b24 c4
a1 b12 c2 a2 b24 c4 a3	A3 B31 B34 A4 b43	a3 b31 c1 A4 b44 C4	A3 B34 a4 b42 c2 C4	A3 B31 A4 b42 C2 C1
b33 c3 A4 B41 C1	C3 C1 C4	a1 b12 c2 A2 b23 C3	a1 b13 c3 a2 b21 c1	A3 B32 A4 b41 C1 C2
a1 b12 c2 a2 b24 c4 a3	a1 b12 c2 A2 B21 B23	a3 b34 c4 a4 b41 c1	A3 B32 a4 b44 c4 C2	a1 b13 c3 a2 b24 c4
b33 c3 A4 b41 C1	A3 B31 B33 A4 b44	a1 b12 c2 A2 b23 C3	A3 B32 B34 A4 B42	a1 b13 c3 a2 b24 c4
a1 b12 c2 a2 b24 c4	C4 C1 C3	a3 b34 c4 A4 b41 C1	B44 C2 C4	a1 b13 c3 a2 b24 c4
A3 B33 a4 b41 c1 C3	a1 b12 c2 A2 B24 A3	a3 b34 c4 A4 b41 C1	a1 b13 c3 a2 b21 c1	A3 b31 C1 A4 b42 C2
a1 b12 c2 a2 b24 c4	b31 C1 a4 b43 c3 C4	a1 b12 c2 A2 b23 C3	A3 B32 B34 A4 B42	A3 b31 C1 A4 b42 C2
A3 B31 a4 b43 c3 C1	a1 b12 c2 A2 B23 A3	a3 b34 c4 A4 b41 C1	a1 b13 c3 a2 b21 c1	a1 b13 c3 a2 b24 c4
a1 b12 c2 a2 b24 c4	b31 C1 a4 b44 c4 C3	a1 b12 c2 A2 b23 C3	A3 B34 A4 b42 C2 C4	A3 b31 C1 A4 B42 C4
A3 B31 B33 A4 B43	a1 b12 c2 A2 B23 B24	A3 B34 a4 b41 c1 C4	a1 b13 c3 a2 b21 c1	a1 b13 c3 a2 b24 c4
C1 C3	A3 b31 C1 A4 B43	a1 b12 c2 A2 b23 C3	A3 B32 A4 b44 C4 C2	A3 b31 C1 A4 B42 C2
a1 b12 c2 a2 b24 c4	B44 C3 C4	A3 B31 a4 b44 c4 C1	a1 b13 c3 a2 b21 c1	a1 b13 c3 a2 b24 c4
A3 B33 A4 b41 C1 C3	a1 b12 c2 A2 B24 A3	a1 b12 c2 A2 b23 C3	A3 B32 B34 A4 B42	a1 b13 c3 a2 b24 c4
a1 b12 c2 a2 b24 c4	b31 C1 A4 b43 C3 C4	A3 B31 B34 A4 B41	B44 C2 C4	a1 b13 c3 a2 b24 c4
A3 B31 A4 b43 C3 C1	a1 b12 c2 A2 B23 A3	B44 C1 C4	a1 b13 c3 a2 b21 c1	A3 b31 C1 A4 B42 C2
a1 b12 c2 a2 b24 c4	b31 C1 A4 b44 C4 C3	a1 b12 c2 A2 b23 C3	A3 b32 C2 A4 B44 C4	a1 b13 c3 a2 b24 c4
A3 b31 C1 a4 b43 c3	a1 b12 c2 A2 B24 A3	A3 B34 A4 b41 C1 C4	a1 b13 c3 a2 b21 c1	A3 b32 C2 A4 B41 C1
a1 b12 c2 a2 b24 c4	b33 C3 a4 b41 c1 C4	a1 b12 c2 A2 b23 C3	A3 b32 C2 A4 b44 c4	a1 b13 c3 a2 b21 c1
A3 b31 C1 A4 B43 C3	a1 b12 c2 A2 B21 A3	A3 B31 A4 b44 C4 C1	a1 b13 c3 a2 b22 c2 a3	a1 b13 c3 a2 b24 c4
a1 b12 c2 a2 b24 c4	b33 C3 a4 b44 c4 C1	a1 b12 c2 A2 b23 C3	A3 b34 C4 a4 b42 c2	a1 b13 c3 A2 B22 a3
A3 b31 C1 A4 b43 C3	a1 b12 c2 A2 B21 B24	A3 b31 C1 a4 b44 c4	a1 b13 c3 a2 b21 c1	b31 c1 a4 b44 c4 C2
a1 b12 c2 a2 b24 c4	A3 b33 C3 A4 B41	a1 b12 c2 A2 b23 C3	A3 B34 C4 A4 B42 C2	a1 b13 c3 A2 B22 B24
A3 b33 C3 a4 b41 c1	B44 C1 C4	A3 b31 C1 A4 B44 C4	a1 b13 c3 a2 b21 c1	a3 b31 c1 A4 B42 B44
a1 b12 c2 a2 b24 c4	a1 b12 c2 A2 B24 A3	a1 b12 c2 A2 b23 C3	A3 b34 C4 A4 b42 C2	C2 C4
A3 b33 C3 A4 B41 C1	b33 C3 A4 b41 C1 C4	A3 b31 C1 A4 b44 C4	a1 b13 c3 a2 b22 c2 a3	a1 b13 c3 A2 B24 a3
a1 b12 c2 a2 b24 c4	a1 b12 c2 A2 B21 A3	a1 b12 c2 A2 b23 C3	b31 c1 a4 b44 c4	b31 c1 A4 b42 C2 C4
A3 b33 C3 A4 b41 C1	b33 C3 A4 b44 C4 C1	A3 b34 C4 a4 b41 c1	a1 b13 c3 a2 b22 c2 a3	a1 b13 c3 A2 B22 a3
a1 b12 c2 A2 B24 a3	a1 b12 c2 A2 B23 A3	a1 b12 c2 A2 b23 C3	b31 c1 A4 B44 C4	b31 c1 A4 b44 C4 C2
b31 c1 a4 b43 c3 C4	b34 C4 a4 b41 c1 C3	A3 b34 C4 A4 B41 C1	a1 b13 c3 a2 b22 c2 a3	a1 b13 c3 A2 B24 a3
a1 b12 c2 A2 B23 a3	a1 b12 c2 A2 B21 A3	a1 b12 c2 A2 b23 C3	b31 c1 A4 b44 C4	b32 c2 a4 b41 c1 C4
A3 b33 C3 A4 B41 B44	b34 C4 a4 b43 c3 C1	A3 b34 C4 A4 b42 C4	a1 b13 c3 a2 b22 c2 a3	a1 b13 c3 A2 B21 a3
C1 C4	a1 b12 c2 A2 B23 B24	a3 b31 c1 a4 b43 c3	b34 c4 a4 b41 c1	b32 c2 a4 b44 c4 C1
a1 b12 c2 A2 B24 a3	A3 b34 C4 A4 B41 B44	a1 b12 c2 A2 b24 C4	a1 b13 c3 a2 b22 c2 a3	a1 b13 c3 A2 B21 B24
b31 c1 A4 b43 C3 C4	B43 C1 C3	a3 b31 c1 A4 B43 C3	b34 c4 A4 B41 C1	a3 b32 C2 A4 B41 B44
a1 b12 c2 A2 B23 a3	a1 b12 c2 A2 B23 A3	a1 b12 c2 A2 b24 C4	b34 c4 A4 b41 C1	C1 C4
b31 c1 A4 b44 C4 C3	b34 C4 A4 b41 C1 C3	a3 b31 c1 A4 b43 C3	a1 b13 c3 a2 b22 c2	a1 b13 c3 A2 B24 a3
a1 b12 c2 A2 B24 a3	a1 b12 c2 A2 B21 A3	a1 b12 c2 A2 b24 C4	A3 B34 a4 b41 c1 C4	b32 c2 A4 B41 C1 C4
b33 c3 a4 b41 c1 C4	b33 C3 A4 b44 C4	A3 b33 c3 a4 b41 c1	a1 b13 c3 a2 b22 c2	a1 b13 c3 A2 B21 a3
a1 b12 c2 A2 B21 a3	a1 b12 c2 A2 b21 C1	a1 b12 c2 A2 b24 C4	A3 B31 a4 b44 c4 C1	b34 c4 A4 b42 C2 C1
b33 c3 a4 b44 c4 C1	a3 b33 c3 A4 B44 C4	a3 b33 c3 A4 B41 C1	a1 b13 c3 a2 b22 c2	a1 b13 c3 A2 B22 a3
a1 b12 c2 A2 B21 B24	a1 b12 c2 A2 b21 C1	a1 b12 c2 A2 b24 C4	A3 B31 B34 A4 B41	b34 c4 a4 b42 c2 C1
a3 b33 c3 A4 B41 B44	a3 b33 c3 A4 b44 C4	A3 b33 c3 A4 B42 C4	B44 C1 C4	a1 b13 c3 A2 B21 B22
C1 C4	a1 b12 c2 A2 B21 B23	A3 B34 a4 b41 c1 C3	a1 b13 c3 a2 b22 c2	a3 b34 c4 A4 B41 B42
a1 b12 c2 A2 B24 a3	A3 b34 C4 A4 B43 C3	a1 b12 c2 A2 b24 C4	A3 B31 A4 b44 C4 C1	C1 C2
b33 c3 A4 b41 C1 C4	a1 b12 c2 A2 b21 C1	A3 B31 a4 b43 c3 C1	a1 b13 c3 a2 b22 c2	a1 b13 c3 A2 B22 a3
a1 b12 c2 A2 B21 a3	a3 b34 c4 A4 b43 c3	a1 b12 c2 A2 b24 C4	A3 b31 C1 a4 b44 c4	b34 c4 A4 b41 C1 C2
b33 c3 A4 b44 C4 C1	a1 b12 c2 A2 b21 C1	A3 B31 B33 A4 B41	a1 b13 c3 a2 b22 c2	a1 b13 c3 A2 B21 a3
a1 b12 c2 A2 B23 a3	a3 b34 c4 A4 b43 C3	B43 C1 C3	a1 b13 c3 a2 b22 c2	b34 c4 A4 b42 C2 C1
a1 b12 c2 A2 B21 a3	a1 b12 c2 A2 b21 C1	a1 b12 c2 A2 b24 C4	A3 b31 C1 A4 B44 C4	a1 b13 c3 A2 B22 B24
b34 c4 a4 b41 c1 C3	A3 B34 a4 b43 c3 C4	A3 B33 A4 b41 C1 C3	a1 b13 c3 a2 b22 c2	A3 B32 B34 a4 b41 c1
a1 b12 c2 A2 B21 a3	a1 b12 c2 A2 b21 C1	a1 b12 c2 A2 b24 C4	A3 b31 C1 A4 b44 C4	C2 C4
b34 c4 a4 b43 c3 C1	a1 b12 c2 A2 b21 C1	A3 B31 A4 b43 C3 C1	a1 b13 c3 a2 b22 c2	a1 b13 c3 A2 B21 B24
a1 b12 c2 A2 B21 B23	a3 b34 c4 A4 B43 C3	a1 b12 c2 A2 b24 C4	A3 b34 C4 a4 b41 c1	A3 B31 B34 a4 b42 c2
a3 b34 c4 A4 B41 B43	a1 b12 c2 A2 b21 C1	A3 B31 B33 A4 B41	a1 b13 c3 a2 b22 c2	C1 C4
C1 C3	a3 b34 c4 A4 b43 C3	B43 C1 C3	a1 b13 c3 a2 b22 c2	a1 b13 c3 A2 B21 B22
a1 b12 c2 A2 B23 a3	a1 b12 c2 A2 b21 C1	a1 b12 c2 A2 b24 C4	A3 b34 C4 A4 B41 C1	A3 B31 B32 a4 b44 C1
b31 c1 A4 b44 C4 C3	A3 B34 a4 b43 c3 C4	A3 B33 A4 b41 C1 C3	a1 b13 c3 a2 b22 c2	C1 C2
a1 b12 c2 A2 B24 a3	a1 b12 c2 A2 b21 C1	a1 b12 c2 A2 b24 C4	A3 b31 C1 A4 B44 C4	a1 b13 c3 A2 B22 B24
b33 c3 a4 b41 c1 C4	A3 B33 a4 b43 c3 C1	a1 b12 c2 A2 b24 C4	a1 b13 c3 a2 b22 c2	A3 B32 B34 a4 b41 c1
a1 b12 c2 A2 B21 a3	a1 b12 c2 A2 b21 C1	A3 B31 a4 b43 c3 C1	A3 B31 A4 b44 C4 C1	C2 C4
b33 c3 a4 b44 c4 C1	a3 b33 c3 A4 B44 C4	a1 b12 c2 A2 b24 C4	a1 b13 c3 a2 b22 c2	a1 b13 c3 A2 B21 B22
a1 b12 c2 A2 B21 B24	a1 b12 c2 A2 b21 C1	A3 b33 c3 A4 b41 C1	A3 b34 C4 A4 b41 C1	B24 A3 B31 B32 B34
a3 b33 c3 A4 B41 B44	a3 b34 c4 a4 b43 c3	A3 B33 A4 b41 C1 C3	b31 c1 A4 B42 C2	A4 B41 B42 B44 C1
C1 C4	a1 b12 c2 A2 B21 B23	a1 b12 c2 A2 b24 C4	a1 b13 c3 a2 b24 c4 a3	C2 C4
a1 b12 c2 A2 B24 a3	A3 b33 A4 b43 c3 C1	A3 B31 A4 b43 C3 C1	a1 b13 c3 a2 b24 c4 a3	a1 b13 c3 A2 B22 B24
b33 c3 A4 b41 C1 C4	a1 b12 c2 A2 b21 C1	a1 b12 c2 A2 b24 C4	b31 c1 A4 B42 C2	A3 B32 B34 A4 b41
a1 b12 c2 A2 B21 a3	a3 b34 c4 A4 b43 c3	A3 b33 c3 A4 B41 C1	a1 b13 c3 a2 b24 c4 a3	C1 C2 C4
b33 c3 A4 b44 C4 C1	a1 b12 c2 A2 b21 C1	a1 b12 c2 A2 b24 C4	b31 c1 A4 B42 C2	

A1 B12 a2 b24 c4 A3
b31 C1 A4 b43 C3 C2
A1 B13 a2 b24 c4 A3
b32 C2 a4 b41 c1 C3
A1 B11 a2 b24 c4 A3
b32 C2 a4 b43 c3 C1
A1 B11 B13 a2 b24
c4 A3 b32 C2 A4 B41
B43 C1 C3
A1 B13 a2 b24 c4 A3
b32 C2 A4 b41 C1 C3
A1 B11 a2 b24 c4 A3
b32 C2 A4 b43 C3 C1
A1 B12 a2 b24 c4 A3
b33 C3 a4 b41 c1 C2
A1 B11 a2 b24 c4 A3
b33 C3 a4 b42 c2 C1
A1 B11 B12 a2 b24
c4 A3 b33 C3 A4 B41
B42 C1 C2
A1 B12 a2 b24 c4 A3
b33 C3 A4 b41 C1 C2
A1 B11 a2 b24 c4 A3
b33 C3 A4 b42 C2 C1
A1 B13 B14 A2 B23
B24 a3 b31 c1 a4 b42
c2 C3 C4
A1 B12 B14 A2 B22
B24 a3 b31 c1 a4 b43
c3 C2 C4
A1 B12 B13 A2 B22
B23 a3 b31 c1 a4 b44
c4 C2 C3
A1 B12 B13 B14 A2
B22 B23 B24 a3 b31
c1 A4 B42 B43 B44
C2 C3 C4
A1 B13 B14 A2 B23
B24 a3 b31 c1 A4 b42
C2 C3 C4
A1 B12 B14 A2 B22
B24 a3 b31 c1 A4 b43
C3 C2 C4
A1 B12 B13 A2 B22
B23 a3 b31 c1 A4 b44
C4 C2 C3
A1 B13 B14 A2 B23
B24 a3 b31 c1 A4 b43
C3 C2 C4
A1 B13 B14 A2 B22
B24 a3 b31 c1 A4 b43
C3 C2 C4
A1 B11 B13 A2 B21
B21 B22 B23 A3 B31
B32 B33 A4 b44 c4 B41
C2 C3
A1 B11 B12 B13 B14
A2 B21 B22 B23 B24
A3 B31 B32 B33 B34
A4 B41 B42 B43 B44
C1 C2 C3 C4
A1 B12 B13 B14 A2
B22 B23 B24 A3 B32
B33 B34 A4 b41 C1
C2 C3 C4
A1 B11 B12 B13 A2
B21 B22 B24 A3 B31
B32 B33 A4 b43 c3 C1
C2 C4
A1 B11 B12 B13 A2
B21 B22 B23 A3 B31
B32 B33 A4 b43 c3
C1 C2 C4
A1 B11 B12 B13 A2
B21 B22 B23 A3 B31
B32 B33 A4 b43 C3
C1 C2 C4
A1 B11 B12 B13 A2
B21 B22 B23 A3 B31
B32 B33 A4 b44 C4
C1 C2 C3
A1 B13 B14 A2 B23
B24 A3 b31 C1 a4 b42
c2 C1 C4
A1 B11 B12 A2 B21
B21 B22 B24 A3 B31
B32 B33 A4 b42 C2
C1 C3 C4
A1 B11 B12 B14 A2
B21 B22 B24 A3 B31
B32 B33 A4 b43 C3
C1 C2 C4
A1 B11 B12 B13 A2
B21 B22 B23 A3 B31
B32 B33 A4 b44 C4
C1 C2 C3
A1 B13 B14 A2 B23
B24 A3 b31 C1 a4 b42
c2 C3 C4
A1 B11 B12 A2 B21
B21 B22 B24 A3 B31
B32 B33 c3 a4 b44
c4 C1 C2

a3 b31 c1 A4 b43 C3	A1 b13 C3 a2 b22 c2	b32 c2 A4 b41 C1 C4	A1 b13 C3 A2 b21 C1	A3 B31 a4 b42 c2 C1
A1 b12 C2 A2 b24 C4	A3 B34 a4 b41 c1 C4	A1 b13 C3 A2 B21 a3	a3 b34 c4 A4 B42 C2	A1 b13 C3 A2 b24 C4
a3 b33 c3 A4 B41 C1	A1 b13 C3 a2 b22 c2	b32 c2 A4 b44 C4 C1	A1 b13 C3 A2 b21 C1	A3 B31 B32 A4 B41
A1 b12 C2 A2 b24 C4	A3 B31 a4 b44 c4 C1	A1 b13 C3 A2 B22 a3	a3 b34 c4 A4 b42 C2	B42 C1 C2
a3 b33 c3 A4 b41 C1	A1 b13 C3 a2 b22 c2	b34 c4 a4 b41 c1 C2	A1 b13 C3 A2 b21 C1	A1 b13 C3 A2 b24 C4
A1 b12 C2 A2 b24 C4	A3 B31 B34 A4 B41	A1 b13 C3 A2 B21 a3	A3 B34 a4 b42 c2 C4	A3 B32 A4 b41 C1 C2
A3 B33 a4 b41 c1 C3	B44 C1 C4	b34 c4 a4 b42 c2 C1	A1 b13 C3 A2 b21 C1	A1 b13 C3 A2 b24 C4
A1 b12 C2 A2 b24 C4	A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 B21	A3 B32 a4 b44 c4 C2	A3 B31 A4 b42 C2 C1
A3 B31 a4 b43 c3 C1	A3 B34 A4 b41 C1 C4	B22 a3 b34 c4 A4 B41	A1 b13 C3 A2 b21 C1	A3 B31 C3 A2 b24 C4
A1 b12 C2 A2 b24 C4	A1 b13 C3 a2 b22 c2	B42 C1 C2	A3 B32 B34 A4 B42	A3 b31 C1 a4 b42 c2
A3 B31 B33 A4 B41	A3 B31 A4 b44 C4 C1	A1 b13 C3 A2 B22 a3	B44 C2 C4	A1 b13 C3 A2 b24 C4
B43 C1 C3	A1 b13 C3 a2 b22 c2	b34 c4 A4 b41 C1 C2	A1 b13 C3 A2 b21 C1	A3 b31 C1 A4 B42 C2
A1 b12 C2 A2 b24 C4	A3 b31 C1 a4 b44 c4	A1 b13 C3 A2 B21 a3	A3 B34 A4 b42 C2 C4	A1 b13 C3 A2 b24 C4
A3 B33 A4 b41 C1 C3	A1 b13 C3 a2 b22 c2	b34 c4 A4 b42 C2 C1	A1 b13 C3 A2 b21 C1	A3 b31 C1 A4 b42 C2
A1 b12 C2 A2 b24 C4	A3 b31 C1 A4 B44 C4	A1 b13 C3 A2 B22	A3 B32 A4 b44 C4 C2	A1 b13 C3 A2 b24 C4
A3 B33 A4 b41 C1 C3	A1 b13 C3 a2 b22 c2	B24 A3 B32 B34 a4	A1 b13 C3 A2 b21 C1	A3 b32 C2 a4 b44 c4
A1 b12 C2 A2 b24 C4	A3 b31 C1 A4 b44 C4	b41 c1 C2 C4	A3 b32 C2 a4 b44 c4	A1 b13 C3 A2 b21 C1
A3 B31 A4 b43 C3 C1	A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 B21	A1 b13 C3 A2 b21 C1	A3 b32 C2 A4 B41 C1
A1 b12 C2 A2 b24 C4	A3 b34 C4 a4 b41 c1	B24 A3 B31 B34 a4	A3 b32 C2 A4 B44 C4	A1 b13 C3 A2 b21 C1
A3 b31 C1 a4 b43 c3	A1 b13 C3 a2 b22 c2	b42 c2 C1 C4	A1 b13 C3 A2 b21 C1	A3 b32 C2 A4 b41 C1
A1 b12 C2 A2 b24 C4	A3 b34 C4 A4 B41 C1	A1 b13 C3 A2 B21	A3 b32 C2 A4 b44 C4	A1 b14 C4 a2 b21 c1
A3 b31 C1 A4 B43 C3	A1 b13 C3 a2 b22 c2	B22 A3 B31 B32 a4	A1 b13 C3 A2 b21 C1	a3 b32 c2 a4 b43 c3
A1 b12 C2 A2 b24 C4	A3 b34 C4 A4 b41 C1	b44 c4 C1 C2	A3 b34 C4 a4 b42 c2	A1 b14 C4 a2 b21 c1
A3 B31 C1 A4 b43 C3	A1 b13 C3 a2 b24 c4	A1 b13 C3 A2 B21	A1 b13 C3 A2 b21 C1	a3 b32 c2 A4 B21 C3
A1 b12 C2 A2 b24 C4	a3 b31 c1 a4 b42 c2	B22 B24 A3 B31 B32	A3 b34 C4 A4 B42 C2	A1 b14 C4 a2 b21 c1
A3 b33 C3 a4 b41 c1	A1 b13 C3 a2 b24 c4	B34 A4 B41 B42 B44	A1 b13 C3 A2 b21 C1	a3 b32 c2 A4 b43 C3
A1 b12 C2 A2 b24 C4	a3 b31 c1 A4 B42 C2	C1 C2 C4	A3 b34 C4 A4 b42 C2	A1 b14 C4 a2 b21 c1
A3 B33 C3 A4 B41 C1	A1 b13 C3 a2 b24 c4	A1 b13 C3 A2 B22	A1 b13 C3 A2 b22 C2	a3 b33 c3 a4 b42 c2
A1 b12 C2 A2 b24 C4	a3 b31 c1 A4 b42 C2	B24 A3 B32 B34 A4	a3 b31 c1 a4 b44 c4	A1 b14 C4 a2 b21 c1
A3 b33 C3 A4 b41 C1	A1 b13 C3 a2 b24 c4	b41 C1 C2 C4	A1 b13 C3 A2 b22 C2	a3 b33 c3 A4 B42 C2
A1 b13 C3 a2 b21 c1	a3 b32 c2 a4 b41 c1	A1 b13 C3 A2 B21	a3 b31 c1 A4 B44 C4	A1 b14 C4 a2 b21 c1
a3 b32 c2 a4 b44 c4	A1 b13 C3 a2 b24 c4	B24 A3 B31 B34 A4	A1 b13 C3 A2 b22 C2	a3 b33 c3 A4 b42 C2
A1 b13 C3 a2 b21 c1	a3 b32 c2 A4 B41 C1	b42 C2 C1 C4	a3 b31 c1 A4 b44 C4	A1 b14 C4 a2 b21 c1
a3 b32 c2 A4 B44 C4	A1 b13 C3 a2 b24 c4	A1 b13 C3 A2 B21	A1 b13 C3 A2 b22 C2	A3 B33 a4 b42 c2 C3
A1 b13 C3 a2 b21 c1	a3 b32 c2 A4 b41 C1	B22 A3 B31 B32 A4	a3 b34 c4 a4 b41 c1	A1 b14 C4 a2 b21 c1
a3 b32 c2 A4 b44 C4	A1 b13 C3 a2 b24 c4	b44 C4 C1 C2	A1 b13 C3 A2 b22 C2	A3 B32 a4 b43 c3 C2
A1 b13 C3 a2 b21 c1	A3 B32 a4 b41 c1 C2	A1 b13 C3 A2 B24 A3	a3 b34 c4 A4 B41 C1	A1 b14 C4 a2 b21 c1
A3 b33 c3 a4 b41 c1	A1 b13 C3 a2 b24 c4	b31 C1 a4 b42 c2 C4	A1 b13 C3 A2 b22 C2	A3 B32 B33 A4 B42
A1 b13 C3 a2 b21 c1	A3 B31 a4 b42 c2 C1	A1 b13 C3 A2 B22 A3	a3 b34 c4 A4 b41 C1	B43 C2 C3
a3 b34 c4 A4 B42 C2	A1 b13 C3 a2 b24 c4	b31 C1 a4 b44 c4 C2	A1 b13 C3 A2 b22 C2	A1 b14 C4 a2 b21 c1
A1 b13 C3 a2 b21 c1	A3 B31 B32 A4 B41	A1 b13 C3 A2 B22	A3 B34 a4 b41 c1 C4	A3 B33 A4 b42 C2 C3
a3 b34 c4 A4 b42 C2	B42 C1 C2	B24 A3 b31 C1 A4	A1 b13 C3 A2 b22 C2	A1 b14 C4 a2 b21 c1
A1 b13 C3 a2 b21 c1	A1 b13 C3 a2 b24 c4	B42 B44 C2 C4	A3 B31 a4 b44 c4 C1	A3 B32 A4 b43 C3 C2
A3 B34 a4 b42 c2 C4	A3 B32 A4 b41 C1 C2	A1 b13 C3 A2 B24 A3	A1 b13 C3 A2 b22 C2	A1 b14 C4 a2 b21 c1
A1 b13 C3 a2 b21 c1	A1 b13 C3 a2 b24 c4	b31 C1 A4 b42 C2 C4	A3 B31 B34 A4 B41	A3 b32 C2 a4 b43 c3
A3 B32 a4 b44 c4 C2	A3 B31 A4 b42 C2 C1	A1 b13 C3 A2 B22 A3	B44 C1 C4	A1 b14 C4 a2 b21 c1
A1 b13 C3 a2 b21 c1	A1 b13 C3 a2 b24 c4	b31 C1 A4 b44 C4 C2	A1 b13 C3 A2 b22 C2	A3 b32 C2 A4 B43 C3
A3 B32 B34 A4 B42	A3 b31 C1 a4 b42 c2	A1 b13 C3 A2 B24 A3	A3 B34 A4 b41 C1 C4	A1 b14 C4 a2 b21 c1
B44 C2 C4	A1 b13 C3 a2 b24 c4	b32 C2 a4 b41 c1 C4	A1 b13 C3 A2 b22 C2	A3 b32 C2 A4 b43 C3
A1 b13 C3 a2 b21 c1	A3 b31 C1 A4 B42 C2	A1 b13 C3 A2 B21 A3	A3 B31 A4 b44 C4 C1	A1 b14 C4 a2 b21 c1
A3 B34 A4 b42 C2 C4	A1 b13 C3 a2 b24 c4	b32 C2 a4 b44 c4 C1	A1 b13 C3 A2 b22 C2	A3 b33 C3 a4 b42 c2
A1 b13 C3 a2 b21 c1	A3 b31 C1 A4 b42 C2	A1 b13 C3 A2 B21	A3 b31 C1 a4 b44 c4	A1 b14 C4 a2 b21 c1
A3 B32 A4 b44 C4 C2	A1 b13 C3 a2 b24 c4	B24 A3 b32 C2 A4	A1 b13 C3 A2 b22 C2	A3 b33 C3 A4 B42 C2
A1 b13 C3 a2 b21 c1	A3 b32 C2 a4 b41 c1	B41 B44 C1 C4	A3 b31 C1 A4 B44 C4	A1 b14 C4 a2 b21 c1
A3 b32 C2 a4 b44 c4	A1 b13 C3 a2 b24 c4	A1 b13 C3 A2 B24 A3	A1 b13 C3 A2 b22 C2	A3 b33 C3 A4 b42 C2
A1 b13 C3 a2 b21 c1	A3 b32 C2 A4 B41 C1	b32 C2 A4 b41 C1 C4	A3 b31 C1 A4 b44 C4	A1 b14 C4 a2 b22 c2
A3 b32 C2 A4 B44 C4	A1 b13 C3 a2 b24 c4	A1 b13 C3 A2 B21 A3	A1 b13 C3 A2 b22 C2	a3 b31 c1 a4 b43 c3
A1 b13 C3 a2 b21 c1	A3 b32 C2 A4 b41 C1	b32 C2 A4 b44 C4 C1	A3 b34 C4 a4 b41 c1	A1 b14 C4 a2 b22 c2
A3 B32 C2 A4 b44 C4	A1 b13 C3 A2 B24 a3	A1 b13 C3 A2 B22 A3	A1 b13 C3 A2 b22 C2	a3 b31 c1 A4 B43 C3
A1 b13 C3 a2 b21 c1	b31 c1 a4 b42 c2 C4	b34 C4 a4 b41 c1 C2	A3 b34 C4 A4 B41 C1	A1 b14 C4 a2 b22 c2
A3 b34 C4 a4 b42 c2	A1 b13 C3 A2 B22 a3	A1 b13 C3 A2 B21 A3	A1 b13 C3 A2 b22 C2	a3 b31 c1 A4 b43 C3
A1 b13 C3 a2 b21 c1	b31 c1 a4 b44 c4 C2	b34 C4 a4 b42 c2 C1	A3 b34 C4 A4 b41 C1	A1 b14 C4 a2 b22 c2
A3 b34 C4 A4 B42 C2	A1 b13 C3 A2 B22	A1 b13 C3 A2 B21	A1 b13 C3 A2 b24 C4	a3 b33 c3 a4 b41 c1
A1 b13 C3 a2 b21 c1	B24 a3 b31 c1 A4 B42	B22 A3 b34 C4 A4	a3 b31 c1 a4 b42 c2	A1 b14 C4 a2 b22 c2
A3 B34 C4 A4 b42 C2	B44 C2 C4	B41 B42 C1 C2	A1 b13 C3 A2 b24 C4	a3 b33 c3 A4 B41 C1
A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 B24 a3	A1 b13 C3 A2 B22 A3	a3 b31 c1 A4 B42 C2	A1 b14 C4 a2 b22 c2
a3 b31 c1 a4 b44 c4	b31 c1 A4 b42 C2 C4	b34 C4 A4 b41 C1 C2	A1 b13 C3 A2 b24 C4	a3 b33 c3 A4 b41 C1
A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 B22 a3	A1 b13 C3 A2 B21 A3	a3 b31 c1 A4 b42 C2	A1 b14 C4 a2 b22 c2
a3 b31 c1 A4 B44 C4	b31 c1 A4 b44 C4 C2	b34 C4 A4 b42 C2 C1	A1 b13 C3 A2 b24 C4	A3 B33 a4 b41 c1 C3
A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 B24 a3	A1 b13 C3 A2 b21 C1	a3 b32 c2 a4 b41 c1	A1 b14 C4 a2 b22 c2
a3 b31 c1 A4 b44 C4	b32 c2 a4 b41 c1 C4	a3 b32 c2 a4 b44 c4	A1 b13 C3 A2 b24 C4	A3 B31 a4 b43 c3 C1
A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 B21 a3	A1 b13 C3 A2 b21 C1	a3 b32 c2 A4 B41 C1	A1 b14 C4 a2 b22 c2
A1 b12 C2 A2 b24 C4	b32 c2 a4 b44 c4 C1	A1 b13 C3 A2 b21 C1	A1 b13 C3 A2 b24 C4	A3 B31 B33 A4 B41
A3 B33 A4 b41 C1	A1 b13 C3 A2 B21	a3 b32 c2 A4 b44 C4	a3 b32 c2 A4 b41 C1	B43 C1 C3
A1 b13 C3 a2 b22 c2	B24 a3 b32 c2 A4 B41	a3 b32 c2 A4 b44 C4	A1 b13 C3 A2 b24 C4	A1 b14 C4 a2 b22 c2
a3 b34 c4 A4 B41 C1	B44 C1 C4	A1 b13 C3 A2 b21 C1	A3 B32 a4 b41 c1 C2	A3 B33 A4 b41 C1 C3
A1 b13 C3 a2 b22 c2	A1 b13 C3 A2 B24 a3	a3 b34 c4 a4 b42 c2	A1 b13 C3 A2 b21 C1	A1 b14 C4 a2 b22 c2

A3 B31 A4 b43 C3 C1 b31 c1 a4 b42 c2 C3 B23 A3 B31 B33 A4 a3 b33 c3 A4 b42 C2 A1 b14 C4 A2 b22 C2
A1 b14 C4 a2 b22 c2 A1 b14 C4 A2 B22 a3 b42 C2 C1 C3 A1 b14 C4 A2 b21 C1 A3 b31 C1 A4 B43 C3
A3 b31 C1 a4 b43 c3 b31 c1 a4 b43 c3 C2 A1 b14 C4 A2 B21 A3 B33 a4 b42 c2 C3 A1 b14 C4 A2 b22 C2
A1 b14 C4 a2 b22 c2 A1 b14 C4 A2 B22 b43 C3 C1 C2 A1 b14 C4 A2 b21 C1 A3 b31 C1 A4 b43 C3
A3 b31 C1 A4 B43 C3 B23 a3 b31 c1 A4 B42 A1 b14 C4 A2 B23 A3 A3 B32 a4 b43 c3 C2 A1 b14 C4 A2 b22 C2
A1 b14 C4 a2 b22 c2 B43 C2 C3 A1 b14 C4 A2 B23 A3 A1 b14 C4 A2 b21 C1 A3 b33 C3 a4 b41 c1
A3 b31 C1 A4 b43 C3 A1 b14 C4 A2 B22 a3 b31 C1 a4 b42 c2 C3 A3 B32 B33 A4 B42 A1 b14 C4 A2 b22 C2
A1 b14 C4 a2 b22 c2 b31 c1 A4 b42 C2 C3 A1 b14 C4 A2 B22 A3 B43 C2 C3 A3 b33 C3 A4 B41 C1
A3 b33 C3 a4 b41 c1 A1 b14 C4 A2 B22 a3 b31 C1 a4 b43 c3 C2 A1 b14 C4 A2 b21 C1 A1 b14 C4 A2 b22 C2
A1 b14 C4 a2 b22 c2 b31 c1 A4 b43 C3 C1 A1 b14 C4 A2 B22 A3 B33 A4 b42 C2 C3 A3 b33 C3 A4 b41 C1
A3 b33 C3 A4 B41 C1 A1 b14 C4 A2 B23 a3 B23 A3 b31 C1 A4 A1 b14 C4 A2 b21 C1 A1 b14 C4 A2 b23 C3
A1 b14 C4 a2 b22 c2 b32 c2 a4 b41 c1 C3 B42 B43 C2 C3 A3 B32 A4 b43 C3 C2 a3 b31 c1 a4 b42 c2
A3 b33 C3 A4 b41 C1 A1 b14 C4 A2 B21 a3 A1 b14 C4 A2 B23 A3 A1 b14 C4 A2 b21 C1 A1 b14 C4 A2 b23 C3
A1 b14 C4 a2 b23 c3 b32 c2 a4 b43 c3 C1 b31 C1 A4 b42 C2 C3 A3 b32 C2 a4 b43 c3 a3 b31 c1 A4 B42 C2
a3 b31 c1 a4 b42 c2 A1 b14 C4 A2 B21 A1 b14 C4 A2 B22 A3 A1 b14 C4 A2 b21 C1 A1 b14 C4 A2 b23 C3
A1 b14 C4 a2 b23 c3 B23 a3 b32 c2 A4 B41 b31 C1 A4 b43 C3 C2 A3 b32 C2 A4 B43 C3 a3 b31 c1 A4 b42 C2
a3 b31 c1 A4 B42 C2 B43 C1 C3 A1 b14 C4 A2 B23 A3 A1 b14 C4 A2 b21 C1 A1 b14 C4 A2 b23 C3
A1 b14 C4 a2 b23 c3 b32 c2 A4 b41 C1 C3 b32 C2 a4 b41 c1 C3 A3 b32 C2 A4 b43 C3 a3 b32 c2 a4 b41 c1
a3 b31 c1 A4 b42 C2 A1 b14 C4 A2 B21 A3 A1 b14 C4 A2 B21 A3 A1 b14 C4 A2 b21 C1 A1 b14 C4 A2 b23 C3
A1 b14 C4 a2 b23 c3 A1 b14 C4 A2 B21 a3 b32 C2 a4 b43 c3 C1 A3 b33 C3 a4 b42 c2 a3 b32 c2 A4 B41 C1
a3 b32 c2 a4 b41 c1 b32 c2 A4 b43 C3 C1 A1 b14 C4 A2 B21 A1 b14 C4 A2 b21 C1 A1 b14 C4 A2 b23 C3
A1 b14 C4 a2 b23 c3 A1 b14 C4 A2 B22 a3 B23 A3 b32 C2 A4 A3 b33 C3 A4 B42 C2 a3 b32 c2 A4 b41 C1
a3 b32 c2 A4 B41 C1 b33 c3 a4 b41 c1 C2 B41 B43 C1 C3 A1 b14 C4 A2 b21 C1 A1 b14 C4 A2 b23 C3
A1 b14 C4 a2 b23 c3 A1 b14 C4 A2 B21 a3 A1 b14 C4 A2 B23 A3 A3 b33 C3 A4 b42 C2 A3 B32 a4 b41 c1 C2
a3 b32 c2 A4 b41 C1 b33 c3 a4 b42 c2 C1 b32 C2 A4 b41 C1 C3 A1 b14 C4 A2 b22 C2 A1 b14 C4 A2 b23 C3
A1 b14 C4 a2 b23 c3 A1 b14 C4 A2 B21 A1 b14 C4 A2 B21 A3 a3 b31 c1 a4 b43 c3 A3 B31 a4 b42 c2 C1
A3 B32 a4 b41 c1 C2 B22 a3 b33 c3 A4 B41 b32 C2 A4 b43 C3 C1 A1 b14 C4 A2 b22 C2 A1 b14 C4 A2 b23 C3
A1 b14 C4 a2 b23 c3 B42 C1 C2 A1 b14 C4 A2 B22 A3 a3 b31 c1 A4 B43 C3 A3 B31 B32 A4 B41
A3 B31 a4 b42 c2 C1 A1 b14 C4 A2 B22 a3 b33 C3 a4 b41 c1 C2 A1 b14 C4 A2 b22 C2 B42 C1 C2
A1 b14 C4 a2 b23 c3 b33 c3 A4 b41 C1 C2 A1 b14 C4 A2 B21 A3 a3 b31 c1 A4 b43 C3 A1 b14 C4 A2 b23 C3
A3 B31 B32 A4 B41 A1 b14 C4 A2 B21 a3 b33 C3 a4 b42 c2 C1 A1 b14 C4 A2 b22 C2 A3 B32 A4 b41 C1 C2
B42 C1 C2 A1 b14 C4 A2 B22 A1 b14 C4 A2 B21 a3 b33 c3 a4 b41 c1 A1 b14 C4 A2 b23 C3
A1 b14 C4 a2 b23 c3 A1 b14 C4 A2 B22 B22 A3 b33 C3 A4 A1 b14 C4 A2 b22 C2 A3 B31 A4 b42 C2 C1
A3 B32 A4 b41 C1 C2 B23 A3 B32 B33 a4 B41 B42 C1 C2 a3 b33 c3 A4 B41 C1 A1 b14 C4 A2 b23 C3
A1 b14 C4 a2 b23 c3 b41 c1 C2 C3 A1 b14 C4 A2 B22 A3 A1 b14 C4 A2 b22 C2 A3 b31 C1 a4 b42 c2
A3 B31 A4 b42 C2 C1 A1 b14 C4 A2 B21 b33 C3 A4 b41 C1 C2 a3 b33 c3 A4 b41 C1 A1 b14 C4 A2 b23 C3
A1 b14 C4 a2 b23 c3 B23 A3 B31 B33 a4 A1 b14 C4 A2 B21 A3 A1 b14 C4 A2 b22 C2 A1 b14 C4 A2 b23 C3
A3 b31 C1 a4 b42 c2 b42 c2 C1 C3 A1 b14 C4 A2 B21 A3 A3 B33 a4 b41 c1 C3 A3 b31 C1 A4 B42 C2
A1 b14 C4 a2 b23 c3 A1 b14 C4 A2 B21 A1 b14 C4 A2 B21 A3 A1 b14 C4 A2 b22 C2 A1 b14 C4 A2 b23 C3
A3 b31 C1 A4 B42 C2 B22 A3 B31 B32 a4 A1 b14 C4 A2 b21 C1 A1 b14 C4 A2 b22 C2 A3 b31 C1 A4 b42 C2
A1 b14 C4 a2 b23 c3 b43 c3 C1 C2 a3 b32 c2 a4 b43 c3 A3 B31 a4 b43 c3 C1 A1 b14 C4 A2 b23 C3
A3 b31 C1 A4 b42 C2 A1 b14 C4 A2 B21 A1 b14 C4 A2 b21 C1 A1 b14 C4 A2 b22 C2 A3 b32 C2 a4 b41 c1
A1 b14 C4 a2 b23 c3 B22 B23 A3 B31 B32 a3 b32 c2 A4 B43 C3 A3 B31 B33 A4 B41 A1 b14 C4 A2 b23 C3
A3 b32 C2 a4 b41 c1 B33 A4 B41 B42 B43 A1 b14 C4 A2 b21 C1 B43 C1 C3 A3 b32 C2 A4 B41 C1
A1 b14 C4 a2 b23 c3 C1 C2 C3 A1 b14 C4 A2 b21 C1 A1 b14 C4 A2 b22 C2 A1 b14 C4 A2 b23 C3
A3 b32 C2 A4 B41 C1 A1 b14 C4 A2 B22 a3 b33 c3 a4 b42 c2 A1 b14 C4 A2 b22 C2 A1 b14 C4 A2 b23 C3
A1 b14 C4 a2 b23 c3 B23 A3 B32 B33 A4 A1 b14 C4 A2 b21 C1 A3 B31 A4 b43 C3 C1 A3 b32 C2 A4 B41 C1
A3 b32 C2 A4 b41 C1 b41 C1 C2 C3 a3 b33 c3 A4 B42 C2 A1 b14 C4 A2 b22 C2 A3 b32 C2 A4 B41 C1
A1 b14 C4 A2 B23 a3 A1 b14 C4 A2 B21 A1 b14 C4 A2 b21 C1 A3 b31 C1 a4 b43 c3

Bibliografia

- [1] J. M. Anderson, K. L. Carroll, N. P. DeVilbiss, J. T. Gillis, J. C. Hinks, B. W. O. Hanlon, J. J. Rushanan, L. Scott, R. A. Yazdi, "Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals", in *International Technical Meeting of The Satellite Division of the Institute of Navigation, ION GNSS+*, (Portland, Oregon), pp. 2388-2416, sep. 2017
- [2] F. Dovis, "GNSS Interference Threats and Countermeasures", pp. 193-197, 2015
- [3] D. Blazhevski, A. Bozhinovski, B. Stojchevska, V. Pachovski, "Modes of Operation of the AES Algorithm", in *The 10th Conference for Informatics and Information Technology*, 2013
- [4] F. Lever, Entropia, in Franco Lever - Pier Cesare Rivoltella - Adriano Zanicchi (edd.), *La comunicazione. Dizionario di scienze e tecniche*, www.lacomunicazione.it, 09/04/2018
- [5] E. D. Kaplan, "Understanding GPS: Principles and Applications", ed. Boston: Artech House, 1996
- [6] I. Popa, "Spreading Codes", *Buletinul AGIR* nr. 4, pp. 259-264, ott./dic. 2011
- [7] www.activexperts.com/sms-messaging-server/cellular/cdmaspectrum/
- [8] J.A Ávila Rodríguez, "MBOC Modulation", 2011
- [9] <http://www.comefunziona.net/arg/gps/1/>

Ringraziamenti

Comincio ringraziando il mio correlatore Nicola Laurenti, per avermi seguita costantemente nella stesura di questa tesi e per avermi dato l'opportunità di svolgere un lavoro che ho amato. Ringrazio anche Gianluca Caparra, per essere stato un prezioso aiuto nonché il punto di partenza per questa tesi, e il mio relatore Alberto Tonolo, per avermi indirizzata verso questo meraviglioso ambiente in cui ho adorato lavorare.

Ringrazio la mia famiglia, per essere stata sempre al mio fianco, per avermi supportata incondizionatamente e per aver creduto in me anche da molto prima che cominciassi a scrivere questa tesi.

Ringrazio per ultimi, ma non per importanza, il mio ragazzo Elia e i miei amici più cari Lisa, Elia e Lorenzo, per la loro fondamentale presenza e per essere stati quattro pilastri portanti di questo percorso, universitario e di vita.