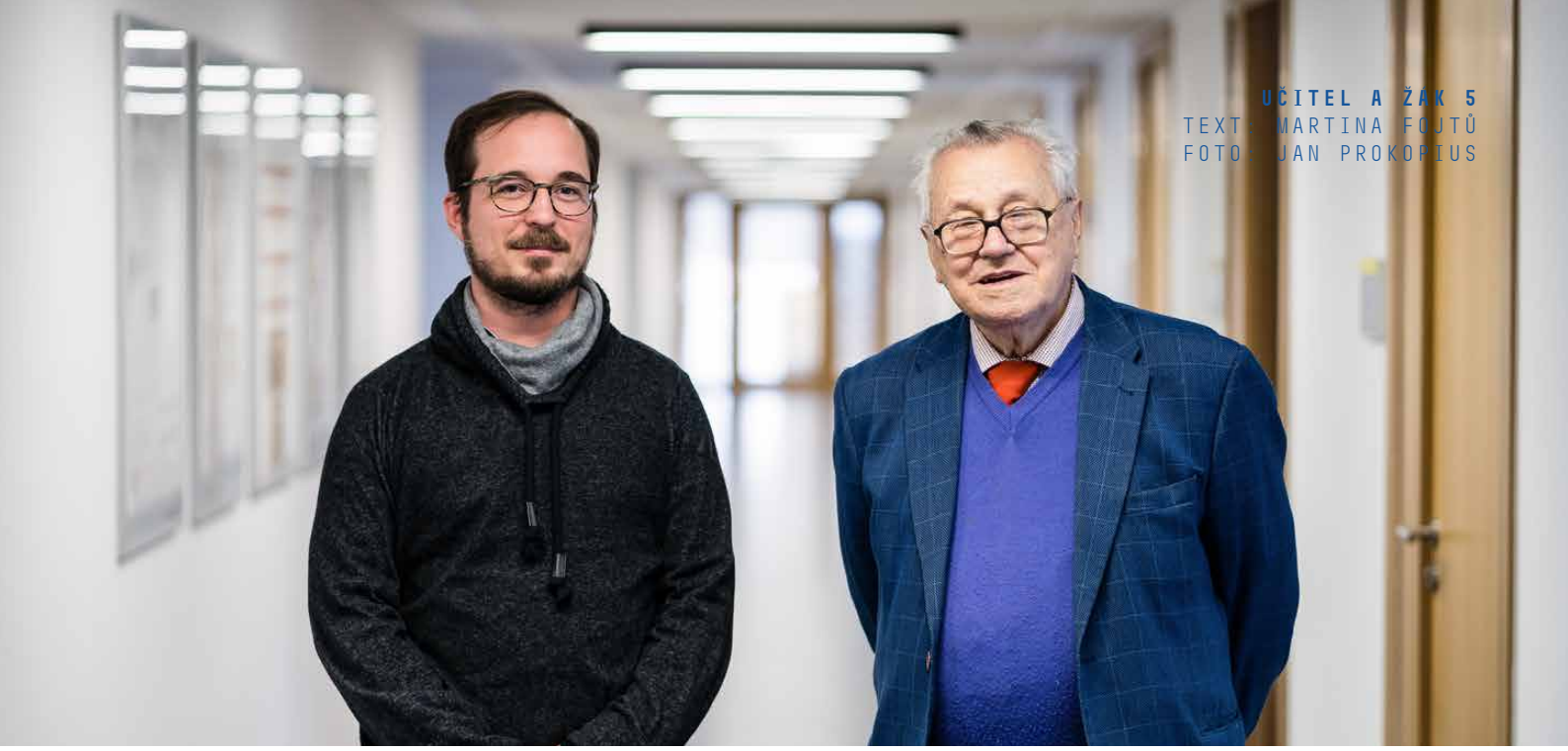
TEXT: MARTINA FOJTŮ
FOTO: JAN PROKOPIUS



Nejdřív známka F, pak úspěšná spolupráce

JOSEF GRUSKA byl v 80. letech jedním z prvních, kdo se pustil do kvantových počítačových systémů a je podepsaný pod texty, které vědci citují po celém světě. Stanovil vize, které teď jeho následovník **MATEJ PIVOLUSKA** pomáhá naplňovat.

Jejich první setkání už si ani jeden nepamatuje, každopádně bylo minimálně pro jednu stranu dost depresivní. Matej Pivoluska byl čerstvým studentem fakulty informatiky, když si hned v prvním ročníku zapsal přednášky z kryptografie vedené Jozefem Gruskou a na konci semestru skončil se známkou F. „Vůbec jsem to tehdy nezvládal, ničemu jsem nerozuměl, takže jsem tam přestal chodit," vzpomíná dnes už expert s doktorátem z teoretické informatiky.

Jen co nabral vědomosti jinde, zapsal si kryptografii ve čtvrťáku znovu a to už mu šla tak dobře, že se zařadil do skupiny lidí, kteří později chystali úkoly v tomto předmětu pro svoje nástupce. Někdy v této době se Pivoluska teoretickou informatiku oblíbil, což vedlo až k tomu, že dnes dělá na ústavu výpočetní techniky neobyčejně složitou vědeckou práci v oblasti využívání kvantových jevů pro zabezpečení informací a počítačů.

Jeho školitelem na doktorátu byl právě Jozef Gruska. Muž, jenž je jednou z nejvýznamnějších postav oboru v celém bývalém Československu i na světě. Značnou část života strávil na univerzitách a institucích v zahraničí – v Asii například založil a 15 let ideově vedl jednu z nejdůležitějších oborových konferencí, stanovil vize oboru a v roce 1999 ve Velké Británii vydal vůbec první monografii v oblasti kvantových počítačových systémů, 430stránkovou publikaci Quantum computing.

„Když se zrodila myšlenka kvantového počítače, bylo to, jako když biologové objevili DNA – nikdo ještě nevěděl, co všechno to způsobí, ale bylo jasné, že se to promítne do mnoha oblastí," přibližuje Gruska.

Jeho obor se pořád vědecky pohybuje na úrovni základního výzkumu, v němž se mapují vlastnosti kvantových jevů i potenciální možnosti využití. Řečeno zcela jednoduše jde hlavně o to, že kvantové počítače by dokázaly proniknout daleko hlouběji do poznání světa a podat daleko víc informací.

Pivoluska dává konkrétní příklad třeba z chemie. „V ní je potřeba simulovat chování velmi malých objektů. Když máte například molekulu kofeinu, tak ta má 14 atomů, a když chcete pohyb všech sledovat v čase, v tuto chvíli to ani na superpočítačích nejde. Limitují to kvantové jevy, které se v částicích dějí. Proto se tolik uvažuje o využití kvantových počítačů, které to budou schopny zachytit," naznačuje Pivoluska jejich ohromný potenciál.

Kvantové počítače však zatím existují jen v malém provedení, jsou to zatím spíš jen modely toho, co by mohlo být. Přesto se právě do této oblasti výzkumu, která vyžaduje také zapojení fyziků nebo logiků, pouští čím dál víc expertů a také vědecké instituce už se do nich naučily investovat prostředky a vypisovat patřičné výzvy.

Pivoluska rozvíjí jeden konkrétní směr – zabezpečení informací. V létě publikoval spolu s kolegy z Vídně a Edinburghu v časopise Nature Physics článek o tom, jak pro efektivnější obranu využít takzvané kvantové zapletení. V současnosti se při ochraně informací využívá toho, že částice, do kterých se informace kóduje, nabývají jenom dvou hodnot – jedniček nebo nul. Zmiňované kvantové zapletení lze ale vytvořit i za pomoci vícedimenzionálních částic, které nabývají až nekonečného množství hodnot, což by znamenalo navýšení kapacity i bezpečnosti. •