

Šã~^Áæ~c^¦Á|[&\å[¸}KÁà¦ã^'}\*Á]æ]^¦ÁlÁ



### Ó`ã|åÁ[}Á^¢ã•cã}\*Á,æ|\ã}\*Áæ}åÁ&^&|ã}\*Áā}ç^•c { ^}cÁ ã}Áæ||ÁWSÁ}æcã[}•Ác[Á { ^^cÁc@^Á}^^å•A[~Áà`•ã}^••^•Á ~[¦Á^Ë&æ!\*[Áàã\^Á`•^

### c¦ã]•Ác@æcÁ&[~|åÁà^Á&^&|^åÈÁ

#### •&@^ { ^Ác@~•Á~æ¦È

### Q}&!^æ•^Áã}ç^•c { ^}cÁc [Á•~]][¦cÁ~]cæ\^Á[~Á ^Ë&æ¦\*[Áàã\^•

We need to:

## 1

- $\begin{array}{l} G \dot{E} & Q & A \\ G \dot{E} & A \\ \dot{E} &$
- FÈA Q}ç^•chá}há}~!æ•c¦`&c`!^hæ}åh•`]][!ch-[!h^Ë&æ!\*[hàá\^•h ~[!hà`•i}^••h`•nÈ

 $V@i \bullet h] @]^{h} [] [ \bullet ^ \bullet hc@!^^h!^& [ { ^} a @ ci [ } \bullet hc@ @ cch _ ^hc@i } h ^ ah @ chi + hc@ i +$ 

Y^A}^^åAc[A^}•`!^A^¢@•c@}\*Aæ}åA}^\_A&^&|^A@}-!æ•c!`&c`!^EA@}&|`&@}\*A ]![c^&c^åA&^&|^Ac!æ&\•Aæ}åA][\_Ac!æ-'&A}^@à[`!@[[å•Aæ!^A-`]|^Aæ&&^••@à]^A

æ}åÁ{æi}c^}æ}&^È

Q}ç^•c{ ^}c4~[!Aå { ]![çå} \*Aå}~!æ•c!`&c`!^A~[!A^Ë&æ!\*[Aàå\^A|[\*å•ci&•Aæ•A ]æ!c4[-Ac@ã•Aå•A&!äci&æMå3&|`åä}\*A&^&|^A}^c, [!\•ÊA•c[!æ\*^Aæ}åA]æ!\ä}\*ÊA

 $\begin{array}{l} & \label{eq:constraint} & \label{eq:constraint$ 

Œ}Åå}ç^•c{^}ch]![\*!æ{{^A•@[`|åÅà^Á|æ`}&@^åÅc[Å•^ch`]ÅæÅ}^c,[!\Å [~Å&æ!\*[Åài\^Å|åà!æ!å^•Åæ&![••Åc@^ÅWSÈÅV@å•Åå}ç^•c{^}cÅ•@[`|åÅà^Á-[!ÅæÅ {æ¢å{`{Å[-Å'ç^Å^^æ!•Å,åc@å}ÅæÅ][}\*^!Åc^!{Å\*[æ|Å[-Åc!æ}•åcå[}å}\*Å&æ!\*[Å àå\^Å|åà!æ!å^•Åå}c[Å&&!\*[Åàä\^Å|^æ•å}\*Å•&@^{^•A,@å&@&&!^Å•^]-Ē'}æ}&å}\*Å

Ô[çiåËFJÅ@æ•Å@ick|[&æjkà`•i}^••^•Aæ}åk[!\*æ}i•æci[}•Aàæå|^Aæ}åk{æ}^k @æç^Å@æåkc[k[!kæ!^ki}kc@^k]![&^••k[~kæåæ]ci}\*kc@^i!kà`•i}^••k{{ [å^|•k æ•kæk!^•`|ctÅPi\*@Å•c!^^c•Aæ}åk!^cæij^!•Aæ!^k^•]^&iæ!|^kæ~^&c^åkæ}åk{æ}^Å @æç^kà^^}kc!iæ||i}\*A@[{ ^kå^|iç^!i^•kc[k&[{]|^{ ^}chc@^i!k[-~^!tk

Ö^ç^|[]ÁæÁ}^c [¦\Á[~Á&æ¦\*[Áàã\^Á|ãà¦æ¦ã^•Áæ&¦[••Á

## c@^ÁWŚÁc@¦[`\*@Ácã { ^Á|ã { ãc^åÁã}ç^•c { ^}cÁ ¸ ãc@ÁæÁ •cæc^åÁæã { Á[-Ác¦æ}•ãcã[}ã}\*Ác@^•^Áã}c[Á•^|~Ë'}æ}&ã}\*Á |^æ•ã}\*Á•&@^ { ^•

8

Ù&@^ { ^•Ac [A•`]] [ :chæAc!æ}•äci [ } Ac [A^|^&c!ä&Aç^@ä&|^•A•@ [ ` |&Aæ|• [ Aæ&&!^•+A çæ}A`•^A^•]^&äæ||^Aä}A`:`aæ}Aæ!^æ+Aæ}aÅæåäci [ }æ|A•`]] [ :ch { `•chà^A\*äç^}A

¦ã\*@cÁ\*[ç^¦} { ^}cÁã}&^}cãç^●ĚÁ

Q} Aæååacă [ } Ac [ A!^å ~&i} \* Ac@^A' •^A[\_A { [c[!Aç^@ā&|^•ÊAā-A, ^Aæ!^Ac[A !^å~&^AÕPÕÁ^{ {ā•sā} } •A-![ { Ac!æ}•] [ :c4, ^A}^^åAc[A`!\*^}c]^A•c[] A `•ā} \*A { [c[!Aç^@ā&|^•A] [ \_^!^åAà^Aåà^•^|Aæ}Å]^c![!ÈAÞ[!, æ^A@æ•A •@[ \_}Ac@ā•Aā•Aæ&@ā^çæà]^Aá}AæA!^|æciç^|^A•@[!cAci { ^-!æ { ^A} āc@Ac@^A

# $\dot{O}|^&c!a^{\dot{A}} \{ [c[!Ac!æ] • ] [!cA • [Ac@æcAæ]|A }^ Açæ \} • A æ!^A^]^&c!a&A^{A} = A c!a&A^{A} = A c.a&A^{A} = A c.a&A^{A}$

Ô[} • [|ååæci]} Å [-Å|[&æ|Åå^|äç^1å^•Å~![{ Å@å\*@Å•c!^^cÅ!^cæi]^!•Åå•Åæ|•[Å\*æi}å}\*Å ][]`|æ!åc^ÈÁÚ^[]|^Å^åc@^!Å[]}å}^Å[!Åä}Å]^!•[]Å&æ}Å•^|^&ckåc^{{}}&{}^{A}-![{ &æA çæ!å^c^Å[-Ååä-^!^}ck!^cœi]^!•Åä}ÅæÅ][&æ|Åæ!^æÅæ}åſŕ^!çä&^Åi=Å`\*^åÅc[Åå^]äç^!Å c@^•^Å\*[[å•Åc[Å^[`1Å@]{ ^ÊÅc^]å&æ]]^Åà^Å^Ë&æ!\*[Åàå`\^ĖÅV@å•Å{ &\^Å][&æ]Å c@^•^Å\*[[å•Åc[Å^[`1Å@]{ ^ÊÅc^]å&æ]]^Åà^Å^Ë&æ!\*[Åàå`\^ĖÅV@å•Å{ &\^Å][&æ]Å c@[]]å}\*Å { [!^Åä}&]`\*äç^Å-[!Å]^[]!^Å, @[Å { æ^Å•c!`\*\*|^Åc[Å&æ!!^Å { `[ci]]^Å åc^ { •Åæ}åÅä[Å][cÅ, @}cÅc[Åä!äç^Å[!Å&æ}}[c&æ&&^•AæÅç^@å&|^ÈÅØä}æ}&åæ]Å •`]][!cÅæ}åÅå]-!æ\*c!`&c`!^Åc[Åæ•\*i\*cÅc@^\*^A\*&@^ { ^•Å, [`|åÅà^Å@^]]~`]ĖÅ

$$\begin{split} \dot{U}_{c^{-}} & \bullet & \oplus & [ \ aha^{kcw} \ back \ b$$

###