Sto vězňů a žárovka

Filip Hlásek

Abstrakt. Příspěvek se zamýšlí nad známým komunikačním problémem, kde se agenti (vězni) pomocí jednoduchého média (žárovky) a lokálních změn systému (přepnutí žárovky) snaží předat globální informaci týkající se jich všech. Na první pohled je až neuvěřitelné, že lze úlohu vůbec vyřešit. Když vězeň vidí svítící žárovku, neví, kdo ji rozsvítil; pokud se rozhodne zhasnutou žárovku rozsvítit, neví zase, kdo ji poté uvidí svítit. Přesto ukážeme, že pomocí takto jednoduchého komunikačního prostředku lze navrhnout protokol k přenosu mnoha informací.

Budeme se zabývat známou a tradiční úlohou. Nebyla vždy takto populární a do obecného povědomí se dostala až začátkem jednadvacátého století. Vše začalo v roce 2002, kdy americká technologická společnost IBM vypsala soutěž týkající se této úlohy. Poté se objevily nové varianty hádanky a vědecké články, které vedou k pozoruhodným aplikacím při návrhu komunikačních protokolů. Především teoreticky se jedná o velmi zajímavý problém a existuje mnoho dosud nezodpovězených otázek souvisejících s tímto tématem.

Zadání problému

Do nejmenované věznice právě nastoupilo sto nových vězňů. Bachař jim dá šanci vymanit se ze svého trestu. Počínaje zítřkem budou vězněni v oddělených celách a každý den bude vybrán jeden vězeň k výslechu. Jediným zajímavým předmětem ve výslechové místnosti je běžná žárovka, což je také jediný prostředek, pomocí kterého spolu mohou vězni komunikovat. Žárovku vidí pouze právě vyslýchaný vězeň a může ji dle svého uvážení zhasnout nebo rozsvítit. Kdykoliv může kterýkoliv vězeň ohlásit: „Všech sto vězňů již bylo alespoň jednou vyslechnuto.“ Pokud je to pravda, budou všichni okamžitě propuštěni, v opačném případě budou všichni popraveni. Pomozte vězňům domluvit si spolehlivou strategii, díky které se jim podaří dosáhnout svobody.

Předpoklady

(a) Každý vězeň bude vyslechnut nekonečněkrát. V některých případech budeme potřebovat dokonce, aby každý den byl vyslechnut náhodný vězeň.
(b) Žárovka je na začátku zhasnutá.
(c) Každý den je vyslechnut právě jeden vězeň.

Řešení úlohy

V této sekci navrhneme několik různých postupů, jak spolu mohou vězni pomocí žárovky komunikovat. Navíc ke každému uvedeme také střední počet dní než vězni budou propuštěni. Předpokládáme, že každý den má každý vězeň se stejnou pravděpodobnost, že bude vyslechnut.

Zkusíme štěstí

Rozdělíme dny na bloky po 100 dnech. Během každého bloku budou vězni komunikovat podle následujících pravidel:

(1) Pokud je první den bloku a žárovka je zhasnutá, rozsviť ji.
(2) Je-li žárovka rozsvícená a jsi v tomto bloku vyslechnut podruhé, zhasni ji.
(3) Pokud je první den bloku a žárovka je rozsvícená, ohlaš, že již všichni byli vyslechnuti.
(4) Ve všech ostatních případech ponechej stav žárovky nezměněný.

Když některý vězeň ohlásí, že všichni byli vyslechnuti, musel být každý vyslechnut právě jednou v přecházejících 100 dnech. Pokud by tam někdo v minulém bloku byl dvakrát, žárovku by zhasnul. Ona ale zůstala rozsvícená, a proto tam byl každý jenom jednou.

(střední doba trvání: $\frac{n^{n+1}}{n!} \sim \sqrt{\frac{n}{2\pi}} e^n \doteq 1,072 \times 10^{44}$ *dní)*

Počtář

Následující protokol nespoléhá na počítání dní, ale dává speciální funkci jednomu vězni. Před začátkem se domluví na jednom z nich, který bude mít roli *počtáře*. Tento počtář si bude pamatovat jedno celé číslo: počet spoluvězňů, o kterých si je jist, že již byli vyslechnuti.

Všichni ostatní vězni si budou pamatovat také jednu hodnotu: zda již počtáři sdělil, že již byl vyslechnut. Pro lepší představu uvážíme, že má na začátku jeden *token* (= virtuální předmět, který se snaží předat počtáři).

Dále popíšeme detailněji systém, jakým si vězni budou předávat tokeny:

(1) Pokud nejsi počtář, máš ještě token a je zhasnuto, rozsviť a uber si jeden token.
(2) Jsi-li jsi počtář a je-li rozsvíceno, zhasni a připočti si jeden token.
(3) Pokud jsi počtář a nasbíral jsi všech 100 tokenů (včetně svého), ohlaš úspěch.
(4) Ve všech ostatních případech ponechej stav žárovky nezměněný.

(střední doba trvání: $O(n^2) \sim 10417,74$ *dní* $\doteq 28,54$ *let)*

Dynamická volba počtáře

Trochu vylepšíme předcházející protokol tím, že zvolíme počtáře až v průběhu, nikoliv dopředu. Počtářem se stane ten, kdo bude první vyslechnut podruhé během prvních n dní. Celý protokol se tedy skládá ze dvou fází:

(1) prvních n dní – Pokud budeš vyslechnut podruhé a je v mísnosti zhasnuto, rozsviť a staň se počtářem. Ostatní poté vidí rozsvíceno a ví tedy, že funkci počtáře už si někdo vzal. Kdyby nikdo nepřišel do místnosti podruhé, bude v n-tém dni pořád zhasnuto a vězeň vyslýchaný ten den bude vědět, že všichni byli jednou vyslechnuti. Může tedy ohlásit úspěch.
(2) dny $n+1, n+2, \ldots$ – Uvažme, že počtář byl vyslechnut podruhé v k-tém dni. Předtím bylo vyslechnuto $k-1$ různých lidí. Jsou to právě ti, kteří viděli v první fázi zhasnutou žárovku. Můžeme tedy postupovat podle předcházejícího protokolu s tím rozdílem, že těch $k-1$ různých lidí již své tokeny počtáři předalo (vědí to oni i počtář).

Pomocní počtáři

Zásadní nevýhodou jednoho počtáře je, že se vždy poměrně dlouho (průměrně 100 dní) než přijde a vezme si token. Navrhneme protokol, který používá 10 *pomocných počtářů* a jednoho *hlavního počtáře* (může to být dokonce jeden z pomocných počtářů). Každý pomocný počtář bude sbírat tokeny až dokud jich nebude mít 10 a poté je pošle hlavnímu počtáři. Ten je nasbírá po desítkách a teoreticky by stačilo, aby byl každý vyslechnut přibližně dvacetkrát místo předchozích minimálně 100 výslechů počtáře.

Na první pohled to může vypadat přímočaře, otázkou ale zůstává jak předávat tokeny. Samozřejmě, že pomocí žářovky (žádný jiný prostředek totiž nemáme). Problém je ale v tom, že není jasné, zda rozsvícená žárovka znamená poslání jednoho tokenu od *nepočtáře* nebo jednoho *desítkového* tokenu od pomocného počtáře tomu hlavnímu. Je potřeba je nějak odlišit, ale žárovka bohužel může být pouze rozsvícená nebo zhasnutá. Tento problém vyřešíme úskokem. Rozdělíme dni na jednotlivé fáze. V první fázi (například 100 dní) budou posílat nepočtáři svoje jednotkové tokeny a pomocní počtáři je budou sbírat. Poté bude následovat druhá fáze (například také 100 dní), kdy budou moci pomocní počtáři poslat své desítkové tokeny (pokud již

nasbírali deset jednotkových) a hlavní počtář je bude sbírat. Po druhé fázi bude následovat opět první fáze a takto se budou střídat, dokud hlavní počtář neposbírá všech 100 tokenů. Každý vězeň si musí důkladně počítat dni a vědět, která fáze právě probíhá.

Ani tentokrát nemáme ještě vyhráno. Problém nyní může nastat tak, že nepočtář vyšle v první fázi token, ale do konce fáze nebude vyslechnut žádný počtář. Potom bude druhá fáze a když bude vyslechnut hlavní počtář, může si myslet, že rozsvícená žárovka symbolizuje desítkový token poslaný od pomocného počtáře. Takto může velmi snadno dojít k nedorozumění, které povede k neúspěchu. Bude potřeba důsledněji hlídat, aby tokeny „nepřetékaly“ mezi fázemi. Opravíme to tak, že během posledního dne každé fáze vyslýchaný vězeň sebere token, pokud je žárovka rozsvícená, a to nezávisle na tom, zda je to počtář. I nepočtář tak může mít u sebe několik jednotkových i několik desítkových tokenů. Tyto tokeny se pokusí při nejbližší vhodné příležitosti doručit správým příjemcům. Když má nějaké tokeny, které mu nenáležejí, je správná fáze a zhasnutá žárovka, vyšle jeden z nich rozsvícením žárovky.

Tento poměrně komplikovaný doručovací mechanizmus již funguje a nyní ho popíšeme přesněji. Každý vezeň si bude pamatovat počet jednotkových a desítkových tokenů, které vlastní. Každý začíná s jedním jednotkovým tokenem.

Hlavní počtář

(1) Pokud máš 10 desítkových tokenů, ohlaš vítězství.
(2) Pokud je druhá fáze a žárovka je rozsvícená, zhasni a připočti si desítkový token.
(3) Pokud je první fáze, máš jednotkový token a žárovka je zhasnutá, rozsviť a odeber si jeden token.
(4) Je-li poslední den první fáze a je-li rozsvíceno, zhasni a připočti si jednotkový token.

Pomocný počtář

(1) Pokud máš 10 jednotkových tokenů, zahoď je a vyrob z nich jeden desítkový token. Přestáváš být pomocným počtářem a stáváš se nepočtářem.
(2) Pokud je první fáze, žárovka je rozsvícená, zhasni a připočti si jednotkový token.
(3) Pokud je druhá fáze, máš desítkový token a žárovka je zhasnutá, rozsviť a odeber si desítkový token.
(4) Je-li poslední den druhé fáze a je-li rozsvíceno, zhasni a připočti si desítkový token.

Nepočtář

(1) Pokud je první fáze, máš jednotkový token a žárovka je zhasnutá, rozsviť a odeber si jeden token.
(2) Je-li poslední den první fáze a je-li rozsvíceno, zhasni a připočti si jednotkový token.

(3) Pokud je druhá fáze, máš desítkový token a žárovka je zhasnutá, rozsviť a odeber si desítkový token.
(4) Je-li poslední den druhé fáze a je-li rozsvíceno, zhasni a připočti si desítkový token.

(střední doba trvání: $3\,500 - 4\,000$ *dní* $\doteq 9,5 - 11$ *let)*

Binární tokeny

Myšlenku uvedenou v předcházejícím řešení se nyní pokusíme ještě zobecnit a dosáhnout tak téměř nejlepšího dosud známého postupu. Jak již název napovídá, nebudou počtáři shlukovat tokeny po deseti, ale po mocninách dvojky. Budeme potřebovat, aby počet všech tokenů byla mocnina čísla dva. Když počet vězňů není mocnina dvojky, dáme na začátku některému vězni tokenů více.

Uvažujme dále, že všichni vězni dohromady mají 2^k tokenů. Jejich počáteční rozdělení si domluví před začátkem, jediné důležité je, aby měl každý alespoň jeden. Jakmile je někdo získá všechny, může ohlásit úspěch. Podobně jako v minulém případě budou i tentokrát jednotlivké tokeny různě cenné. Konkrétně máme $k+1$ druhů tokenů o hodnotách $2^0, 2^1, \ldots, 2^k$. Jakmile někdo získá dva tokeny stejné hodnoty 2^i udělá z nich jeden hodnoty 2^{i+1}.

Jak si budou vězni tokeny mezi sebou předávat? Opět nás nezklame myšlenka rozdělení na fáze z pomocných počtářů. Tentokrát bude ovšem fází k a bude mnohem více záviset na jejich velikosti. Jako nejlepší se ukazují stejně dlouhé fáze o zhruba 613 dnech. Máme již všechno potřebné k tomu, abychom pořádně popsali jak budou vězni komunikovat v i-té fázi:

(1) Pokud máš token hodnoty 2^k, ohlaš úspěch.
(2) Pokud máš dva tokeny hodnoty 2^j pro nějaké celé j, udělej z nich jeden token hodnoty 2^{j+1}.
(3) Je-li žárovka rozsvícená, zhasni ji a připočti si token hodnoty 2^i.
(4) Je-li žárovka zhasnutá a máš-li token hodnoty 2^i, rozsviť a odeber si token.

(střední doba trvání: $O(n(\ln n)^2) \sim 3\,500$ *dní* $\doteq 9$ *let)*

Varianty úlohy

(1) **Zákeřný bachař** – Je dáno předem známé přirozené číslo k. Bachař může k-krát během celého procesu změnit stav žárovky (rozsvítit nebo zhasnout).
(2) **Všichni musí ohlásit** – Vězni budou propuštěni jedině tehdy, pokud všichni ohlásí, že již všichni byli vyslechnuti.
(3) **Propuštěný po ohlášení** – Všichni vězni musejí ohlásit, ale pokud někdo ohlásí, je okamžitě propuštěn a už nikdy nebude vyslýchán.
(4) **Červené a modré cely** – Někteří vězni jsou ubytovaní v červených celách,

zatímco ostatní v modrých. Při ohlášení musí vězeň také nahlásit, kolik jeho kolegů bydlí v červených a kolik v modrých celách.

(5) A **pošle zprávu** B – Předem určený vězeň A musí poslat zprávu (přirozené číslo) vězni B.

(6) **Čísla v celách** – V každé cele je napsáno jedno celé číslo. Vězeň, který ohlašuje, musí nahlásit také všechna tato čísla.

(7) **Všichni posílají zprávy všem** – Navrhněte obecný protokol, pomocí kterého si budou moci navzájem posílat jakékoliv zprávy.

(8) **Všichni musejí ohlásit ve stejný den** – Vězni mohou ohlásit, že již všichni byli vyslechnuti, také ve dny, kdy nejsou vyslýcháni. Budou propuštěni jedině tehdy, pokud to všichni ohlásili ve stejný den. Ohlásí-li to někdo dříve, budou všichni popraveni.

(9) **Náhodné časy** – Řešte všechny předcházející úlohy bez předpokladu (c). Vězni jsou vyslýcháni v náhodné časy a nemohou tedy počítat dny.

Návody na řešení jednotlivých variant

(1) Zákeřný bachař

Každý vězeň bude mít $2k + 1$ tokenů (méně nestačí!) a když počtář napočítá do $100(2k + 1) - k$ může ohlásit, že již všichni byli vyslechnuti.

(2) Všichni musí ohlásit

Použijeme strategii *počtář*, jenom budou tokeny n různých druhů (tedy n fází). Každý vězeň bude mít na začátku token určený pro každého jiného. Každý vězeň je počtářem svého druhu tokenů.

(3) Propuštění po ohlášení

Funguje předcházející strategie – vězeň ohlásí až tehdy, když nasbírá svých sto tokenů a zbaví se všech ostatních.

(4) Červené a modré cely

Použijeme jednoho *počtáře*, který bude sbírat dva druhy tokenů – červené a modré (dvě fáze). Nasbírá-li dohromady 100 tokenů, ohlásí kolik z nich bylo červených a kolik modrých.

(5) A pošle zprávu B

Vězeň A zakóduje zprávu do binární soustavy. Chce-li používat jiné znaky než jedničky a nuly, mohou se domluvit na posílání například po pěti bitech, kde každá pětice bude vyjadřovat jedno písmeno. Navíc potom pět nul může znamenat konec zprávy. Jak ale posílat jedničky a nuly?

Použijeme opět dva druhy tokenů: *nulový* a *jedničkový*. Vězeň A bude postupně posílat věznì B jednotlivé bity zprávy až do konce. Bohužel se ale při přenosu nezachová pořadí a vezeň B dostane nejspíše bity přeházené. Abychom tomu zabránili, přidáme ještě potvrzovací token, který pošle vezeň B věznì A, po přijetí jednoho bitu (nulového nebo jedničkového tokenu). Vezeň A vždy po vyslání bitu čeká na potvrzovací token než bude pokračovat vysíláním dalšího bitu. Potřebujeme tedy celkem tři fáze a tomu odpovídající tři typy tokenů. Všichni ostatní věznì si musejí pamatovat kolik mají kterých tokenů, ale naštěstí mohou mít všichni dohromady v každém okamžiku nejvýše jeden token (buď se posílá bit nebo čeká na potvrzení přijetí).

(6) Čísla v celách

Komunikační kanál popsaný v předchozí pasáži realizujeme mezi počtářem a každým vězněm. Celkem tak bude potřeba 3×99 různých tokenů. Stejný počet bude také fází a každý vezeň si bude muset pamatovat, kolik kterých tokenů drží.

(7) Všichni posílají zprávy všem

Opět použijeme stejný mechanizmus, ale tentokrát budeme potřebovat dokonce $\frac{3n(n-1)}{2}$ druhů tokenů. Každý vezeň takto může komukoliv poslat jakoukoliv zprávu a to vše věznì realizují pomocí jediné žárovky.

(8) Všichni museji ohlásit ve stejný den

Vzhledem k předchozím výsledkům to může znít poměrně překvapivě, ale skutečně není možné navrhnout spolehlivý postup, pomocí kterého by věznì ohlásili, že již všichni byli vyslechnuti, ve stejný den. Pro spor předpokládejme, že taková strategie existuje a uvažme nějakou posloupnost vyslýchání vezňů, při které všichni věznì ohlásí, že již byli vyslechnuti. Každý vezeň se musí někdy rozhodnout, že i pokud by už nebyl vyslechnut, tak v nějaký den D ohlásí. Podívejme se na takového vězně, který se pro to rozhodne jako první. Od toho dne už ho nebudeme vyslýchat a jako zákeřný bachař budeme stále vyslýchat jednoho jiného vězně až do dne D. Žádný jiný vězeň se tedy nerozhodne ohlásit (jedině tito dva) a jejich spolehlivá strategie selhává. To je spor s existencí takové strategie.

Přestože si věznì mohou vyměnit jakékoliv zprávy, nemohou se domluvit na jednom konrétním dni tak, aby se to všichni stihli dozvědět. Schopnost vyměňovat si

zprávy je sice silný nástroj, ale vězni nemají žádný odhad na to, jak dlouho bude posílání zprávy trvat.

A co bez počítání dní?

Dále navrhneme protokol, pomocí něhož si vězni mohou posílat zprávy bez toho, aby počítali dni. Ve všech předchozích řešeních bylo naprosto klíčové, aby vězni přesně věděli, která právě probíhá fáze a není možné uvedené postupy přímo aplikovat. Zprávu budeme reprezentovat jako nezáporné celé číslo N (například ve dvojkové soustavě). Vězeň A bude vězni B postupně posílat N tokenů. Jelikož A je jediným odesilatelem (jediný, kdo rozsvěcí žárovku) a B jediným příjemcem (jediný, kdo žárovku zhasíná), nemohou se tokeny nikde ztratit a po určité době dojde jistě celá zpráva k B. Poté A přestane vysílat tokeny, ale problém je s tím, že B neví jestli má ještě čekat, že mu něco přijde.

Na první pohled to opět vypadá na neřešitelný problém, ale přesto ukážeme postup jak ho vyřešit. Vězeň B občas pošle jeden token zpátky, aby vyzkoušel, jestli už A poslal všechno. Pokud A již poslal všechno a viděl zhasnuto (t.j. ví, že B vše přijal), je potom ochoten přijmout jeden token. Když se potvrzení podaří, uvidí poté B opět zhasnuto a bude si jist, že dostal celou zprávu. Pokud potvrzení nedostane (buď proto, že A bude ještě posílat, nebo mezitím nebyl vyslechnut), zkusí to B po nějaké době znovu.

Uvedeným postupem může předem zvolený vězeň poslat jakoukoliv zprávu jinému předem určenému vězni. Tentokrát ovšem není vůbec jasné, jak protokol rozšířit pro komunikaci každé dvojice vězňů. Je možné navrhnout systém, jak se budou vězni dorozumívat každý s každým i pokud nemohou počítat dni. Je ale poměrně náročný a zdlouhavý, a proto ho nebudeme uvádět. Jeho kompletní popis spoleně s detailním rozborem většiny uvedených metod naleznete v článku [4].

Literatura a zdroje

[1] IBM Research, *100 prisoners and a lightbulb challenge*, 2002.
[2] *https://www.math.washington.edu/~morrow/336_11/papers/yisong.pdf*
[3] *http://www.ocf.berkeley.edu/~wwu/papers/100prisonersLightBulb.pdf*
[4] *http://www.segerman.org/prisoners.pdf*
[5] *http://personal.us.es/hvd/newpubs/FinalLightKR.pdf*