Tato práce se zaměřuje na důkaz redukce přibližného SBP na SIS. Důkaz provedl již Miklós Ajtai v roce 1996 ve své přelomové práci, avšak jeho důkaz je místy často nejasný a některé kroky nejsou dostatečně rozepsány. Redukce je typu nejhorší případ převeden na průměrný případ. Před zmíněnou prací Ajtaie nebyla známa žádná redukce takového typu. Proto nám přijde vhodné se k důkazu vrátit a rozepsat všechny jeho kroky do většího detailu. Dále je v práci shrnuta složitost základních problémů na mřížkách. Na základě těchto složitostí a dokázané redukce je možné definovat hashovací funkce odolné vůči kolizím. Na takové funkce se tato práce také zběžně zaměřuje.